БОГУШ В.М., КРИВУЦА В.Г., КУДІН А.М.

ІНФОРМАЦІЙНА БЕЗПЕКА

* * *

ТЕРМІНОЛОГІЧНИЙ ЕЛЕКТРОННИЙ НАВЧАЛЬНИЙ ДОВІДНИК

Близько 4000 термінів та понять

За ред. професора Кривуци В.Г.

Київ
2004

Електронна версія навчального видання

УДК 681.3

Богуш В.М.,Кривуца В.Г.,Кудін А.М.
Інформаційна безпека: Термінологічний навчальний довідник / За ред. Кривуци В.Г. — Київ:ООО "Д.В.К.", 2004 . — 508 с.

ISBN 966 - 96313 - 1 - 0

У структурованому вигляді викладено близько 4000 загальних та спеціальних термінів і понять, склад яких відповідає навчальним програмам профільних дисциплін вищих навчальних закладів для всіх спеціальностей з інформаційної безпеки.

Докладно розглянуті сучасні основи інформаційної безпеки особистості, суспільства та держави. Значну увагу приділено загрозам інформаційній безпеці, інформаційним війнам та інформаційній боротьбі, інформаційно-психологічній безпеці, безпеці інформаційних технологій, криптології, технічним методам та засобам захисту інформації, правовому та організаційно-технічному захисту інформації, захисту інформації в комп'ютерних системах та мережах, державній та комерційній таємниці тощо.

Для студентів, що навчаються на освітнім напрямом "Інформаційна безпека". Може бути корисний широкому колу читачів: від політиків і бізнесменів до науковців та інженерів.

SBN 966 - 96313 - 1 - 0

ПЕРЕДМОВА

На початок XXI сторіччя припадає революційна фаза розвитку суспільства — на зміну індустріальному суспільству приходить інформаційно-індустріальне суспільство, в якому велике значення набувають системи розповсюдження, зберігання і оброблення інформації.

Автоматизовані інформаційні системи проникають в усі напрямки діяльності держави, суспільства, громадянина. З появою нових інформаційних технологій, заснованих на широкому впровадженні засобів обчислювальної техніки, зв'язку, систем телекомунікацій, вони стають постійним і необхідним атрибутом забезпечення діяльності держави, юридичних осіб, суспільних об'єднань і навіть пересічних громадян. Системи електронного документообігу в державних установах, система електронних платежів, карткова система сплати телефонних дзвінків, телевізор із телетекстом або телефонні та відеотелефонні розмови через Інтернет уже стали часткою повсякденного життя. Наслідком цього стало те, що процес електроного урядування в передових країнах втілюється в життя уже з кінця 90-х років минулого сторіччя. Насьогодні до цього процесу приєдналась і Україна. З прийняттям в 2002-2003 роках Законів України "Про Національну систему конфіденційного зв'язку", "Про електронні документи та електронний документообіг" та "Про електронний цифровий підпис" утворюється правова база для реалізації в України ефективної системи електронного уряду.

Іншою стороною цих процесів є збільшення кількості цінної інформації, яка обробляється в автоматизованих системах, від якості, достовірності і оперативності одержання якої залежить більшість важливих рішень, що приймаються на різних рівнях – від голови дер-

жави до громадянина. Як наслідок — нормальне життя суспільства все більше залежить від правильності функціонування таких інформаційних систем. Більш того, вони стають і найважливішим об'єктом для атаки з боку сил, ворожих для суспільства (або окремої держави). Інформаційна сфера стає не тільки однією з найважливіших сфер міжнародного співробітництва, але і об'єктом суперництва.

Інформаційний вплив на державу, суспільство, громадянина зараз більш ефективний і економний, ніж політичний, економічний і навіть воєнний. Країни з більш розвиненою інформаційною інфраструктурою, встановлюючи технологічні стандарти й надаючи покупцям свої ресурси, визначають умови формування і діяльності інформаційних структур в інших країнах, здійснюють суттєвий вплив на розвиток їхніх інформаційних сфер.

При формуванні державної інформаційної політики і програми входження в інформаційне суспільство одним із найбільших пріоритетів стає розвиток і гарантування безпеки інформаційної сфери на основі створення державної системи інформаційної безпеки.

Зважаючи на підвищення інтересу до проблеми забезпечення інформаційної безпеки, появі спеціальностей за освітнім напрямом "Інформаційна безпека" у вищих навчальних закладах України, на думку авторів, сьогодні існує гострий дефіцит навчально-методичної та популярної літератури з цих питань. Окремою проблемою є відсутність "середньої" літератури: досить простої для сприйняття навіть нефахівцями при строгості викладення та довідкової літератури. На думку авторів її створення слід починати з системного розроблення загальносприйнятливої наукової термінології, тлумаченню якої і присвячена ця книга.

Вона побудована у вигляді термінологічного навчального довідника, складеного на основі термінів та понять, що міститься у вітчизняних та зарубіжних словниках і довідниках, виданих за останні роки, і нової термінології, що зустрічається в монографіях, підручниках, журналах. При визначенні складу термінів та понять, які увійшли до довідника автори притримувалися такого принципу: "при ознайомленні з літературою профільних дисциплін спеціальностей з інформаційної безпеки читачу в більшості випадків достатньо користуватися тільки одним словником".

Гніздове групування термінів і понять дозволило подати достатньо складні і змістовні терміни і поняття, а також основний зміст профільних дисциплін спеціальностей з інформаційної безпеки сукупністю статей, що описують основні та похідні терміни і поняття на основі їхніх структурно-логічних зв'язків.

Найбільш повно представлені терміни і поняття в таких предметних частинах галузі інформаційної безпеки, як загрози інформаційній безпеці, інформаційні війни та інформаційна боротьба, інформаційно-психологічна безпека, безпека інформаційних технологій, криптологія, технічні методи та засоби захисту інформації, правовий та організаційно-технічний захист інформації, захист інформації в комп'ютерних системах та мережах, державна та комерційна таємниця тощо.

Автори цілком усвідомлюють складність тлумачення термінології інформаційної безпеки, котра до того ж продовжує формуватися. Тому терміни та їх тлумачення ні в якому разі не претендують на повноту і закінченість. Автори заздалегідь перепрошують за це перед читачем та мають надію, що дане видання приведе до певного поштовху в напрямку

систематизації поглядів на напрямки подальшого розвитку галузі інформаційної безпеки та вирішення проблем захисту життєво важливих інтересів особистості, суспільства, держави в умовах входження в інформаційне суспільство.

Автори виражають щиру вдячність усім, хто брав участь в обговоренні та підготовці книги до друку. Особлива вдячність Задірацї В.К., Смірнову Ю.О., Бащенку О.А., Булгачу В.Л., Куляниці О.Й., Мухачову В.А., Фалю О.М., Бредельову Б.А., Довидькову О.А., Дручилу В.І., Лавриненко О.С. за цінні зауваження та допомогу під час роботи над книгою.

ЯК КОРИСТУВАТИСЯ ДОВІДНИКОМ

У довіднику прийнята алфавітно-гніздова система групування термінів і понять. Кожне гніздо починається заголовним терміном — заголовком гнізда. Заголовок гнізда являє собою слово (іноді словосполучення) — іменник у називному відмінку (як правило, в однині). Головний термін входить до всіх похідних термінів, що складають гніздо. Похідний термін являє собою переважно словосполучення з двох чи більше слів. Наприклад, у гнізді **“БЕЗПЕКА”** розміщуються похідні терміни **“Безпека даних”**, **“Безпека даних операційна”**, **“Безпека інформаційна”**, **“Безпека інформаційна держави”** і т. ін.

Заголовні терміни гнізд у довіднику упорядковані за алфавітом і набрані великими літерами. Похідні терміни також подані в алфавітному порядку в межах гнізда і набрані малими літерами. Усі терміни виділені напівжирним шрифтом. Порядок розміщення слів у похідних термінах установлений таким, що відображає порядок та логіку їхнього утворення. Заголовний термін в усіх похідних термінах гнізда замінений своєю першою літерою з крапкою і завжди стоїть на першому місці.

Кожний термін у довіднику описується окремою статтею, що містить сам термін, російський та англійський еквіваленти термінів, коротке визначення терміна, пояснення і приклади. Крім того, даються посилання і на етимологію (первісне походження) великого масиву понять (приводяться терміни з латинської, грецької, німецької, французької та інших мов). Формат статті:

український термін /російський термін/ [англійський термін] (етимологія) — визначення терміна.

Окремі терміни або їхнє визначення містять часто вживану абревіатуру, що записується прописними буквами, наприклад, для гнізда **БАЗА**: **Б. даних** (БД) /б. данных (БД)/ [database (DB)].

В окремих термінах наводяться декілька варіантів одного і того ж визначення, відокремлених одне від одного крапкою з комою. Якщо термін має декілька смислових значень, то на кожне значення дається окреме визначення і всі визначення нумеруються наскрізною нумерацією.

Слова (словосполучення), що складають назву статті, в разі повторення в тексті статті, позначені першими літерами цих слів (слів цього словосполучення) із крапками. Наприклад: **модель політики безпеки**

— м. п. б.; **об'єкт доступу** — о. д.

З метою привнесення у визначення терміна (поняття) додаткових відомостей з даного питання даються посилання на інші статті. Тоді заголовні та похідні терміни, що згадуються у словнику, в тексті статті виділяються курсивом.

В окремих термінах указані такі посилання: "те ж, що" і "див." — на синоніми і терміни, близькі до синонімів; "див. також" — на інші терміни з метою розширення відомостей про даний термін. Після вказаних поміток курсивом записується сам термін, на який дається посилання.

Пошук терміна здійснюється шляхом знаходження гнізда і послідовного перегляду термінів гнізда. Для визначення доцільності пошуку терміна в даному довіднику зручно користуватися покажчиком термінів і понять, наведеним у кінці книги.

УКРАЇНСЬКИЙ АЛФАВІТ

Аа *[а]*,	**Бб** *[бе]*,	**Вв** *[ве]*,	**Гг** *[ге]*,	**Дд** *[де]*,	**Ее** *[е]*,	**Єє** *[є]*,
Жж *[же]*,	**Зз** *[зе]*,	**И** *[и]*,	**Іі** *[і]*,	**Її** *[ї]*,	**Йй** *[й]*,	**Кк** *[ка]*,
Лл *[ел]*,	**Мм** *[ем]*,	**Нн** *[ен]*,	**Оо** *[о]*,	**Пп** *[пе]*,	**Рр** *[ер]*,	**Сс** *[ес]*,
Тт *[те]*,	**Уу** *[у]*,	**Фф** *[еф]*,	**Хх** *[ха]*,	**Цц** *[це]*,	**Чч** *[че]*,	**Шш** *[ша]*,
Щщ *[ща]*,	**Ьь** *[знак м'якшення]*,		**Юю** *[ю]*,	**Яя** *[я]*		

ПЕРЕЛІК АБРЕВІАТУР І СКОРОЧЕНЬ

Українська мова

АБД — адміністратор бази даних
АІМ — амплітудно-імпульсна модуляція
АІС — автоматизована інформаційна система
АМ — амплітудна модуляція
АНБ — Агентство національної безпеки
АОМ — аналогова обчислювальна машина
АС — автоматизована система
АСК — автоматизована система керування
АСОД — автоматизована система оброблення даних
АСОІ — автоматизована система оброблення інформації
БД — база даних
БДЗ — база даних і знань
БнД — банк даних
ВВС — взаємодія відкритих систем
ВВЧ — вельмивисока частота
ВГБ — вимоги гарантій безпеки
ВЧ — висока частота
ГВС — гіпервисока частота
ГМД — гнучкий магнітний диск
ДВЧ — дуже висока частота
ДКОІ — двійковий код обміну інформацією
ДНЧ — дуже низька частота
ЕС — експертна система
ЕОМ — електронно-обчислювальна машина
ЕПР — ефективна поверхня розсіювання
ЕЦП — електронний цифровий підпис
ЄІС — єдине інформаційне середовище
ЗІТ — загальні інформаційні технології
ЗКТ — засоби комп'ютерної техніки
ЗМІ — засоби масової інформації
ІНЧ — інфранизька частота
ІОК — інформаційно-обчислювальний комплекс
ІОМ — інформаційно-обчислювальна мережа
ІС — інформаційна система
ІСС — інформаційна система з самонавчанням
ІТТ — інформаційно-комунікаційні технології
КЗА — комплекс засобів автоматизації
КОІ — код обміну інформацією
КПП — контрольно-пропускний пункт

КС — комп'ютерна система
КСЗІ — комплексна система захисту інформації
ЛЛС — лазерна локаційна станція
ЛОМ — локальна обчислювальна мережа
МВВС — модель взаємодії відкритих систем
МОІ — мережа обміну інформацією
МОС — Міжнародна організація із стандартизації
МПД — мережа передавання даних
МСЕ — Міжнародна спілка електрозв'язку
НВЧ — надвисока частота
ННЧ — наднизька частота
НСД — несанкціонований доступ
НЧ — низька частота
ОК — обчислювальний комплекс
ОС — операційна система
ПЕМВН — побічні електромагнітні випромінювання і наведення
ПЕОМ — персональна електронно-обчислювальна машина
ПІМ — періодно-імпульсна модуляція
ПІН — персональний ідентифікаційний номер
ПЗП — постійний запам'ятовуючий пристрій
ППЗП — програмований постійний запам'ятовуючий пристрій
ППЕОМ — персональна професійна електронно-обчислювальна машина
ПРД — правила розмежування доступу
РБД — розподілена база даних
РЕБ — радіоелектронна боротьба
РЕЗ — радіоелектронні засоби
РЕР — радіоелектронна розвідка
РЛС — радіолокаційна станція
РТС — радіотехнічна система
САПР — система автоматизованого проектування
СКЗД — система криптографічного захисту даних
СЗІ — система захисту інформації
СІТ — спеціальні інформаційні технології
СКБД — система керування базами даних
СКРБД — система керування розподіленими базами даних
СЧ — середня частота
ТЗ — технічне завдання
ТЗО — технічні засоби охорони
УВЧ — ультрависока частота
ФВЧ — функціональні вимоги безпеки
ФІМ — фазово-імпульсна модуляція
ФМ — фазова модуляція
ХОА — хибний об'єкт атаки

ЦРУ — Центральне розвідувальне управління
ЧІМ — частотно-імпульсна модуляція
ЧМ — частотна модуляція
ШІМ — широтно-імпульсна модуляція

Російська мова

АБД — администратор базы данных
АВМ — аналоговая вычислительная машина
АИМ — амплитудно-импульсная модуляция
АИС — автоматизированная информационная система
АМ — амплитудная модуляция
АНБ — Агентство национальной безопасности
АС — автоматизированная система
АСОД — автоматизированная система обработки данных
АСОИ — автоматизированная система обработки информации
АСУ — автоматизированная система управления
БД — база данных
БДЗ — база данных и знаний
БнД — банк данных
ВК — вычислительный комплекс
ВЧ — высокая частота
ГВС — гипервысокая частота
ГМД — гибкий магнитный диск
ДКОИ — двоичный код обмена информацией
ЕИС — единая информационная среда
ИВК — информационно-вычислительный комплекс
ИВС — информационно-вычислительная сеть
ИНЧ — инфранизкая частота
ИС — информационная система
ИСС — информационная система с самообучением
ИТТ — информационно-коммуникационные технологии
КВЧ — крайне высокая частота
КОИ — код обмена информацией
КПП — контрольно-пропускной пункт
КС — компьютерная система
КСА — комплекс средств автоматизации
КСЗИ — комплексная система защиты информации
ЛВС — локальная вычислительная сеть

ЛЛС — лазерная локационная станция
ЛОА — ложный объект атаки
МВОС — модель взаимодействия открытых систем
МОС — Международная организация по стандартизации
МСЭ — Международный союз электросвязи
НСД — несанкционированный доступ
НЧ — низкая частота
ОВЧ — очень высокая частота
ОИТ — общие информационные технологии
ОНЧ — очень низкая частота
ОС — операционная система
ПЗУ — постоянное запоминающее устройство
ПИМ — периодно-импульсная модуляция
ПИН — персональный идентификационный номер
ППЗУ — программируемое постоянное запоминающее устройство
ППЭВМ — персональная профессиональная электронно-вычислительная машина
ПРД — правила разграничения доступа
ПЭМИН — побочные электромагнитные излучения и наводки
ПЭВМ — персональная электронно-вычислительная машина
РБД — распределенная база данных
РЭБ — радиоэлектронная борьба
РЭС — радиоэлектронные средства
РЭР — радиоэлектронная разведка
РЛС — радиолокационная станция
РТС — радиотехническая система
САПР — система автоматизированного проектирования
СВЧ — сверхвысокая частота
СЗИ — система защиты информации
СКЗД — система криптографической защиты информации
СИТ — специальные информационные технологии
СКТ — средства компьютерной техники
СМИ — средства массовой информации
СНЧ — сверхнизкая частота
СОИ — сеть обмена информацией
СПД — сеть передачи данных
СНЧ — сверхнизкая частота
СУБД — система управления базами данных
СУРБД — система управления распределенными базами данных
СЧ — средняя частота
ТГБ — требования гарантий безопасности

ТЗ — техническое задание
ТСО — технические средства охраны
УВЧ — ультравысокая частота
ФАПСИ — Федеральное агентство правительственной связи и информации
ФИМ — фазово-импульсная модуляция
ФТБ — функциональные требования безопасности
ЦРУ — Центральное разведывательное управление
ЧИМ — частотно-импульсная модуляция
ШИМ — широтно-импульсная модуляция
ЭВМ — электронно-вычислительная машина
ЭПР — эффективная поверхность рассеивания
ЭС — экспертная система
ЭЦП — электронная цифровая подпись

Англійська мова

ACOUSINT — ACOUStic INTelligence
AES — Advances Encryption Standard
AM — Amplitude Modulation
ANSI — American National Standards Institute
ARP — Address Resolution Protocol
ASCII — American Standard Code for Information Interchange
BGP — Border Gateway Protocol
CCITSE — Common Criteria for Information Technology Security Evaluation
CEMITS — Common Evaluation Methodology for Information Technology Security
CIA — Central Intelligence Agency
COMINT — COMmunications INTelligence
CRL — Certificate Revocation List
CTCPEC — Canadian Trusted Computer Product Evaluation Criteria
DB — DataBase
DBMS — DataBase Management System
DEA — Data Encryption Algorithm
DES — Data Encryption Standard
DLP — Discrete Logarithm Problem
DMZ — DeMilitarized Zone
DNS — Domain Name Service (System)
DVD — Digital Video Disk
EAL — Evaluation Assurance Level
EBCDIC — Extended Binary-Coded Decimal Interchange Code

EGP — Exterior Gateway Protocol
EHF — Extremely High Frequency
ELF — Extremely Low Frequency
ELINT — ELectronic INTelligence
FCITS — Federal Criteria for Information Technology Security
FEAL — Fast data Encipherment ALgorithm
FIPS — Federal Information Protection Standard
FM — Frequency Modulation
FTP — File Transfer Protocol
HF — High Frequency
HTML — HyperText Markup Language
HTTP — Hypertext Transfer Protocol
HUMINT — HUman INTelligence
IAB — Internet Architecture Board
IANA — Internet Assigned Numbers Authority
ICMP — Internet Control Message Protocol
IDEA — International Data Encryption Algorithm
IEC — International Electrotechnical Commission
IESG — Internet Engineering Steering Group
IETF — Internet Engineering Task Force
IGRP — Interior Gateway Routing Protocol
ILM — Infra Low Frequence
IMAP — Internet Message Access Protocol
InterNIC — Internet Network Information Center
IP — Internet Protocol
IPSec — Internet Protocol Security
IRSG — Internet Research Steering Group
IS — Information System
ISO — International Organization for Standardization
ISOC — Internet SOCiety
IRTF — Internet Research Task Force
IT — Information Technology
ITU — International Telecommunication Union
ITU-T — International Telecommunication Union Telecommunication standardization sector
ITSEC — Information Technology Security Evaluation Criteria
LAN — Local Area Network
LF — Low Frequency
KDC — Key Distribute Center
KTC — Key Translation Center
MASINT — Measurement And Signature INTelligence
MF — Medium Frequency
MTA — Mail Transfer Agent
NIST — National Institute of Standard and Technology
NSA — National Security Agency
NTP — Network Time Protocol

NUCINT — NUClear INTelligence
OS — Operating System
OSPF — Open Shortest Path First
PIN — Personal Identification Number
PGP — Pretty Good Privacy
PKI — Public Key Infrastructure
PM — Phase Modulation
POP — Post Office Protocol
PP — Protection Profile
PPC — Personal Professionoriented Computer
PVN — Private Virtual Network
RIP — Routing Information Protocol
PROM — Programmable Read-Only Memory
RADINT — RADar INTelligence
ROM — Read-Only Memory
RPV — Remotely Piloted Vehicle
SANTA — Security Analysis Network Tool for Administrator
SHF — Super High Frequency
SIGINT — SIGnal INTelligence
SKIP — Simple Key management for Internet Protocol
SMTP — Simple Mail Transfer Protocol
SSL — Secure Sockets Layer (Protocol)
ST — Security Target
THF — Tremendously High Frequency
TCP — Transmissin Control Protocol
TCSC – Trusted Computer System Criteria
TOE — Target Of Evaluation
TSF — TOE Security Policy
TTP — Trusted Third Party
UDP — User Datagram Protocol
UHF — Ultra High Frequency
URL — Uniform Resource Locator
VHF — Very High Frequency
VLF — Very Low Frequency
WWW — World Wide Web

Скорочення

ам. — американізм (англійська мова в США)
англ. — англійська мова
араб. — арабська мова
букв. — буквально
голл. — голландська мова
грец. — давньогрецька мова

дат. — датська мова
ісп. — іспанська мова
італ. — італійська мова
лат. — латинська мова
нім. — німецька мова
польс. — польська мова
сканд. — скандинавські мови
франц. — французька мова
чеськ. — чеська мова

А

АБЕТКА /алфавит/ [alphabet] (від грец. $\grave{\alpha}\lambda\varphi\acute{\alpha}\beta\eta\tau\text{ø}\varsigma$, від назви перших літер алфавіту — альфа та вета, або віта) — 1) Сукупність всіх літер, розміщених у певному, встановленому в даній мові порядку. 2) Довільна скінченна множина. Елементи цієї множини називають символами або буквами алфавіту. Словами в алфавіті є скінченна послідовність букв цього алфавіту. Довжина слова — кількість букв у ньому.

АБОНЕНТ /абонент/ [subscriber, user node, communicant] (нім. Abonnent, від франц. abonne) — орган керування, особа або технічний засіб, що може використовувати зв'язок протягом певного терміну для обміну повідомленнями.

АБРЕВІАТУРА /аббревиатура/ [abbreviation] (італ. abbreviatura, від лат. abbrevio — скорочую) — складноскорочене слово, утворене з початкових складів або з перших літер словосполучення.

АВТЕНТИФІКАЦІЯ /аутентификация/ [authentication] (від грец. $\alpha\grave{\upsilon}\vartheta\varepsilon\nu\tau\iota\kappa\acute{\text{ó}}\varsigma$ справжній і лат. ...ficatio, від facio — роблю) — 1) Перевірка належності суб'єктові доступу пред'явленого ним ідентифікатора; процес установлення достовірності ідентифікаційної інформації. 2) Процедура перевірки відповідності пред'явленого ідентифікатора об'єкта комп'ютерної системи на предмет належності його цьому об'єктові; установлення або підтвердження автентичності (див. автентичний).

А. багатофакторна /а. многофакторная/ [multifactor a.] — автентифікація, яка здійснюється за допомогою захищених механізмів двох або більше типів. Наприклад, застосування для автентифікації паролем разом із токеном або автентифікації біометричної разом із паролем.

А. біометрична /а. биометрическая/ [biometrical a.] — методи автентифікації, які засновані на використанні унікальних біологічних характеристик об'єкту. В якості таких характеристик можуть бути вико-

ристані: відбиток пальця, геометрія обличчя, геометрія руки, сітчатка ока і т.ін.

А. взаємна /а. взаимная/ [peer-to-peer a.] — взаємне підтвердження ідентифікаторів сутностей.

А. джерела даних /а. источника данных/ [data origin a.] — функція захисту, в результаті виконання якої з певними гарантіями встановлюється належність даних (повідомлень) джерелу даних повідомлень.

А. користувача /а. пользователя/ [user a.] — перевірка відповідності користувача ідентифікаторові, що пред'являється ним.

А. однофакторна /а. однофакторная/ [single-factor a.] — на відміну від автентифікації багатофакторної, автентифікація, яка здійснюється за допомогою захищеного механізму одного типу, наприклад тільки за допомогою пароля або тільки автентифікації біометричної.

А. повідомлень /а. сообщений/ [message a.] — перевірка, що повідомлення були передані не пошкодженими, не модифікованими та надіслані від достовірного джерела саме тому абонентові, якому вони призначалися. А. п. може здійснюватися за допомогою додавання до блоку даних контрольного поля для виявлення будь-якої зміни в даних. При обчисленні значень цього поля використовується ключ, відомий тільки приймачеві даних.

А. проста /а. простая/ [simple a.] — автентифікація, що передбачає надання інформації секретної (особистої) стороні, що перевіряє.

А. сильна /а. сильная/ [strong a.] — автентифікація без надання інформації секретної (особистої) стороні, що перевіряє.

А. суб'єкта /а. субъекта/ [subject a.] — функція захисту, в результаті виконання якої з певними гарантіями виконується підтвердження суб'єкта заявленим про себе характеристикам (наприклад, ідентифі-

каторові).

А. суттєвості /а. сущности/ [entity a.] — функція захисту, в результаті виконання якої з певними гарантіями виконується перевірка відповідності суттєвості заявленим про себе характеристикам (наприклад, ідентифікаторові).

АВТЕНТИЧНИЙ /аутентичный/ [authentic] (від грец. *αὐθεντικός* — справжній) — дійсний, вірний, той, що ґрунтується на першоджерелі.

АВТО... /авто.../ [auto...] (від грец. *αὐτός* — сам) — у складних словах відповідає поняттю "само".

АВТОМАТИЗАЦІЯ /автоматизация/ [automation] — упровадження автоматичних засобів для реалізації процесів; система заходів, спрямованих на підвищення продуктивності праці людини через заміну частини цієї праці роботою машин. Базується на використанні сучасних засобів обчислювальної техніки і наукових методів та реалізується за допомогою різноманітних систем автоматичних і автоматизованих.

А. процесу оброблення конфіденційної інформації /а. процесса обработки конфиденциальной информации/ — забезпечення адекватної реалізації у системі комп'ютерній схеми потоків інформаційних і правил керування ними, які існували до застосування комп'ютерних засобів оброблення інформації. Здійснюється послідовним виконанням наступних дій: визначення формального механізму, що адекватно визначає задану схему інформаційних потоків і правила керування ними; побудова моделі безпеки, що відображає заданий порядок оброблення інформації, і, можливо, формальний доказ її безпеки; реалізація системи оброблення інформації у відповідності з моделлю, що пропонується; доказ гарантій можливих в автоматизованій системі потоків інформації і правил розмежування доступу вихідній схемі інформаційних потоків і правил керування ними.

АВТОРИЗАЦІЯ /авторизация/ [authorization] (франц. autorisation, букв. — дозвіл) — 1) Надання сутності офіційної санкції робити щось або бути чимось. 2) Надання повноважень; установлення відповідності

між повідомленням (пасивним об'єктом) і його джерелом (користувачем або процесом, що його створили). 3) Гарантоване надання привілею доступу програмам, користувачам або процесам, засноване на правах доступу.

А. програми /а. программы/ [program a.] — установлення обмежень на доступ до системної програми або програми користувача з боку інших програм і користувачів.

АВТОРИТАРИЗМ /авторитаризм/ [authoritarianism] (франц. autoritarisme, від лат. autoritas — вплив, влада) — 1) Антидемократична система політичного володарювання. Характеризується повною відсутністю або абсолютною фіктивністю демократичних інституцій, зосередженням у руках однієї особи або невеликої групи осіб необмеженої влади, що спирається на військово-каральний апарат репресій і терору, на відверту соціальну й націоналістичну демагогію. 2) Політика жорсткого контролю державних органів влади над засобами масової інформації.

АГЕНТ /агент/ [agent] (від лат. agens (agentis) — діючий) — 1) Особа, що діє за чиїмось дорученням, уповноважений. У міжнародному праві й дипломатичній практиці — агент дипломатичний та агент консульський. 2) Особа, що діє за завданнями служби розвідувальної, не будучи при цьому штатним співробітником цієї служби. А. доручають добування (або допомогу в добуванні) розвідувальної або контррозвідувальної інформації. Його також можуть використовувати в різноманітних операціях розвідувальних.

А. впливу /а. влияния/ — 1) Особа, що використовується для здійснення таємного впливу на державних чиновників, засоби масової інформації або активну частину населення і для досягнення цілей, до яких прагне іноземна держава. 2) Суспільний діяч, що проводить політику на користь будь-якої партії, організації або іноземної держави в середовищі, що не належить до цих структур.

А. дипломатичний /а. дипломатический/ — збірне найменування дипломатичних представників і

членів дипломатичного персоналу посольств, місій.

А. законсервований (“сплячий”) /а. законсервированный (“спящий”)/ — шпигун, який знаходиться в зоні оперативної діяльності, але якого до пори до часу не залучають до участі в розвідувальній роботі.

А. залучений /а. привлеченный/ — громадянин країни, розвідувальні органи якої залучають його до співробітництва.

А. консульський /а. консульский/ — один з консульських рангів у ряді країн. У практиці деяких держав — службова особа консульської установи.

А. користувача /а. пользователя/ — див. пошта електронна.

А. пересилки пошти /а. пересылки почты/ [Mail Transfer A. (MTA)] — програмний модуль для передавання повідомлень між пристроями мережі. Див. також пошта електронна.

А. під прикриттям /а. под прикрытием/ — див. таємний агент.

А. подвійний /а. двойной/ — 1) Агент, що використовується в оперативних цілях одночасно двома або більше розвідувальними службами і постачає одну з них інформацією про інші або інформацію кожній про інші служби. А. п. можна стати як спеціально, так і мимоволі. 2) Перевербований противником агент, що працює на обидві розвідки. 3) Завербований противником співробітник розвідки (або контррозвідки).

А. подвійний перевербований / а. двойной перевербованный/ — подвійний агент, чия нещирість викрита спеціальною службою, проти якої він працює і якого ця служба використовує (добровільно або примусово) для ведення гри оперативної проти його колишніх господарів.

А. потенційний /а. потенциальный/ — особа, що знаходиться в процесі розробки і розглядається розвідувальною службою як кандидат на роль агента.

А. потрійний /а. тройной/ — агент, що завербований трьома розвідувальними службами, але який

фактично виступає в ролі агента подвійного, використовуючи інформацію від двох спеціальних служб на користь третьої.

А. прихований /а. скрытый/ — особа, що пропонує свої послуги іншій державі, і залишається при цьому на колишньому місці роботи в своїй країні, щоб мати можливість передавати "свіжі" відомості. Різновид агента-"крота".

А. розкритий (провалений) /а. раскрытый (проваленный)/ — агент, про шпигунську діяльність якого відомо протилежній стороні.

А. таємний /а. тайный/ [counterspy, intelligencer] — особа, що діє таємно і займається шпіонажем або підривними діями в інтересах іноземної розвідувальної служби або держави. Також називається агентом під прикриттям.

А. удаваний /мнимый а./ — вигаданий, неіснуючий таємний агент, що використовується при дезінформуванні (наприклад, на нього можуть посилатися як на джерело розвідувальний даних).

А., завербований під "чужим прапором" /а., завербованный под "чужым флагом"/ — особа, яка передає секретну інформацію, не знаючи про те, що її кінцевий одержувач є співробітником розвідки, або не здогадується про національну належність цієї розвідки.

А.-"кріт" /а.-"крот"/ — упроваджений агентрозвідки, що займає порівняно високий пост у ворожих державних структурах або збройних силах, здатний передавати звідти виключно цінні відомості.

А.-"кріт" удаваний /а.-"крот" мнимый/ — вигаданий, неіснуючий агент-"кріт", чутка про якого розповсюджується розвідувальною службою з тим, щоб увести в оману противника.

А.-груповод /а.-групповод/ — агент, який відповідає перед службою розвідувальною за діяльність

решти агентів, тобто виконує роль куратора.

А.-дезінформатор /а.-дезинформатор/ — агентрозвідки, перед яким стоять завдання з уведення в оману розвідувальних і контррозвідувальних служб іноземної держави. А.-д. не займається збиранням інформації.

А.-інформатор /а.-осведомитель/ — малозначний агент, що живе або працює поблизу об'єкта розвідки і передає цінну інформацію тоді, коли йому трапляється така можливість.

А.-нелегал /а.-нелегал/ — агент, який діє під проводом нелегального резидента і сам працює під чужими документами.

А.-провокатор /а.-провокатор/ (від лат. provocator — той, що кидає виклик) — агент, що підбурює окремих осіб або цілі групи (які вже знаходяться під підозрою) на здійснення протиправних актів з метою дискредитації влади.

АГЕНТСТВО /агентство/ [agency, agents] — 1) Організація, що виконує певні доручення державних і інших установ або приватних осіб. 2) Установа, що збирає та подає інформацію в пресу, на радіо, телебачення. 3) Представництво, відділення центральної установи.

А. інформаційне /а. информационное/ [information a.] — див. агентство новин.

А. національної безпеки (АНБ) /А. национальной безопасности (АНБ)/ [National Security A. (NSA)] — основна служба розвідувальна Сполучених Штатів Америки в галузі розвідки радіоелектронної. АНБ створене в 1952 році в складі міністерства оборони. До його складу входить Центральна служба безпеки (ЦСБ), яка відповідає в США за криптографію й криптоаналіз. Перед ЦСБ стоять два завдання: дешифрування іноземних шифрів і забезпечення безпеки американських телекомунікаційних систем. До ведення ЦСБ віднесені як повідомлення з Білого дому, так і тактичні військові канали зв'язку. Директор АНБ також очолює ЦСБ і контролює всі підрозділи радіоелектронної розвідки воєнних розвідувальних органів.

Хоча АНБ і ЦСБ організаційно входять до складу міністерства оборони, при цьому обидві організації є повноправними членами товариства розвідувального і таким чином підпорядковуються ще директорові центральної розвідки.

А. новин /а. новостей/ [news a.] — організація, що займається збиранням, обробленням і розповсюдженням інформації для газет, журналів, видавництв, радіо і телебачення, державних, науково-культурних та інших закладів. Інша назва — агентство інформаційне. Великі агентства мають власні кореспондентські пункти й передплатників в різних країнах світу, користуються для їхнього обслуговування найновішою електронно-інформаційною технікою й ефективно діючими системами комерційних служб. В США до числа таких агентств відносяться Ассошіейтед Пресс (Associated Press — AP), кооперативне за своєю структурою (засноване у Нью-Йорку в 1848 р.) і приватне за своїм статусом (засноване у 1907 р.) агентство Юнайдет Пресс Інтернейшнл — ЮПІ (Uneted Press International - UPI) із штаб квартирою у Нью-Йорку, Нашвіллі і Далласі. За масштабами своєї діяльності вони є світовими. У Великобританії такими ж великим а. н. є Рейтер (Reuters), у Франції — Агентство Франс Пресс — АФП (Agence France Presse — AFP), у Німеччині — Дойче Прессе-Агентур — ДПА (Deutche Presse-Agentur — DPA), в Італії — Адженція Національе Стампа Ассочата — АНСА (Agenzia Nazionale Stampa Associata) — ANSA).

А. урядового зв'язку та інформації Федеральне /а. правительственной связи и информации Федеральное (ФАПСИ)/ — державний орган уряду Російської Федерації для забезпечення урядового зв'язку, захисту інформації криптографічного і інженерно-технічного в системах засекреченого зв'язку РФ і її установах за кордоном та розвідки радіоелектронної каналів зв'язку ймовірного противника. Серед інших завдань агентства — ліцензування та сертифікація систем зв'язку незалежно від форм власності.

АГЕНТУРА /агентура/ [agents, intelligence network] (нім. Agentur) — 1) Сукупність агентів будь-якої установи, підприємства або організації. 2) Мережа агентів, що створюється для збирання секретних відомостей, проведення підривної роботи.

АГРЕСІЯ /агрессия/ [aggression] (від лат. aggressio - нападение) — 1) Мотивована деструктивна поведінка, що суперечить нормам та правилам співіснування людей у суспільстві, наносить шкоду об'єктам нападу. 2) Міжнародно-правове поняття, що характеризує незаконне застосування збройної сили однієї держави (групи держав) проти іншої держави (групи держав) для її захоплення, поневолення або примусу до прийняття своїх умов шляхом порушення її суверенітету, територіальної цілісності, політичної та економічної незалежності.

А. інформаційно-психологічна /а. информационно-психологическая/ — дії, спрямовані на нанесення противнику конкретного, відчутного впливу в окремих галузях його діяльності. Ознаками а. і.-п. можуть бути: обмежене та локальне за своїми масштабами застосування сили; виключення із засобів інформаційно-психологічного впливу найбільш небезпечних видів інформаційної зброї, які не дозволяють контролювати розміри нанесених збитків; обмеження розмірів простору, об'єктів інформаційної інфраструктури і соціальних груп, що піддаються ураженню інформаційно-психологічним впливом (агресія торкається не всього інформаційно-психологічного простору держави-жертви, а тільки її частини), обмеження за цілями (переслідує локальні, часткові цілі) і часу (як правило, агресія завершується після повного досягнення агресором усіх поставлених цілей і рідко приймає затяжний характер), а також по залученим силам та засобам.

АДМІНІСТРАТОР /администратор/ [administrator, manager] (від лат. administrator — розпорядник) — 1) Адміністративно-посадова особа, керівник, розпорядник, організатор. 2) Користувач, роль якого включає функції керування системою комп'ютерною і (або) комплексом засобів захисту.

А. бази даних (АБД) /а. базы данных (АБД)/ [database a.]— спеціальна посадова особа (група осіб), що володіє службовою інформацією про базу даних(але не обов'язково має доступ до інформації, що зберігається в базі даних) і відповідає за її ведення, використання та розвиток. Функції а. б. д. зводяться до підтримки цілісності бази даних, необхідного рівня захисту даних та її ефективності. А. б. д. входить до

складу адміністрації банку даних.

А. безпеки /а. безопасности/ [security a.] — 1) Особа або група осіб, відповідальних за забезпечення безпеки системи, за реалізацію й безперервність дотримання адміністративних заходів захисту і здійснюючих постійну організаційну підтримку функціонування фізичних і технічних засобів захисту, що застосовуються. 2) Адміністратор, відповідальний за дотримання політики безпеки.

А. даних /а. данных/ [data a.] — особа, що має повну уяву про дані, які використовуються в установі (на підприємстві), і відповідає за зберігання, оновлення та організацію їхнього використання.

А. доступу /а. доступа/ [access a.] — одна з посадових осіб в складі адміністрації банку даних, що відповідає за організацію доступу користувачів до баз даних.

А. доступу груповий /а. доступа групповой/ [protection group a.] — особа, права якої в рівній мірі належать декільком користувачам.

А. завдань /а. задач/ [task a.] — спеціальна посадова особа, яка входить до складу адміністрації банку даних і виконує підготовку запитів на формування звітів складної форми і змісту. Засобами а. з. є діалогова (інтерактивна) мова і генератор звітів.

А. захисту /а. защиты/ [security a.] — суб'єкт доступу, який є відповідальним за захист від несанкціонованого доступу системи інформаційної.

А. системи (системний А.) /а. системы (системный а.)/ [system a.] — особа, що відповідає за експлуатацію системи та підтримку її в працездатному стані (див. також адміністратор бази даних).

АДМІНІСТРАЦІЯ /администрация/ [administration] (від лат. administratio — керування, управління) — 1) Розпорядчі органи державного управління; органи виконавчої влади. 2) Керівний персонал установи,

підприємства, організації.

А. банку даних /а. банка данных/ [databank a.] — група осіб (підрозділ), що відповідає за експлуатацію банку даних: ведення баз даних, організацію колективного доступу до них користувачів та розвиток системи.

АДМІНІСТРУВАННЯ /администрирование/ [administration] (від лат. administro — керую) — 1) Керування, завідування. 2) Формально-бюрократичний метод керування, шляхом команд, наказів та розпоряджень.

А. даних /а. данных/ [data a.] — функції, які включають оброблення загальних визначень даних, керівництво технічним проектуванням баз даних і т. ін., які покладені на певних осіб — адміністраторів даних.

АДРЕСА /адрес/ [address] — 1) Позначення місця проживання чи перебування кого-небудь або місцезнаходження чого-небудь. 2) Місце в пам'яті конкретного комп'ютера; числовий ідентифікатор або символічне ім'я, яке однозначно визначає положення конкретного комп'ютера або пристрою в мережі, а також служить для визначення мережі, підмережі та вузла всередині мережі.

А. IP (IP-А.) /а. IP (IP-а.)/ [IP a.] — унікальна фізична адреса комп'ютера, приєднаного до Інтернету. Складається з чотирьох десяткових чисел, розділених точкою, кожне в діапазоні від 0 до 255 (чотири байти). Наприклад: 193.126.7.29

А. доменна /а. доменный/ — більш практичний аналог адреси IP. А. д. виникла в Інтернеті для зручності користувачів: набагато легше запам'ятати а. д. (наприклад, www.microsoft.com або www.sony.com), ніж чотири числа IP-адреси. А. д. може містити латинські літери, цифри, крапки і деякі інші спеціальні знаки.

А. конспіративна /а. конспиративный/ [secret a.](від лат. conspiratus — таємний) — таємна адреса,

за якою приходить пошта (вид зв'язку може бути яким-небудь іншим) і чекає свого одержувача. Лист (посилка) адресується особі, що проживає за даною адресою, але одержувачем його є співробітник або агент розвідки. А. к. можуть ще називати "поштовим тайником" або "живою" поштовою скринькою.

А. поштова /а. почтовый/ — ідентифікатор поштової скриньки користувача. Утворюється з імені користувача і доменного імені поштового сервера розділених символом @. Приклади: adm@kgtu. kuban. ru, ryabov@kubstu. ru, sribny@chat. ru, ugfile@mailcity. com. Для одержання а. п. необхідно зареєструватися на поштовому сервері (на безкоштовних серверах реєстрація виконується через WWW, у інтрамережах її виконує адміністратор поштового сервера).

АЕРО... /аэро.../ [aerial/air...] (від грец. *ἀήρ* — повітря) — у складних словах відповідає поняттям "авіаційний", "повітряний".

АЕРОЗНІМОК /аэроснимок/ [aerial view] (від аеро..., і знімок) — аерозображення, представлене на твердій основі.

АЕРОЗОБРАЖЕННЯ /аэроизображение/ [aerial image] (від аеро... і зображення) — зображення місцевості, одержане з літака або іншого апарата літального. Може подаватися у зафіксованому вигляді на твердій основі виду (аерознімок) або на екрані відеоконтрольного пристрою.

АЕРОЗОЛІ /аэрозоли/ [aerosol] (від грец. *ἀήρ* — повітря і нім. Sol — колоїдний розчин, від лат. solitio — розкладання) — речовини у вигляді дисперсії твердих часток і капель рідини, які знаходяться у завислому стані в повітрі. Бувають природними і штучними. До а. відносяться дими, тумани, пил, смог. Використовуються для енергетичного приховування об'єктів в діапазоні оптичному.

А. природні /а. естественные/ [natural a.] — аерозолі, що створюються пилом і частками води. Вплив природних аерозольних утворень проявляється як в розсіюванні, так і поглинанні світла частками аерозолю. Коефіцієнт послаблення (поглинання) у видимій частині спектра змінюється в 1,5–2 рази. Із збільшенням

довжини хвилі втрати зменшуються. Втрати енергії хвилі при $\lambda = 0{,}55$ мкм приблизно в 10 разів більші втрат для $\lambda = 1{,}06$ мкм. Аерозольне розсіювання світла залежить від коефіцієнтів його послаблення окремими частками, їхньої концентрації і розмірів. Воно визначає прозорість й метеорологічну дальність видимості. Використання а. п. як засобів захисту від спостереження утруднено із-за випадкового характеру їхніх проявів у вигляді утворень, що призводять до малої метеорологічної дальності. Проте а. п. у вигляді хмар складають серйозні проблеми для розвідки наземних і надводних об'єктів за допомогою засобів космічної розвідки.

А. штучні /а. искусственные/ [artificial a.] — аерозолі у вигляді димових завіс і хмар, що створюються за допомогою димових шашок, спеціальних боєприпасів (снарядів, бомб), аерозольних генераторів і димових машин. А. ш. забезпечують (при врахуванні напрямку і сили вітру) ефективне, але короткочасне приховування енергетичне об'єктів в оптичному діапазоні. Проміжок часу і площа приховування залежать від багатьох факторів (в тому числі від об'єму хмари диму, напрямку і швидкості вітру) і коливається від хвилин до 1–2-х годин. Найбільш ефективні завіси створюються при швидкості вітру 3–5 м/с. Хімічними речовинами для створення диму служать епоксидні, фенольні, поліетиленові, силікатні, уретанові смоли та інші високомолекулярні сполуки. Дими з таких речовин одержують розпилюванням часток речовини у потоці гарячих газів або іншими способами. В залежності від складу компонент частки, що створюють аерозольну хмару, можуть мати діаметр від 1 до 100 мкм. 400 г димоутворювальної речовини може утворити аерозольну хмару на площі 600 м^2, яка забезпечить послаблення випромінювання в інфрачервоному діапазоні приблизно у 80 раз.

АЕРОФОТОАПАРАТ /аэрофотоаппарат/ [aerial camera] (від аеро..., фото... і апарат) — пристрій, призначений для одержання аерозображень (аерофотографування).

АЕРОФОТОГРАММЕТРІЯ /аэрофотограмметрия/ [airophotogrammetry] — розділ фотограмметрії, що вивчає способи визначення форми, розміри і положення об'єктів за їхніми зображеннями на аеро-

фотознімках. Основні положення а. основані на законах перспективи (центральної проекції). Для фотограмметричних робіт використовуються спеціальні прилади: фототрансформатори, діапроектори, стерео- і монокомпаратори, стереопроектори, стереографи і т. ін.

АЕРОФОТОЗНІМОК /аэрофотоснимок/ [aerial photo, airphoto] (від аеро..., фото... і знімок) — аерознімок, одержаний аерофотоапаратом.

АЕРОФОТОГРАФУВАННЯ /аэрофотографирование/ [aerial photography] (від аеро... і фотографування) — фотографування земної поверхні з використанням аерофотоапарата і аерофотоматеріалу, розташованих на апараті літальному.

АЕРОФОТОЗЙОМКА /аэрофотосъемка/ [air photography] (від аеро..., фото... і зйомка) — див. аерофотографування.

АЕРОФОТОМАТЕРІАЛ /аерофотоматериал/ [aerial photographic m.] (від аеро..., фото... і матеріал)— матеріал світлочутливий, призначений для реєстрації аерозображення.

АЕРОФОТОРОЗВІДКА /аэрофоторазведка/ [air photographic reconnaissance] — добування відомостей про противника, місцевість (акваторію) за допомогою технічних засобів фотографування, встановлених на пілотованих та апаратах літальних безпілотних; спосіб розвідки повітряної.

АКРЕДИТАЦІЯ /аккредитация/ [accreditation] — в галузі безпеки інформації — процедура надання формальної заяви або власне формальна заява як така, за якою офіційно уповноважений орган сертифікації повідомляє, що система оброблення даних, мережа, система автоматизована може застосовуватися для оброблення інформації критичної при використанні даної політики безпеки з даними службами та механізмами інформаційної безпеки. Взагалі термін а. відноситься до процедури або самого факту визнання правочинності особи чи органу виконувати конкретні роботи.

АКТ /акт/ [act] (лат. actus від ago — приводжу в рух) — 1) Вчинок, дія. 2) Рішення державних органів утілене в форму закону, указу, постанови і т.ін. державного, суспільного значення. Розрізняють акти законодавчі, парламентські, конституційні, неконституційні, нормативні, підзаконні, правові, міжнародні, а також акти капітуляції, акти доброї волі і т. ін.

А. нормативний /а. нормативный/ [normative a.] — акт компетентного державного органу влади (державної служби), офіційний письмовий документ, яким встановлюються, змінюються або скасовуються норми права. Н. а. класифікуються за їхньою юридичною силою, що визначається компетенцією і положенням органу, що їх видав, в загальній системі правотворчих органів держави, а також характером самих актів. Розрізняють основний закон (конституцію) і інші закони, що приймаються вищим органом державної влади, а також акти підзаконні.

А. підзаконний /а. подзаконный/ [subordinate a.] — правовий акт державного органа влади, виданий в межах його компетенції у відповідності з законом або на основі його і для виконання його. Принцип верховенства законів і підзаконності усіх інших правових актів установлюється конституцією.

АКТИВАЦІЯ /активация/ [activation] (від лат. activus — діяльний) — в психології — стан збудження, підвищення емоційності, переходу від спокою до дії. У комунікативістиці вивчається а. аудиторії, що залежить від тих чи інших типів інформації, форм і засобів її передавання, а також і від складу аудиторії у соціально-демографічному, культурно-освітньому, професіональному, віковому і психологічному відношенні.

АЛГЕБРА /алгебра/ (від араб. аль-джабр, аль-габр) — розділ математики, в якому вивчаються дії над величинами незалежно від їхніх числових значень. Основний зміст а. — методи розв'язування алгебраїчних рівнянь.

АКЦІЯ /акция/ [action] (від лат. actio — дія, дозвіл) — дія, вчинена з будь-якою політичною, економічною

або іншою метою.

А. інформаційна /а. информационная/ [information a.] — дія інформаційна, що виходить за межі боротьби інформаційної в область інформаційного протиборства геополітичних суб'єктів.

А. інформаційна наступальна /наступательная информационная а./ — дія інформаційна наступальна, що здійснюється в межах протиборства інформаційного (наприклад, маніпулювання засобами масової інформації, культури, мистецтва і т. ін.).

АЛГОРИТМ /алгоритм/ [algorithm] (лат. algorithmus) — 1) Система точно визначених правил дії (програма) з зазначенням, як і в якій послідовності ці правила застосувати до первинних даних певної задачі, щоб одержати її розв'язок. Назва походить від імені середньовічного узбецького математика Мухамеда-ібн-Суса (арабізоване аль-Хорезмі). 2) Точний припис, який визначає процес обчислювальний, що йде від варійованих початкових даних до шуканого результату. Одним із способів задавання а. є логічна схема (блок-схема). Програма являє собою опис а. на мові програмування. 3) Точно визначене правило дій (програма), для якого задана вказівка як і в якій послідовності це правило потрібно застосовувати до вхідних даних задачі для того, щоб отримати її рішення. Це поняття не є точним математичним визначенням, а лише визначає суть слова а. Існують декілька точних математичних формалізацій поняття а., серед яких загальнорекурсивні та частково-рекурсивні функції, машини Тьюрінга, нормальні а. Маркова, а. Колмогорова і т.ін. Відомо, що всі формальні визначення а. еквівалентні між собою. При визначенні а. вважаються зафіксованими вхідний A та вихідний B алфавіти. А. отримує на вхід слово w з множини всіх слів вхідного алфавіту A^* і як результат виконання послідовності елементарних операцій (або кроків роботи), подає на вихід слово $f(w)$ з множини всіх слів вихідного алфавіту B^*. А. розв'язує масову задачу, якщо при отриманні на вході будь-якої індивідуальної задачі $w \in A^*$ він за скінченну кількість кроків подає на вихід її розв'язок. Довжиною вхідного слова $|w|$ є кількість букв у слові w. А. розв'язує задачу за час t, якщо на

кожному вході w він робить не більше, ніж t кроків. Звичайно, t залежить від $|w|$.

А. експоненціальний /а. экспоненциальный/ [exponentiation a.] — алгоритм, який на нескінченній послідовності входів робить більше як 2^{n^c} кроків, де n — довжина входу, а $c > 0$ — деяка константа. Е. а. в теорії складності відповідають повільним, неефективним на практиці алгоритмам.

А.імовірнісний /а. вероятностный/ [probabilistic a.] — алгоритм, який крім входу $w(n)$ отримує випадкову двійкову послідовність $r \in 0, 1^{l(n)}$, далі працює як звичайний детермінований алгоритм та подає на вихід правильний зв'язок із імовірністю не менше ніж $1 - \epsilon$, де ϵ — похибка а. й.

А. криптографічний /а. криптографический/ [encryption a.] — алгоритм, згідно якого здійснюється перетворення криптографічне інформації.

А. недетермінований /а. недетерминированный/ [non-deterministic a.] — алгоритм, який реалізується недетермінованою однострічковою машиною Тьюрінга.

А. обчислювальний /а. вычислительный/ [compute a.] — алгоритм точного або наближеного розв'язання задач прикладної математики на ЕОМ.

А. поліноміальний /а. полиномиальный/ [polynomial a.] — алгоритм, час роботи якого t обмежений поліномом певного ступеня, тобто $t(n) \leq c \cdot n^c$ для деякої константи c та будь-якої довжини входу n. А. п. в теорії складності відповідають швидким на практиці алгоритмам.

А. проектування системи захисту інформації /а. проектирования системы защиты информации/ [security system project a.] — розроблення варіанта потрібної системи захисту інформації, засноване на результатах аналізу системного існуючої інформаційної системи. Включає наступні етапи: визначення переліку інформації, що належить захисту, цілей, завдань, обмежень і показників ефективності системи захисту; моделювання існуючої системи і виявлення її недоліків із позицій поставлених цілей і завдань; визначення

і моделювання загроз безпеці інформації; розроблення варіантів (алгоритмів функціонування) системи, що проектується; порівняння варіантів за критерієм глобальним і показниками частковими, вибір найкращих варіантів; обґрунтування обраних варіантів перед керівництвом організації; доопрацювання варіантів або проекту з врахуванням зауважень. У зв'язку з відсутністю формальних способів синтезу системи захисту, її оптимізація при проектуванні можлива шляхом поступового наближення до раціонального варіанта в результаті декількох ітерацій.

А. шифрування /а. шифрования/ [encryption a.] — див. алгоритм криптографічний.

АЛФАВІТ — див. абетка.

АНАГРАМА /анаграмма/ [anagram] (від грец. *άνα*... — префікса, що означає повторну або зворотну дію і ...*γράμμα* — риска, літера, написання) — 1) Синонім шифру перестановки. 2) Переставляння окремих літер або складів у слові, внаслідок чого утворюються нові слова з іншим значенням.

АНАЛІЗ /анализ/ [analysis, interpretation, study, review] (від грец. *ἀνάλυσις* — розклад, розчленування) — 1) Метод дослідження, що полягає в мисленому або практичному розчленуванні цілого на складові частини. Протилежне синтез. 2) Уточнення логічної форми (побудови, структури) міркування засобами формальної логіки.

А. захищеності /а. защищенности/ — 1) Перевірка відповідності якісних і кількісних характеристик показників ефективності заходів із захисту інформації вимогам із безпеки інформації. 2) Процес виявлення уразливостей ресурсів автоматизованої системи, а також вироблення рекомендацій з їхнього усунення.

А. кваліфікаційний /а. квалификационный/ [evaluation] — аналіз системи обчислювальної з метою визначення рівня її захищеності і відповідності вимогам безпеки на основі критеріїв стандарту інформаційної безпеки. Інша назва кваліфікування рівня безпеки, оцінка безпеки інформації. Згідно "критеріїв Загальних" а. к. може здійснюватися як паралельно з розробкою продукту інформаційних технологій, так

і після її завершення. Для проведення к. а. розробник продукту повинен надати наступні матеріали: профіль захисту; проект захисту; різноманітні обґрунтування і підтвердження властивостей та можливостей ІТ-продукту, одержані розробником; сам ІТ-продукт; додаткові відомості, одержані шляхом проведення різноманітних незалежних експертиз. Процес а. к. включає три стадії: аналіз профілю захисту на предмет його повноти, несуперечності, реалізованості й можливості використання у вигляді набору вимог для продукту, що аналізується; аналіз проекту захисту на предмет його відповідності вимогам профілю захисту, а також повноти, несуперечності, реалізованості й можливості використання у вигляді еталона при аналізі ІТ-продукту; аналіз ІТ-продукту на предмет відповідності проекту захисту. Результатом а. к. є висновок про те, що підданий аналізу ІТ-продукт відповідає представленому проекту захисту.

А. криптографічний /a. криптографический/ [cryptoanalysis, cipher a.] — див. криптоаналіз.

А. прихованих каналів /a. скрытых каналов/ [covert channels a.] — послуга безпеки, яка забезпечує гарантію того, що канали приховані в системі комп'ютерній відсутні, знаходяться під наглядом або, принаймні, відомі.

А. радіосигналів технічний /a. радиосигналов технический/ [technical radio a.] — визначення умов добування інформації про радіозасоби та їхніх користувачів, що міститься в радіосигналах. Досягнення цієї мети здійснюється виконанням послідовності часткових завдань: визначення параметрів і розпізнавання типів сигналів і повідомлень; визначення інформативності параметрів сигналів як ознак їхніх джерел (інформативність повідомлень визначається на етапі аналізу їхнього змісту). Результати а. р. т. дозволяють надати рекомендації з пошуку і виявлення, пеленгування, розпізнавання, перехоплення, реєстрації сигналів і повідомлень, а також їхнього оброблення.

А. ризику /a. риска/ [risk a.] — процес визначення загроз безпеці інформації та їхніх характеристик, слабких сторін системи захисту інформації комплексної (відомих і припустимих), оцінки потенційних зби-

тків від реалізації загроз та ступеню їхньої прийнятності для експлуатації автоматизованої системи.

А. системний /а. системный/ [system a.] — 1) Аналіз об'єкта дослідження як сукупності елементів, що утворюють систему. У наукових дослідженнях він передбачає оцінку поведінки об'єкта як системи з усіма факторами, які впливають на його функціонування. А. с. можна здійснювати у відповідності до етапів системного аналізу. Кінцевим результатом а. с. є побудова моделі системи і розробка пропозицій з її удосконалення або зміни. 2) Аналіз призначення системи, яку передбачається проектувати, і встановлення множини вимог, яким вона повинна відповідати. Єдиної методики а. с. у наукових дослідженнях поки що немає. У практиці досліджень він застосовується з використанням таких методик: процедур теорії дослідження операцій, яка дає змогу дати кількісну оцінку об'єктам дослідження; аналізу систем дослідження об'єктів в умовах невизначеності; системотехніки, яка включає проектування і синтез складних систем у процесі дослідження їхнього функціонування.

А. трафіка /а. трафика/ [traffic a., sniffing] — прослуховування трафіка з метою збирання паролів, ключів, іншої ідентифікаційної або автентифікаційної інформації.

АНАЛІЗАТОР /анализатор/ [analyzer] (від аналіз) — 1) В оптиці — прилад (поляризаційна призма, поляроїд і т. ін.) для виявлення і дослідження поляризації світла. 2) А. гармонік — прилад для дослідження складових (гармонік) спектра частот; застосовується у високочастотній техніці. 3) В акустиці — а. звуку — прилад для аналізу звуку за частотними та часовими характеристиками. 4) Фізіологічні а. — анатомо-фізіологічні системи у людини і тварин, що здійснюють сприйняття і аналіз подразників, що поступають з зовнішнього і внутрішнього середовища; до аналізаторів відносяться всі органи чуттів (зоровий, слуховий, нюховий і т. ін.); кожний а. складається з рецептора, провідникової частини і вищого центра — групи нейронів у корі головного мозку.

А. спектру /а. спектра/ [spectrum a.] — прилад для візуального спостереження і вимірювання параметрів амплітудних, середніх за потужністю та фазових спектрів сигналів. За методом апаратурного

спектрального аналізу розрізняють а. с. паралельного (одночасного), послідовного та змішаного аналізу, а за принципом дії — аналогові та цифрові а. с. Основними характеристиками а. с. є: діапазон частот, смуга огляду, роздільна здатність, чутливість, динамічний діапазон вхідних сигналів, час аналізу, основні похибки вимірювання частотних інтервалів і вимірювань амплітуд (потужностей) спектральних компонентів тощо. Аналогові а. с. можуть бути реалізовані на різних принципах (дисперсійному, рециркуляційному, акустооптичному тощо), хоча на практиці найпоширенішими є фільтрові методи паралельного і послідовного аналізу.

АНАЛІТИК /аналитик/ [analyst] (від грец. *ἀναλυτικός* — аналітичний) — 1) Фахівець, який здійснює аналіз. 2) Особа, яка займається систематизацією розрізнених у часі подій, роз'ясненням, тлумаченням, співставленням однозначних або розрізнених фактів. 3) Фахівець в інформатиці й конкретній прикладній галузі, обов'язками якого є аналіз проблем, постановка завдань і розробка пропозицій для їхнього виконання.

А. бази даних /а. базы данных/ [database a.] — фахівець, котрий здійснює аналітичні функції, потрібні при проектуванні та (чи) для підтримки процесу користування базами даних.

А. системний /а. системный/ [system a.] — аналітик в галузі систем операційних, систем програмування, систем автоматизованих.

АНАЛІТИЧНИЙ /аналитический/ [analytical] (грец. *ἀναλυτικός*) — такий, що отримується в результаті розчленування об'єкта й аналізу одержаних унаслідок цього частин.

АНКЕТА /анкета/ [form, questionnaire] — лист для опитування, який самостійно заповнюється опитуваним за вказаними в ньому правилами. Анкетні опитування широко використовуються для одержання інформації про фактичний стан речей в галузі, що вивчається, їхній оцінці, поглядах, інтересах і мотивах діяльності опитуваних (респондентів). Див. також допит анкетний.

АНСАМБЛЬ /ансамбль/ [ensembles] (франц. ensemble, букв. разом) — 1) Узгодженість, струнке ціле. 2) Послідовність випадкових величин Z_n ($n \in \mathbf{N}$), які набувають значення у множині двійкових слів (в $0,1^n$).

А. непередбачуваний /а. непредугадываемый/ [unpredictable e.] — ансамбль, для якого для префіксу довільної довжини $s\sigma$ випадкового слова $Z_n \in /Z_n/_{n\in N}$, $\sigma \in /0,1/$, $s \in /0,1/^{k-1}$ та довільного алгоритму поліноміального ймовірнісного A з входом s виконується нерівність $|P[A(s)=\sigma]-\frac{1}{2}| < \frac{1}{n^c}$ для довільної константи c при досить великих n, де $P[X]$ — ймовірність випадкової події X.

А. нерозрізнені /а. неразличимые/ [indistinguishable e.] — ансамблі, які не можна відрізнити один від одного за допомогою будь-якого алгоритму ймовірнісного поліноміального. Більш точно — це такі ансамблі $/X_n/_{n\in N}$ та $/Y_n/_{n\in N}$, для яких для будь-якого ймовірнісного поліноміального алгоритму A: $|P[A(X_n)=1]-P[A(Y_n)=1]| < \frac{1}{n^c}$ для довільної константи c при досить великих n. Тут $P[A(X_n)=1]$ — ймовірність того, що алгоритм A розпізнає ансамбль X_n.

АНТЕНА /антенна/ [aerial, antenna] (від лат. antenna — рея) — пристрій для випромінювання (передавальна а.) або приймання (приймальна а.) радіохвиль. Передавальна а. перетворює енергію змінного струму високої частоти, що поступає від передавача, в енергію електромагнітних хвиль, які розповсюджуються від а. в просторі. Приймальна а. вловлює енергію електромагнітних хвиль і перетворює її в енергію змінного струму високої частоти (в електричні сигнали, амплітуда, частота і фаза яких відповідає аналогічним характеристикам електромагнітних хвиль). Основними характеристиками а. є діаграма спрямованості антени, коефіцієнт корисної дії антени, коефіцієнт спрямованої дії антени, коефіцієнт підсилення, частотна характеристика, опір випромінювання антени і т.ін. У відповідності з принципом взаємності (оборотності) кожна а. може працювати і як передавальна, і як приймальна, при цьому її основні характеристики не змінюються. Разом із тим передавальні і приймальні антени можуть відрізнятися одна від іншої конструкцією, електричною стійкістю і деякими іншими параметрами. А. класифікуються за наступними основними озна-

ками: за призначенням — передавальні, приймальні і приймально-передавальні, а також у залежності від галузі застосування — зв'язкові, телевізійні, радіолокаційні, радіоастрономічні, радіопеленгаційні і т. ін.; за діапазоном хвиль, що передаються або приймаються, на кілометрові, метрові, декаметрові, сантиметрові і міліметрові; за конструкцією та принципом дії — на проводові антени (вібраторні, штирові), антени акустичного типу (хвилепровідні, рупорні), антени оптичного типу (дзеркальні, лінзові), рамкові антени, спіральні антени, антени поверхневих хвиль (щілинні антени, діелектричні антени, антенні решітки); за розподілом випромінюваної енергії у просторі — на а. неспрямовані і спрямовані (із різноманітною формою діаграми спрямованості); за способом керування положенням діаграми спрямованості — на а. з механічним, електромеханічним і електричним скануванням променя; за місцем установлення — на а. наземні, підземні, танкові, корабельні, літакові (вертолітні), космічних апаратів та і т. ін.; за способом установки — на а. стаціонарні, тимчасові (аварійні), зовнішні, внутрішні, нестабілізовані, стабілізовані.

АНТИВІРУС /антивирус/ [antivirus] (від грец. *ἀντι*, що означає протилежність, протидію і вірус) — в обчислювальній техніці — програма, що виявляє або виявляє та знищує віруси комп'ютерні.

АПАРАТ /аппарат/ [apparatus, camera] (від лат. apparatus — устаткування) — прилад, пристрій.

А. космічний /а. космический/ [cosmic a.] — технічні пристрої для виконання завдань у космосі (космічний корабель, орбітальна станція, міжпланетна автоматична станція, супутник штучний Землі і т. ін.). За способом участі людини у функціонуванні а. к. вони поділяються на автоматичні, пілотовані і комбіновані; за призначенням — на науково-дослідницькі і прикладні (метеорологічні, навігаційні, розвідувальні, зв'язку і т. ін.).

А. літальний (ЛА) /а. летательный (ЛА)/ [airborne vehicle, aircraft, airship, craft, flier] — технічний пристрій для польотів в атмосфері Землі або в космічному просторі. Розрізняють такі ЛА: легші за повітря (повітроплавні), важчі за повітря (авіаційні, космічні, авіаційно-космічні та ракети). ЛА поділяють також на пілотовані та безпілотні, на одно- та багаторазового використання, за призначенням — на науково-дослідні,

народногосподарські та військові. До повітроплавних ЛА відносяться аеростати і дирижаблі. Авіаційні ЛА поділяються на крилаті (літаки, планери) та гвинтокрилі (гелікоптери, автожири, гвинтокрили); ракети — на балістичні та крилаті. До КЛА відносяться навколоземні орбітальні космічні апарати — ШСЗ та міжпланетні автоматичні станції. Авіаційно-космічні апарати поєднують ознаки авіаційних і космічних апаратів (повітряно-космічний корабель, повітряно-космічний літак).

А. літальний безпілотний (БПЛА) /а. летательный беспилотный(БПЛА)/ [pilotless vehicle] — апарат літальний, на борті якого не передбачено розташування екіпажу. Розрізняють а. л. б. легші і важчі за повітря, для атмосферних і космічних польотів, воєнного і цивільного призначення, одноразового і багаторазового застосування, з керуванням від бортового програмного пристрою або з телекеруванням (дискретним або безперервним). Див. також апарат літальний пілотований дистанційно.

А. літальний пілотований дистанційно (ДПЛА) /а. летательный пилотируемый дистанционно (ДПЛА)/ [remotely piloted vehicle (RPV)] — апарат літальний безпілотний, політ якого здійснюється під безперервним контролем, а на певних етапах — під безпосереднім керуванням оператора, що знаходиться на наземному або повітряному пункті управління, з використанням двосторонніх каналів радіозв'язку. Встановлені на ДПЛА засоби огляду навколишнього середовища (телевізійні та інші) забезпечують ніби "ефект присутності" оператора-пілота на борті ЛА. Розрізняють ДПЛА літакової і вертолітної схем, одноразового та багаторазового використання, з наземним і повітряним стартом, посадкою "по літаковому" або на парашуті (у тому числі з підхопленням ДПЛА з повітря вертольотом), а за призначенням — для розвідки і цілевказу, радіоелектронної боротьби, нанесення ударів по наземних (морських) цілях, проведення льотних експериментальних досліджень і т. ін.

А. літальний розвідувальний безпілотний /а. летательный разведывательный беспилотный/ [reconnaissance pilotless vehicle, scout pilotless vehicle] — безпілотний апарат літальний (БПЛА), призначений для ведення стратегічної, оперативної або тактичної повітряної розвідки на сухопутних та морських

ТВД. БПЛА поділяються на малогабаритні і крупногабаритні, літакові або вертолітного компонування, ближньої або дальньої дії, багаторазового (більшість) і одноразового використання. БПЛА запускають різними способами: із спеціалізованих пускових установок, за допомогою літаків-носіїв, власними двигунами. Приземлювання БПЛА здійснюється за допомогою парашутів, гальмівних костилів і сіток-вловлювачів. В різних варіантах БПЛА оснащуються фото- і телевізійними камерами, інфрачервоними приладами, засобами радіо- і радіотехнічної розвідки, апаратурою РЕБ. Наведення і управління БПЛА здійснюють наземні центри.

А. фотографічний /a. фотографический/ [c. (photographic c.)] — оптико-механічний прилад для одержання оптичного зображення об'єкта, що фотографується, на світлочутливому шарі фотоматеріалу. Всі а. ф. складаються зі світлонепроникного корпусу із закріпленим на його передній стінці об'єктивом, пристрою для розташування або фіксації світлочутливого матеріалу, розташованого біля задньої стінки корпусу, і затвора, призначеного для пропускання протягом певного часу (часу експозиції) світлового потоку від об'єкта, що фотографується. Крім того, а. ф. обладнуються допоміжними вузлами і механізмами, які полегшують та автоматизують процес зйомки, дозволяють розширити його можливості, покращити технічні параметри. За розмірами світлочутливих матеріалів а. ф. поділяються на п'ять груп: мікроформатні, півформатні, мало-, середньо- і великоформатні. За призначенням а. ф. поділяються на широкого застосування і спеціального застосування. В залежності від способу наведення на різкість а. ф. можна розділити на наступні групи: з наведенням на різкість за зображенням на екрані ф. а. (дзеркальні або SLR — а. ф.); з наведенням по монокулярному далекомірному пристрою, що механічно зв'язаний з об'єктивом ф. а.; з нерухомим жорстко встановленим об'єктивом, сфокусованим на гіперфокальну відстань; з пристроєм автоматичного фокусування. За технічною оснащеністю а. ф. поділяються на три класи: простий, середній, високий. За показниками оснащення ф. а. вбудованими експонометрами, а також за ступенем автоматизації встановлення експозиційних параметрів а. ф. ділять на три групи: з ручною установкою, з півавтоматичною і з автоматичною

установкою експозиції.

А. фотографічний копіювальний /a. фотографический копировальный/ — спеціальний апарат фотографічний, призначений для оперативного копіювання документів. Складається з дзеркального фотографічного апарата, відкидної стійки, джерела світла, блока живлення від батареї або освітлювальної мережі, а також утримувача документів.

А. фотографічний цифровий /a. фотографический цифровой/ [digital c.] — апарат фотографічний з світлоелектричним перетворювачем на основі приладу із зарядовим зв'язком, електричні сигнали з виходу якого перетворюються в цифровий вигляд і запам'ятовуються в напівпровідниковій пам'яті апарата або записуються на його магнітний диск. Маючи можливості класичного електромеханічного фотографічного апарата, а. ф. ц. дозволяє надати користувачеві додаткові функції, які значно підвищують оперативність фотографування. До таких функцій відносяться: можливість зйомки в безперервному режимі з частотою 5–15 кадрів/с, запис текстових і звукових коментарів, дати з часом фотозйомки, перегляд зображень у процесі й після зйомки на оборотному екрані, відображення поточних параметрів зйомки (кількості знятих кадрів, обсяг вільної пам'яті, потоковий режим компресії) і т.ін. Передбачені різноманітні режими перегляду кадрів і стирання непотрібних, друк вибраних на спеціальному принтері. Стандартний інтерфейс а. ф. ц. дозволяє переглядати зображення на екрані телевізора, записувати на відеомагнітофон або друкувати на відеопринтері. А. ф. ц. також може з'єднуватися з ПЕОМ для подальшого оброблення зображення: відображення на дисплеї, редагування за допомогою графічних редакторів, виведення на друк, передавання комп'ютерними мережами.

А. фотографічні мікроформатні /a. фотографические микроформатные/ [microformat c.] — група апаратів фотографічних достатньо простої конструкції, що заряджаються вузькою фотоплівкою шириною 8–16 мм, і призначені для оперативного потайного фотографування об'єктів спостереження або копіювання документів. Ранні а. ф. м. мають горизонтальне компонування апарата з об'єктивом, втопленим у

корпус, який складається з двох частин, одна з яких рухома і є одночасно захисним кожухом, важелем зводу і протягу плівки до наступного кадру. Нові моделі а. ф. м. мають традиційну форму, найчастіше є півавтоматичними з пружинним приводом, який дозволяє працювати в будь-яких кліматичний умовах, і передбачають можливість дистанційного управління процесом зйомки.

АПАРАТУРА /аппаратура/ [apparatus, hardware, equipment] — фізичне обладнання: механічні, магнітні, електричні і електронні пристрої.

А. передавання даних (АПД) /а. передачи данных (АПД)/ [data communication (circuit-terminating) group e.] — пристрій у складі станції передавання даних, який забезпечує перетворення і кодування сигналів між кінцевим обладнанням даних і лінією.

А. передавання даних групова /а. передачи данных групповая/ [data communication group e.] — апаратура передавання даних для роботи з декількома каналами передавання даних.

АПАТІЯ /апатия/ [apathy] — емоційний стан, що виникає внаслідок утрати перспективи, емоційного придушування, втрати віри в кінцеву мету, в керівництво, в успіх компанії і т.ін. А. характеризується емоційною пасивністю, байдужістю до подій навколишньої дійсності і розвивається на фоні зниження фізичної і психічної активності.

АРБІТР /арбитр/ [arbiter] (франц. arbitre, від лат. arbiter — посередник) — посередник, що його обирають сторони за взаємною згодою або в передбаченому законом порядку з метою розв'язання спору. Див. також третя сторона.

АРГУМЕНТ /аргумент/ [argument] (лат. argumentum, від arguo — показую, виявляю) — 1) Підстава, доказ, які наводяться для обґрунтування, підтвердження чого-небудь. При використанні впливу змісту інформації застосовують три основні категорії а. для переконування: правдиві факти; а., що дають "психологічне задоволення", оскільки вони апелюють до позитивного очікування; а., що апелюють до негативних

очікувань. За способом подання а. розрізняють так звані повідомлення односторонні й повідомлення двосторонні. 2) А. функції — незалежна змінна величина.

АРГУМЕНТАЦІЯ /аргументация/ [argumentation] (лат. argumentatio) — 1) Наведення аргументів. 2) Сукупність аргументів на користь чого-небудь. Підбір, побудова і подання а. є однією з важливих характеристик змісту інформації (див. вплив змісту інформації).

АРХІВ /архив/ [repository] (лат. archivum, від грец. *ἀρείν* — урядовий будинок) — 1) Сукупність документів архівних, а також архівний заклад або структурний підрозділ закладу, організації або підприємства, що здійснюють прийом і зберігання архівних документів в інтересах користувачів. 2) В обчислювальній техніці — система адміністративних заходів і програмних засобів, що забезпечують зберігання і доступність даних у формі документів (модулів, програм, масивів, файлів).

А. секретний /секретный а./ [confidentiality r.] — архів, про який не заявлено публічно.

АРХІТЕКТУРА /архитектура/ [architecture] (лат. architectura, від грец. *ἀρχιτέκτων*) — концепція взаємозв'язку елементів складної структури. Включає компоненти логічної, фізичної і програмної структур.

А. відкритих систем /а. открытых систем/ [open system a.] — концепція мережі обчислювальної, яка розроблена і розвивається Міжнародною організацією зі стандартизації (ISO); семирівнева модель з'єднання відкритих систем, яка відіграє важливу роль як методологічна, концептуальна й термінологічна основа побудови обчислювальних мереж. Див. також модель взаємодії відкритих систем та модель ISO/OSI.

А. захисту інформації в мережах телекомунікацій /а. защиты информации в сетях телекоммуникаций/ — концепція захисту інформації в мережах телекомунікацій, що використовують міжнародні стандарти, яка розроблена і розвивається Міжнародною організацією зі стандартизації (ISO) (див. рекомендації МОС) у відповідності до ідеології моделі взаємодії відкритих систем.

АСОЦІЮВАННЯ /ассоциирование/ [associate] (лат. associatio — сполучення, з'єднання, від associo —

з'єдную) — сполучення, з'єднання чого-небудь в єдине ціле.

А. з іншою програмою /а. с другой программой/ — інтеграція коду програми з потенційно небезпечними наслідками або її частини в код іншої програми таким чином, щоб при деяких умовах керування передавалося на код програми з потенційно небезпечними наслідками.

АСТЕНІК /астеник/ (від грец. *ἀσθενικός* — безсилий, кволий, млявий) — людина, для якої характерна певна будова тіла: довга вузька грудна клітка, довга шия, худорлявість, слабо розвинені м'язи.

АСТЕНІЯ /астения/ [asthenia] (від грец. *ἀσθένεια* — безсилля, слабість) — стан безсилля, загальна кволість організму.

АТАКА /атака/ [attack] (від франц. attague — напад) — 1) Стрімкий напад на противника в поєднанні з навальним вогнем. 2) Дії порушника, спрямовані на порушення однієї з функцій захисту інформації (причетності, автентифікації, цілісності, доступності, конфіденційності); зловмисна дія. 3) Реалізація загрози інформації. 4) Криптоаналіз; метод криптоаналізу.

А. активна /а. активная/ — атака на мережу обміну інформацією віддалена, яка здійснюється з метою нанесення прямих збитків мережі шляхом порушення конфіденційності, цілісності і доступності інформації, а також здійснення впливів психологічних на користувачів мережі. Очевидною особливістю а. а. порівняно з пасивною атакою є принципова можливість її виявлення.

А. без зворотного зв'язку /а. без обратной связи/ — атака на мережу обміну інформацією віддалена, яка здійснюється внаслідок передачі на об'єкт атаки одиночних запитів, відповіді на які суб'єктові атаки не потрібні.

А. безумовна /а. безусловная/ — атака на мережу обміну інформацією віддалена, початок здійснення якої є безумовним по відношенню до об'єкта атаки, тобто атака здійснюється негайно й безвідносно до

стану мережі і об'єкта атаки.

А. віддалена типова /а. удаленная типовая/ [remote a.] — віддалений інформаційний руйнівний вплив, програмно здійснюваний каналами зв'язку та характерний для будь-якої розподіленої обчислювальної системи. Віддаленою може бути будь-яка з типових атак, але характерними для розподілених обчислювальних систем є атака аналізу трафіка та специфічні методи організації типових атак, наприклад, впровадження фальшивого об'єкта шляхом нав'язування фальшивого маршруту, недоліків алгоритму віддаленого пошуку. Специфічними атаками для мережі Інтернет є атаки шляхом упровадження фальшивих ARP та DNS серверів.

А. внутрішньосегментна /а. внутрисегментная/ — атака на мережу обміну інформацією віддалена, при здійсненні якої суб'єкт атаки і об'єкт атаки знаходяться в одному сегменті мережі обміну інформацією.

А. вставкою /а. вставкой/ [Man-In-The-Middle (MITM) a.] — усі повідомлення, що передаються між двома абонентами проходять крізь противника. Таким чином, противник перехоплює всі повідомлення одного абонента та ретранслює їх іншому. При цьому противник може намагатися модифікувати, знищувати перехоплені повідомлення або передавати власні повідомлення. Ця атака наочно демонструє необхідність автентичного передавання відкритих ключів в асиметричних криптосистемах.

А. глобальна (широкомасштабна) /а. глобальная (широкомасштабная)/ — атака на мережу обміну інформацією віддалена, спрямована на декілька сегментів мережі обміну інформацією.

А. довготривала /а. долговременная/ — віддалена атака на мережу обміну інформацією, що передбачає проведення тривалих за терміном багаторазових атак на об'єкти мережі обміну інформацією, як правило, з використанням різноманітних видів зброї інформаційної.

А. електронна /а. электронная/ [electronic a.] — елемент війни електронної, що передбачає активний вплив на електронні засоби противника. За видом впливу е. а. поділяється на дві компоненти: неруйнівні

впливи, які включають електронне придушення і електронну дезінформацію; руйнівні впливи на основі застосування протирадіолокаційних ракет, зброї спрямованої енергії (лазерної, НВЧ) і т. ін.

А. за умови запиту об'єкта /a. на запрос объекта/ — атака на мережу обміну інформацією віддалена, яка здійснюється суб'єктом атаки при умові одержання від потенційного об'єкта атаки запиту певного типу.

А. за умови настання очікуваної події на об'єкті /a. по наступлению ожидаемого события на объекте/ — атака на мережу обміну інформацією віддалена, яка здійснюється суб'єктом атаки при умові виникненні на потенційному об'єкті атаки певної події.

А. із зворотним зв'язком /a. с обратной связью/ — атака на мережу обміну інформацією віддалена, яка характеризується тим, що на деякі запити, передані на об'єкт атаки, суб'єктові атаки потрібно одержати відповідь, тобто, між об'єктом атаки й суб'єктом атаки існує зв'язок зворотний, який дозволяє суб'єктові атаки адекватно реагувати на усі зміни, що відбуваються на об'єкті атаки. Дана атака може здійснюватися наступним чином: установлення суб'єктом атаки контролю над об'єктом атаки (спостереження за об'єктом атаки); очікування суб'єктом атаки встановленого запиту ("доповіді") від системи інформаційного впливу, що функціонує на об'єкті атаки; видача суб'єктом атаки команди на виконання певних операцій; виконання заданих операції; повідомлення суб'єктові атаки про виконання операції. Дальше слід перейти до другого (або третього) пункту послідовності дій. Таким чином, при наявності зворотного зв'язку суб'єкт атаки має можливість керувати віддаленою атакою (в ідеальному випадку — в реальному масштабі часу). Переривання зворотного зв'язку може привести до втрати керування атакою, а, отже, і до припинення атаки.

А. інформаційна /a. информационная/ [information a.] — сукупність активних впливів інформаційних сил і засобів окремих підрозділів на елемент або групу елементів систем інформаційних противника з метою

вирішення тактичних завдань боротьби інформаційної.

А. криптоаналітична /a. криптоаналитическая/ [cryptoanalytic a.] — загальна назва методу, яким криптоаналітик намагається зламати криптосистему. У загальному випадку, атака не є алгоритмом злому криптосистеми, а деякою спробою злому, в результаті якої отримується інформація, що використовується в подальшому для розробки спеціального алгоритму. А. к. за інформацією, якою володіє криптоаналітик, ділять на: *атака криптоаналітична лише із криптотекстом*, *атака криптоаналітична з відомим відкритим текстом*, атака криптоаналітична з вибраним відкритим текстом, атака криптоаналітична з вибраним криптотекстом, атака криптоаналітична з вибраним ключем. При всіх а. к. за *принципами Кергхофа* вважається, що криптоаналітикові відома повна інформація про алгоритм шифрування, за винятком ключа.

А. криптоаналітична з адаптивно вибраним відкритим текстом /a. криптоаналитическая с адаптивно открытым текстом/ [adaptive chosen plaintext a.] — частковий випадок ітеративної атаки криптоаналітичної з вибраним відкритим текстом, при якій криптоаналітик обирає відкритий текст на наступному кроці залежно від отриманого результату на поточному кроці.

А. криптоаналітична з вибраним відкритим текстом /a. криптографическая з выбранным открытым текстом/ [chosen plaintext a.] — атака криптоаналітична, при якій криптоаналітик має можливість сам обирати пари відкритого тексту та відповідного йому шифртексту. Частковим випадком цієї криптографічної атаки є диференційний метод криптоаналізу.

А. криптоаналітична з вибраним ключем /a. криптоаналитическая с выбранным ключом/ [chosen key a.] — атака криптоаналітична, при якій криптоаналітик використовує деяку інформацію про взаємозв'язки між різноманітними ключами.

А. криптоаналітична з вибраним криптотекстом /a. криптоаналитическая с выбранным кри-

птотекстом/ [chosen cryptogram a.] — атака криптоаналітична, при якій криптоаналітик має можливість обирати криптотексти та отримувати з них відкриті тексти.

А. криптоаналітична з відомим відкритим текстом /а. криптографическая с известным текстом/ [known plaintext a.] — атака криптоаналітична, при якій криптоаналітикові відомі деякі випадкові пари відкритого тексту та відповідного йому шифртексту. Завданням криптоаналітика є визначення ключа або отримання ефективного алгоритму для дешифрування деяких інших шифртекстів. Прикладом цієї краптоаналітичної атаки є метод імовірних слів, який складається з визначення шифртексту, відповідного до слів, які часто зустрічаються в повідомленні (наприклад, слова "секретно"). Більш універсальною атакою цього класу є метод лінійного криптоаналізу.

А. криптоаналітична зустрічна /а. криптоаналитическая встречная/ [meet-in-the-middle a.] — в широкому розумінні — метод оптимізації за пам'яттю та часом процедури прямого перебирання рішень. В частковому — криптоаналітична атака з відомим відкритим текстом на криптосистеми з подвійним шифруванням.

А. криптоаналітична лише із криптотекстом /а. криптографическая только с криптотекстом/ [cryptotext-only a.] — атака криптоаналітична, при якій криптоаналітику відома певна кількість криптотекстів, зашифрованих з використанням одного і того ж ключа. Для даного методу атаки широко використовуються методи математичної статистики. Окремим випадком цієї атаки є криптоаналітична атака методом прямого перебору ключів або брутальна (силова) криптоаналітична атака (brute force attack), яка складається з перебору всіх ключів з простору ключового.

А. криптоаналітична силова /а. краптоаналитическая силовая/ [brute force a.] — атака криптоаналітична, яка проводиться шляхом повного перебирання всіх можливих ключів у криптосистемі.

А. локальна /а. локальная/ — атака на мережу обміну інформацією віддалена, спрямована на окремий

сегмент мережі обміну інформацією, а в окремому випадку, на окремий елемент мережі (ПЕОМ, канал зв'язку).

А. міжсегментна /а. междусегментная/ — атака на мережу обміну інформацією віддалена, при здійсненні якої суб'єкт атаки і об'єкт атаки знаходяться в різних сегментах мережі обміну інформацією (наприклад, на відстані багатьох тисяч кілометрів), що може суттєво перешкодити проведенню заходів з відбиття атаки.

А. на мережу обміну інформацією /а. сеть обмена информацией/ — реалізація загрози мережі обміну інформацією, що полягає в пошуку й використанні цієї чи іншої уразливості мережі.

А. на мережу обміну інформацією віддалена /а. сеть обмена информацией удаленная/ — процес впливу інформаційного (неенергетичного) на інформацію, що зберігається, обробляється й передається в мережі обміну інформацією (МОІ) з метою нанесення збитків і (або) забезпечення умов для нанесення збитків МОІ і (або) її користувачам, що здійснюється каналами зв'язку. Виділяють два види віддалених атак — віддалені атаки на інфраструктуру мережі обміну інформацією і протоколи мережі, і віддалені атаки на телекомунікаційні служби. Віддалені атаки можна класифікувати за наступними ознаками: за характером впливу (атаки пасивні, активні і умовно-пасивні); за метою впливу (порушення конфіденційності інформації або інформаційних ресурсів МОІ, порушення цілісності інформації, порушення доступності [працездатності] об'єкта МОІ); за умови початку здійснення впливу (атака за умови запиту об'єкта, що атакується, атака за умови настання очікуваної події на об'єкті, що атакується, атака безумовна); за умови ситуації здійснення впливу (напад інформаційний,[зустрічний] вплив у відповідь на інформаційний напад); за наявністю зворотного зв'язку з об'єктом, що атакується (атака зі зворотним зв'язком, атака без зворотного зв'язку [атака односпрямована]); за розташуванням суб'єкта атаки відносно об'єкта, що атакується (атаки внутрішньосегментні і атаки міжсегментні); за тривалістю впливів (атаки разові, атаки довготривалі); за масштабом впливів (атаки локальні, атаки глобальні [широкомасштабні]); за рівнем моделі взаємодії

відкритих систем (МВВС), на якому здійснюється вплив (атака відповідно на фізичний, канальний, мережний, транспортний, сеансовий, представницький або прикладний рівень). У зв'язку з тим, що віддалена атака реалізується мережною програмою, то найбільш логічно представляти віддалені атаки на МОІ у проекції їх на МВВС.

А. на систему захисту /а. на систему защиты/ [security system a.] — спроба подолання системи захисту. Атака може бути активною, тобто такою, що веде до зміни даних, і пасивною. Той факт, що атака була проведена, ще не означає, що вона була успішною. Міра "успіху" атаки залежить від уразливості системи захисту та ефективності захисних заходів.

А. односпрямована / а. однонаправленная/ — те ж, що атака без зворотного зв'язку.

А. пасивна /а. пассивная/ — атака на мережу обміну інформацією віддалена, яка здійснюється з метою порушення політики безпеки інформації. А. п. не здійснює безпосереднього впливу на роботу мережі.

А. перехоплення та повтору /а. перехвата и повтора/ [replay a.] — спроба реалізації загрози системі, заснована на застосуванні реквізитів доступу або інших даних системи захисту, які використовувалися раніше. Найчастіше здійснюється в системах електронної комерції (електронних фінансових системах, системах електронної торгівлі) у разі застосування незахищеної автентифікації простої.

А. разова /а. разовая/ — атака на мережу обміну інформацією віддалена, що полягає в проведенні обмежених у часі цілеспрямованих впливів на об'єкти мережі обміну інформацією.

А. словникова /а. словарная/ [dictionary a.] — спроба визначення пароля або ключа шляхом перебору по ключових словах, що часто використовуються на практиці. Множина цих слів і складає словник, звідки походить назва атаки. Найбільш відомі приклади цієї атаки на схеми парольної автентифікації операційних

систем.

А. стегоаналітична /а. стегоаналитическая/ — загальна назва методу, яким стегоаналітик намагається зламати систему стеганографічну. А. с. поділяються за критерієм інформації, яка відома противникові — з відомим контейнером, з вибором контейнера, з відомою стеганограмою (стего), з обраною стеганограмою, з відомим прихованим повідомленням, з обраним прихованим повідомленням; за метою порушника — виявлення прихованих повідомлень стегоключів), руйнування прихованих повідомлень, які поділяються на стиск стеганограми з утратою даних, геометричні перетворення стеганограми, зашумлення контейнера, фільтрація

А. умовно-пасивна /а. условно-пассивная/ — атака на мережу обміну інформацією віддалена, яка має за мету підготовку до атаки активної і включає заходи ведення розвідки комп'ютерної та подолання системи захисту інформації мережі.

АТЕСТАЦІЯ /аттестация/ [certification, attestation] (від лат. attestatio — посвідчення) — 1) Авторитетне підтвердження відповідності продукту своєму призначенню. 2) Діяльність, спрямована на підтвердження відповідності об'єкта інформаційної діяльності вимогам державних стандартів, інших нормативних документів із захисту інформації, затвердженими державними органами із сертифікації в межах їхньої компетенції. А. дає право власнику об'єкта інформаційної діяльності обробляти інформацію з рівнем секретності, що відповідає рівню безпеки інформації.

А. випробувальних лабораторій /а. испытательных лабораторий/ — засвідчення компетентності випробувальної лабораторії і її оснащеності, які забезпечують проведення на належному технічному рівні усіх передбачених нормативно-технічною документацією випробувань заданих видів продукції і (або) видів випробувань.

А. засобів захисту /а. средств защиты/ [а. security] — засвідчення ступеня відповідності вимогам до

даного класу засобів захисту.

А. захисту /а. защиты/ [security certification] — підтвердження уповноваженою компетентною особою того, що оцінка захисту була зроблена кваліфіковано і відповідно до встановлених правил.

А. захищеного об'єкта /а. защищенного объекта/ — офіційне підтвердження наявності на захищеному об'єкті необхідних і достатніх умов, які забезпечують виконання встановлених вимог керівних документів і норм ефективності захисту інформації.

А. програми /а. программы/ [program validation] — авторитетне підтвердження якості програми на основі загальноприйнятої або офіційної процедури; комплекс перевірок, що забезпечує одержання гарантії відповідності програми своєму призначенню.

АТЛЕТІК /атлетик/ (від грец. *ἀθλητής* — учасник змагань, борець) — фізично розвинена дужа людина.

АТРИБУТ /атрибут/ [attribute] (від лат. attributum — додане) — елементарне дане, яке описує властивості сутності.

А. доступу /а. доступа/ [tag, access mediation information] — будь-яка зв'язана з об'єктом системи комп'ютерної інформація, яка використовується для керування доступом.

АУДІО... /аудио.../ [audio...] (від лат. audio — слухаю) — у складних словах відповідає поняттю "слуховий".

АУДІОМАГНІТОФОН /аудиомагнитофон/ [audio tape] (від аудіо... і магнітофон) — магнітофон з мікрофоном (винесеним або вбудованим), призначений для реєстрації акустичних сигналів. А. для запису мови називають диктофонами. Диктофони для скритого підслухування мають понижені акустичні шуми стрічкопротягувального механізму, металевий корпус для екранування високочастотного електромагнітного поля колекторного двигуна, в них можуть бути відсутні генератори стирання і підмагнічування. Запис мови здійснюється на мікрокасеті із швидкістю 2, 4 або 1,2 см/с, тривалість запису в залежності від швид-

кості і типу касети може складати від 15 хв. до 3 годин. Різноманітні моделі диктофонів можуть мати сервісні функції: активація (вмикання) запису голосом, можливість приєднання зовнішнього мікрофона, автостоп і автореверс, рідиннокристалічний дисплей з індикацією режимів роботи і витрат стрічки.

АУДІОПЕРЕХОПЛЕННЯ /аудиоперехват/ (від аудіо... і перехоплення) — метод добування інформації, що розповсюджується або відтворюється за допомогою акустичних хвиль. В залежності від місця встановлення акустоперетворюючих пристроїв, можна виділити два основні різновиди а.: аудіоперехоплення без заходу на об'єкт і аудіоперехоплення із заходом на об'єкт.

А. без заходу на об'єкт /а. без захода на объект/ — аудіоперехоплення, що здійснюється за допомогою акустичних та вібраційних датчиків знімання інформації, що встановлюються на інженерно-технічні конструкції, які знаходяться за межами об'єкта (приміщення), з якого необхідно приймати мовні сигнали. Часто для а. використовують мікрофони спрямовані, мікрофони лазерні тощо, призначені для дистанційного знімання мовної інформації через наскрізні отвори (двері, вікна, кватирки, сміттє- і повітропроводи і т. ін.) і віконне (автомобільне) скло.

А. із заходом на об'єкт /а. из заходом на объект/ — аудіоперехоплення, здійснюване за допомогою пристроїв підслухування, встановлених в апаратуру засобів оброблення інформації, в різноманітні технічні пристрої, на проводові комунікаційні лінії (радіо, телефон, телевізійний кабель, охоронно-пожежної сигналізації і т. ін.), а також в різноманітні конструкції інженерно-технічних споруд і побутових предметів, що знаходяться на об'єкті, з метою перехоплення розмов працюючого персоналу і звукових сигналів технічних пристроїв.

АУДИТ /аудит/ [audit] — 1) Процес одержання і аналізу записів системного журналу з метою встановлення поточного стану системи. 2) Експертиза автоматизованої інформаційної системи і всіх її складових з метою визначення стану безпеки системи, її відповідності до вимог діючого законодавства і організаційно-розпорядницьких документів організації.

АФЕКТ /аффект/ [affect] (від лат. affectus — настрій, хвилювання, пристрасть) — короткочасне бурхливе переживання людини (гнів, лють, жах, відчай, раптова велика радість).

Б

БАЗА /база/ [base] (франц. base, від грец. *βάσις* — основа) — заклад, установа, центральний пункт із постачання або обслуговування кого-чого-небудь.

Б. даних (БД) /б. данных (БД)/ [database (DB)] — 1) Об'єктивна форма подання і організації сукупності даних, систематизованих таким чином, щоб ці дані могли бути знайдені і оброблені за допомогою ЕОМ. 2) Незалежна від програм прикладних сукупність даних, організованих за певними правилами, які передбачають загальні принципи опису, зберігання і маніпулювання даними. Являє собою інформаційну модель частини предметної. БД, як правило, представляється трьома рівнями абстракції: зовнішнім, концептуальним і внутрішнім. Відповідно до цих рівнів розрізняють зовнішню, концептуальну і фізичну моделі (схеми) БД. Звернення до БД здійснюється за допомогою системи керування базами даних.

Б. даних архівна /б. данных архивная/ [archive database] — зафіксована в певний момент копія бази даних.

Б. даних колективного користування /б. данных коллективного пользования/ [sharable database] — база даних, до якої має доступ багато користувачів. При цьому користувачі можуть звертатися до даних одночасно або послідовно, а інтерактивному або пакетному режимах.

Б. даних персональна (особиста, приватна) /б. данных персональная (личная, частная)/ [personal (private) database] — база даних, з якою взаємодіє один користувач.

Б. даних розподілена (РБД) /б. данных распределенная (РБД)/ [distributed database] — сукупність баз даних, фізично розподілених по взаємозв'язаних ресурсах системи обчислювальної і доступних для

спільного використання в різноманітних випадках. В РБД реалізований принцип інтеграції баз даних на глобальному, концептуальному рівні, що дозволяє подати всі бази даних як єдину базу даних. Керування РДБ здійснюється за допомогою системи керування розподіленими базами даних.

Б. даних спільна /б. данных общая/ — база даних колективного користування, яка розташовується, як правило, на сервері.

Б. знань /б. знаний/ [knowledge b.] — семантична модель, призначена для подання в ЕОМ знань, накопичених людиною в певній частині предметній. Є основною складовою частиною інтелектуальних, як правило, систем експертних. Для подання знань використовується ряд моделей, таких як мережа семантична, фреймова, продукційна та інші моделі.

Б. інформаційна /б. информационная/ [information b.] — в системах автоматизованих — сукупність даних, розташованих на зовнішніх носіях і призначених для використання програмами та користувачами. Наприклад, в банках даних б. і. — це частина інформаційного фонду, що включає бази даних і їхні описи — метадані.

БАНК /банк/ [bank] (нім. Bank, франц. banque, з італ. banco — лава, конторка, стіл міняйла) — 1) Особливий економічний інститут, що акумулює тимчасово вільні кошти, надає кредит, здійснює грошові розрахунки, випускає в обіг гроші, цінні папери. 2) Сукупність однотипних елементів, засобів або пристроїв, взаємно з'єднаних і спільно використовуваних. Наприклад, банк даних — сукупність баз даних і системи керування ними; банк пам'яті — сукупність елементів основної пам'яті в мультипроцесорній ЕОМ; банк програм — сукупність програм.

Б. даних (БнД) /б. данных (БнД)/ [databank (information b.)] — система інформаційна автоматизована для централізованого зберігання і колективного використання даних. До складу Б. д. входять одна чи декілька баз даних, а також набір прикладних програм, складених на мові даної системи керування базами

даних.

Б. даних локальний /б. данных локальный/ [local databank] — банк даних, розташований в одному обчислювальному центрі або в зовнішній пам'яті однієї ЕОМ.

Б. даних Національний /б. данных Национальный/ (від франц. national — народний, державний) — сукупність взаємозв'язаних масивів даних про територію країни і її адміністративно-територіальний поділ, природні ресурси, виробничо-економічну структуру народного господарства, національне багатство, інфраструктуру, населення і трудові ресурси, а також засоби керування цими масивами. Б. д. Н. існує в ряді країн у зв'язку з необхідністю удосконалення інформаційного забезпечення процесів державного планування і управління народним господарством. В широкому розумінні слова він являє собою інформаційно-пошукову систему, яка складається з окремих (галузевих, відомчих, територіальних або цільових), але взаємозв'язаних банків даних, в яких реалізуються: принцип фактографічної системи (б. д. Н. має централізовані масиви або банки даних, які безпосередньо забезпечують органи управління укрупненою інформацією); принцип адресної системи (б. д. Н. забезпечує можливість звернення за детальною інформацією в локальні банки даних). Б. д. Н. забезпечує також єдине і однозначне кодування інформації на основі централізованого введення класифікаторів або систем однозначного кодування.

Б. даних розподілений /б. данных распределенный/ [distributed databank] — система територіально розподілених банків даних локальних, які функціонують під єдиним керуванням і об'єднуються засобами мережі обчислювальної. Основу такої системи складають бази даних розподілені (РБД) і система керування розподіленими базами даних (СКРБД).

Б. інформаційний /б. информационный/ [information b.] — те ж, що і банк даних.

БЕЗПЕКА /безопасность/ [security, safety] — стан, при якому кому-небудь, чому-небудь не загрожує небезпека (будь-якого виду), існує захист від небезпеки. Виділяють три рівні безпеки: особистості, суспільства,

держави і розрізняють зовнішню, міжнародну, внутрішню, національну, політичну, державну, інформаційну, особисту, воєнну, суспільну, регіональну, господарську, економічну, продовольчу, екологічну безпеку. В державній практиці різних країн створюються міністерства, комітети, ради національної (державної) б., відповідні органи, структури і служби.

Б. автоматизованої системи /б. автоматизированной системы/ — захищеність системи автоматизованої від несанкціонованого втручання в нормальний процес її функціонування, а також від спроб розкрадання, незаконної модифікації або руйнування її компонентів.

Б. банківської інформації /б. банковской информации/ — безпека інформації, яка обробляється в банківських системах. Основним фактором, за яким забезпечення б. б. і. виділяється в окреме завдання є те, що банківські системи автоматизовані є платіжними системами, які використовуються багатьма організаціями та приватними особами.

Б. воєнна /б. военная/ [military s.] — положення, що характеризує можливість забезпечення інтересів безпеки національної засобами збройного насильства. Зовнішній аспект б. в. відображає здатність нації протидіяти або стримувати вплив воєнної сили із-за кордону. Це досягається наявністю сучасних збройних сил, формуванням системи колективної та загальної безпеки, входженням до складу тих чи інших воєнно-політичних союзів. Внутрішній аспект б. в. зв'язаний з деструктивними проявами гонки озброєнь, мілітаризації суспільної свідомості, збільшенням політичної ролі армії у державі. Відмова від мілітаризації економіки й усіх сфер суспільного життя, деполітизація армії, пріоритет інтересів національної безпеки над інтересами військових ведуть до зміцнення б. в. держави.

Б. даних /б. данных/ [data s.] — 1) Стан даних, що зберігаються, обробляються й передаються, при якому неможливе їхнє випадкове або навмисне одержання, змінювання або знищення. 2) Властивість організації доступу до даних, що забезпечує їхнє оброблення за заздалегідь установленими правилами і тільки за ними. Під такими правилами найчастіше розуміють захист даних від несанкціонованого використан-

ня, розкривання, навмисного чи ненавмисного спотворення або руйнування. Б. д. досягається за рахунок застосування організаційних, етично-правових та технічних методів захисту.

Б. даних операційна /б. данных операционная/ [operational data s.] — захищеність даних від несанкціонованого, навмисного чи випадкового їхнього розкривання, модифікування або знищення під час оброблення даних.

Б. держави /б. государства/ [state s.] — положення, при якому державі не загрожує небезпека. Досягається наявністю ефективного механізму управління і координації діяльності політичних сил та суспільних груп, а також активних інститутів (органів) їхнього захисту.

Б. економічна /б. экономическая/ [economy s.] — положення, при якому економіці держави не загрожує небезпека. Характеризується рівнем розвитку виробничих сил та економічних відносин, спрямованих на реалізацію потреб особистості і суспільства, наявністю розвиненої інфраструктури та корисних копалин, кваліфікованої робочої сили і системи її підготовки, а також характером інтеграції у систему світових господарських зв'язків. Створення замкненого самодостатнього господарства в межах окремої країни або групи країн, спрямоване на максимальне обмеження імпорту, стимулювання експорту товарів і капіталу, а також економічна залежність руйнують системи б. е.

Б. інформації /б. информации/ [information s.] — стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації.

Б. інформаційна /б. информационная/ [information s.] — 1) Стан захищеності потреб в інформації особистості, суспільства і держави, при якому забезпечується їхнє існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх загроз інформаційних. В залежності від виду загроз інформаційній безпеці б. і. можна розглядати як забезпечення стану захищеності особистості, суспільства, держави від впливу неякісної інформації; інформації і інформаційних ресурсів від неправомірного впливу

сторонніх осіб; інформаційних прав і свобод людини і громадянина. 2) Стан захищеності середовища інформаційного суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави. 3) У праві інформаційному — одна із сторін розгляду відносин інформаційних у межах законодавства інформаційного з позицій захисту інтересів життєво важливих особистості, суспільства, держави та акцентування уваги на загрозах цим інтересам і на механізмах усунення або запобігання таким загрозам правовими методами.

Б. інформаційна держави (суспільства) /б. информационная государства (общества)/ [state information s.] — ступінь захищеності держави (суспільства) та стійкість основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи і т. ін.) відносно небезпечних (дестабілізуючих, деструктивних, що уражають державні інтереси і т. ін.) впливів інформаційних, причому як з упровадження, так і добування інформації. Б. і. д. визначається здатністю нейтралізувати такі впливи. В основу забезпечення Б. і. д. повинні бути покладені наступні принципи: законність, дотримання балансу інтересів особистості, суспільства і держави; взаємна відповідальність суб'єктів забезпечення інформаційної безпеки; інтеграція систем національної і міжнародної безпеки.

Б. інформаційна особистості /б. информационная личности/ [personal information s.] — захищеність психіки і свідомості людини від небезпечних впливів інформаційних: маніпулювання, дезінформування, спонукання до самогубства, образ і т. ін.

Б. інформаційно-психологічна /б. информационно-психологическая/ — стан захищеності психіки людини від деструктивного інформаційного впливу (впровадження деструктивної інформації у свідомість і (або) підсвідомість людини, що приводить до неадекватного сприйняття нею дійсності). Б. і.-п. є складовою частиною безпеки інформаційної і повинна займати особливе місце при її забезпеченні. Ця особливість визначається специфікою загроз і їхніх джерел у галузі б. і.-п., особливим характером принципів і завдань

при реалізації державної політики в цій галузі.

Б. інформаційної мережі /б. информационной сети/ [information network s.] — стан мережі інформаційної, при якому забезпечується безпека даних, які знаходяться в ній.

Б. інформаційної системи /б. информационной системы/ [information system s.] — стан системи інформаційної, при якому забезпечується безпека даних, які знаходяться в ній.

Б. комп'ютерних (обчислювальних) систем /б. компьютерных (вычислительных) систем/ [computer s.] — такий стан комп'ютерних систем, при якому забезпечується безпека даних, які обробляються ними.

Б. національна /б. национальная/ [national s.] — категорія політичної науки (політології), яка характеризує стан соціальних інститутів, який забезпечує їхню ефективну діяльність для підтримки оптимальних умов існування особистості та суспільства. Б. н. як категорія політології відображає зв'язок безпеки з нацією. В цьому плані вона характеризує стан нації як цілісної системи, що включає суспільні відносини і суспільну свідомість, інститути суспільства, їхня діяльність, які сприяють або шкодять реалізації національних інтересів у конкретній обстановці, що склалася історично. Суть б. н. — у протидії і компенсації будь-яких деструктивних заворушень, що формуються всередині суспільства або за його межами, які шкодять потребам життєдіяльності і розвитку суспільства та особистості. В б. н. виділяють три рівні безпеки: особистості, суспільства і держави. Їхнє місце і роль динамічні та визначаються характером суспільних відносин, політичним устроєм, ступенем внутрішніх та зовнішніх загроз. У критичні для нації періоди може домінувати безпека суспільства або держави. Як правило, авторитарні та тоталітарні режими, які постійно створюють такі критичні умови, висувають на передній план безпеку держави за рахунок безпеки особистості. Для демократичних суспільств найбільш цінні свобода та безпека особистості. Для них безпека держави і суспільства не є самоціллю, а функцією забезпечення свободи і безпеки особистості. В змістовному плані в б. н. розрізняють різноманітні галузі, структурні елементи, до яких, у першу чергу, відносяться: безпека

політична, економічна, воєнна, екологічна, інформаційна та безпека культурного розвитку нації.

Б. особистості /б. личности/ [personal s.] — положення, при якому особистості не загрожує небезпека. Б. о. полягає у формуванні комплексу правових і моральних норм, суспільних інститутів та організацій, які дозволили би їй розвивати й реалізовувати соціально значимі здібності й потреби, не зазнаючи при цьому протидії держави і суспільства.

Б. політична /б. политическая/ [political s.] — здатність і можливості нації та її державних інститутів самостійно вирішувати питання державного устрою, незалежно проводити внутрішню і зовнішню політику в інтересах особистості та суспільства. Б. п. передбачає наявність стійкого політичного суверенітету в межах міждержавних відносин і політичної стабільності суспільства, що досягається формуванням політичної системи, яка би забезпечувала баланс інтересів різноманітних соціальних груп з опорою на пріоритет особистості. Відсутність як першого, так і другого неминуче руйнує б. п. країни.

Б. ресурсів автоматизованої системи /б. ресурсов автоматизированной системы/ — стан системи автоматизованої, при якому забезпечується конфіденційність, цілісність і доступність компонентів системи. Конфіденційність компонента системи полягає у тому, що він доступний тільки тим суб'єктам доступу (користувачам, програмам, процесам), яким надані на це відповідні повноваження. Цілісність компонента передбачає, що він може бути модифікований тільки суб'єктом, що має на це відповідні права. Цілісність є гарантією коректності (незмінності, працездатності) компонента в будь-який момент часу. Доступність компонента означає, що суб'єкт, який має відповідні повноваження, може і будь-який час без особливих проблем одержати доступ до необхідного компонента (ресурсу).

Б. системи оброблення даних /б. системы обработки данных/ [data processing system s.] — технологічні та адміністративні охоронні заходи, що застосовуються в системі оброблення даних для захисту обладнання, програмного забезпечення та даних від несанкціонованого, навмисного чи випадкового моди-

фікування, розривання або руйнування.

Б. суб'єктів інформаційних відносин /б. субъектов информационных отношений/ — захищеність суб'єктів відносин інформаційних від нанесення їм матеріальних, моральних або інших збитків шляхом впливу на інформацію і (або) засоби її оброблення та передавання.

Б. суспільства /б. общества/ [society s.] — наявність суспільних інститутів, норм, розвинених форм суспільної свідомості, які дозволяють реалізувати права та свободи усіх груп населення і протистояти діям, що ведуть до розколу суспільства (у тому числі і зі сторони держави).

БИТВА /сражение/ [battle] — 1) Складова частина воєнної операції, сукупність найбільш важливих і напружених боїв і ударів, об'єднаних загальним замислом, що здійснюються певними угрупованнями військ (сил) і спрямованих на виконання одного оперативного завдання; форма бойових дій. 2) Уперта, наполеглива політична, господарська і т. ін. боротьба.

Б. інформаційна /с. информационное/ [information b.] — складова частина операції інформаційної, сукупність узгоджених і взаємопов'язаних за метою, завданнями, місцем і часом дій і ударів інформаційних, об'єднаних загальним замислом, які здійснюються спеціально виділеними силами і засобами та спрямовані для вирішення одного оперативного завдання боротьби інформаційної. В залежності від масштабу і виду інформаційної операції в ній може бути одна або декілька б. і., що здійснюються одночасно або послідовно.

БІГРАМА /биграмма/ [bigram] (лат. bi..., від bis — двічі і ...грама, від грец. $\gamma\rho\acute{\alpha}\mu\mu\alpha$ — літера, написання) — послідовність із двох символів алфавіту. Див. також поліграма.

БІЙ /бой/ [battle, combat, fight] — узгоджені за метою, місцем і часом удари, вогонь і маневр з'єднань, частин (кораблів), підрозділів із метою знищення (розгрому) противника, оволодіння важливими районами (рубежами) або утримання їх і виконання інших тактичних завдань в обмеженому районі протягом короткого проміжку часу.

БІНОКЛЬ /бинокль/ [binoculars] (франц. binocle, від лат. bini — два і oculum — око) — оптичний прилад, що складається з двох паралельних, з'єднаних між собою зорових труб. В залежності від оптичної схеми зорової труби бінокли поділяються на звичайні і призматичні.

Б. звичайний /б. обычный/ [simple b.] — бінокль, у якого оптичні осі об'єктива і окуляра зорової труби співпадають, а відстань між центрами об'єктивів і центрами окулярів зорових труб однакова і дорівнює середній відстані між зіницями очей спостерігача. Бінокли цього типу прості, мають високу світлосилу, але мале поле зору і не дозволяють встановлювати кутомірну сітку.

Б. панкратичний /б. панкратический/ [pancratic b.] (від грец. $\pi\tilde{\alpha}\nu$ — що у складних словах означає все, всеохоплюючий та $\kappa\rho\acute{\alpha}\tau\text{ø}\varsigma$ — сила) — бінокль, збільшення зорових труб якого плавно змінюється в значних межах (від 4 до 20 і більше). При цьому в оберненій пропорційній залежності змінюється величина поля зору. Такі бінокли найбільш зручні для спостереження, дозволяють здійснювати пошук об'єктів при великому полі зору, але малому збільшенні, а вивчення об'єкта — при великому збільшенні.

Б. призматичний /б. призматический/ [prism(atic) b.] — бінокль, у якого зорова труба складається з об'єктива, повернутого в бік об'єкта спостереження, системи призм, що обертають зображення, і окуляра об'єктива, повернутого до зіниці ока. В б. п. встановлюють кутомірну сітку у фокальній площині об'єктива. Зорові труби в п. б. шарнірно закріплені на загальній осі, що дозволяє підбирати відстань між окулярами за базою очей спостерігача. Об'єктиви і призми обертаючої системи закріплені в зорових трубах нерухомо, а окуляри можуть висуватися для встановлення за силою зору спостерігача. Для цього на окулярних трубах наносяться діоптрійні шкали. Щоб покращити спостереження при тумані, яскравому сонячному освітленні, на фоні снігу, на окуляри бінокля чіпляють жовто-зелені світлофільтри. В деяких біноклях для виявлення активних приладів інфрачервоних в нічний час застосовують спеціальний екран, чутливий до інфрачервоних променів.

БІОМЕТРІЯ /биометрия/ [biometric] — технологія вимірювання й аналізу людського тіла з метою його автентифікації.

БІОПОЛІТИКА /биополитика/ [biopolitics] (від грец. *βίφς* — життя і політика) — 1) Концепція, що дозволяє застосовувати біологічні методи, аналогії, в тому числі з частинами людського тіла, у вивченні політики і влади (наприклад, рука влади, мозок влади, її очі і вуха, серце держави і т. ін.). 2) Політика, влада, що враховує і застосовує у своїх цілях потенціал біологічних систем, психологічні і навіть моральні можливості людини, способи впливу на неї.

БІПОЛЯРНІСТЬ /биполярность/ [bipolarity] — поняття, яке вживалося в комунікативістиці для характеристики періоду холодної війни, коли в міжнародному політичному житті й у світовому просторі інформаційному існували два конфронтуючих полюси. Один був оплотом імперіалізму, інший — соціалізму. Після закінчення холодної війни відкрилися перспективи або однополюсного світу, внаслідок чого виникають загрози імперіалізму інформаційного і колоніалізму культурного, або багатополюсного світу.

БІТ /бит/ [bit] (від англ. binary — двійковий і digit — знак, цифра) — мінімальна одиниця кількості інформації в ЕОМ, що дорівнює одному двійковому розряду.

Б. вилучення /б. извлечения/ [deletion b.] — біт, що додається до запису і призначений для зазначення того, чи вилучений даний запис.

Б. достовірності /б. достоверности/ [validity b.] — двійковий розряд, що додається до слова в пам'яті ЕОМ для зазначення достовірності інформації.

Б. захисту /б. защиты/ [protection b.] — двійковий розряд у ключі захисту пам'яті ЕОМ, що встановлює захист відповідного блоку пам'яті від записування або від читання та записування.

Б. змін /б. изменений/ [change b.] — двійковий розряд, який додається до блоку даних для зазначення

того, що в блоці здійснюється зміна інформації.

Б. керування доступом /б. управления доступом/ [access b.] — один або декілька бітів ключа захисту пам'яті, що порівнюється з ключем захисту при зверненні до відповідного блоку пам'яті з метою організації її захисту.

Б. контрольний /Б. контрольный/ [parity b.] — біт, що додається до даних для контролю їхньої правильності таким чином, щоб сума двійкових одиниць, які складають дані, включаючи одиницю Б. к., завжди була парною (або завжди непарною).

Б. контролю на парність /б. контроля на четность/ [parity b.] — те ж, що біт контрольний.

Б. маски /б. маски/ [mask b.] — сполучення бітів, що встановлюються в нульове або одиничне значення для дозволу чи заборони певних операцій або зміни вмісту поля.

Б. парності /б. четности/ [parity b.] — те ж, що біт контрольний.

БІХЕВІОРИЗМ /бихевиоризм/[behaviorism] (від англ. behaviour — поведінка) — напрям психологічних досліджень. Вивчає поведінку людей в різних життєвих ситуаціях як сукупність відповідних реакцій на впливи (стимули) зовнішнього середовища. У комунікативістиці концепції й методи б. використовуються для вивчення й моделювання різноманітних типів активації і загального стану аудиторії, в залежності від якого змінюється характер і обсяг інформації й відношення, то тих чи інших засобів масової інформації. Методи б. використовуються також і для визначення ефективності форм керування мас-медіа.

БЛОК /блок/ [block] (англ. block) — 1) Сукупність взаємопов'язаних елементів та вузлів пристрою, що виконують певну функцію. 2) Фізичний запис на носії даних. 3) Сукупність даних, що передаються по лінії зв'язку.

Б. пам'яті ключів захисту /б. памяти ключей защиты/ [key b.] — спеціальний надшвидкодіючий

запам'ятовуючий пристрій малої ємності з прямим доступом, призначений для збереження ключів захисту.

БЛОКАДА /блокада/ [blockade] (від франц. bloquer — перекрити доступ) — воєнна, політична або економічна ізоляція чи оточення держави (або частини її, групи держав, їхніх збройних сил), насильницьке порушення її зовнішніх зв'язків із метою змусити виконати вимоги організаторів б.

Б. воєнна /б. военная/ — спосіб воєнних дій, що полягає в ізоляції (порушення зовнішніх зв'язків) ворожої держави, великого угруповання військ, міста, порту та інших об'єктів. Метою б. в. можуть бути: підривання воєнно-економічної могутності, виснаження угруповання противника з наступним його розгромом або примушенням до капітуляції і т. ін. В. б. може бути повною або частковою, сухопутною, морською, повітряною або змішаною. В залежності від масштабу і змісту завдань, кількості залучених сил та засобів в. б. поділяється на стратегічну і оперативну. Б. в., що проводиться в тактичному масштабі, називається блокуванням.

Б. інформаційна /б. информационная/ — узгоджене за завданнями, місцем і часом застосування сил і засобів із метою найбільш повного зниження можливостей противника з одержання і використання інформації, необхідної для ефективного ведення операцій (бойових дій). Одним з основних способів досягнення мети б. і. є блокування радіоелектронне.

БЛОКУВАННЯ /блокирование/ [blocking] — 1) Ізоляція будь-якого об'єкта з метою наступного його знищення або захоплення при веденні бойових дій тактичного масштабу. 2) Заборона на виконання наступних операцій до завершення поточної операції; механізм організації контрольованого доступу до спільно використовуваного ресурсу. 3) Див. замок.

Б. даних /б. данных/ [data interlock] — захист файла або його частини (блока, запису) шляхом заборони доступу до нього всіх користувачів, за винятком одного.

Б. інформації /б. информации/ [information interlock] — дії, наслідком яких є припинення доступу до

інформації користувачів інформаційної системи.

Б. радіоелектронне /б. радиоэлектронное/ [electronic b.] — узгоджений вплив засобами придушення радіоелектронного і функціонального ураження на технічні елементи систем розвідки і канали передавання інформації.

БОМБА /бомба/ [bomb] (франц. bombe, від лат. bombus — шум, гул, з грец. *βόμβος* — гуркіт) — розривний снаряд.

Б. логічна /б. логическая/ [logic b.] — закладка програмна, що здійснює зловмисні дії при виконанні ряду певних логічних умов. Вноситься таємно в програмне забезпечення ЕОМ і виконується внаслідок збігу певних обставин або у визначений момент часу з метою спотворення, знищення, модифікування або викрадення даних.

Б. часова /б. временная/ [time b.] — різновид бомби логічної, яка спрацьовує у певний (визначений) момент часу.

БОРОТЬБА /борьба/ [struggle] — 1) Активне противенство, зіткнення між протилежними соціальними групами, течіями в суспільстві і т. ін., протистояння. 2) Діяльність, що має на меті подолати або знищити кого-, що-небудь. 3) Діяльність, скерована на створення, досягнення чого-небудь.

Б. з комп'ютерною злочинністю /б. с компьютерной преступностью/ [computer crime s.] — профілактика та попередження злочинів комп'ютерних. Б. з к. з. передбачає: створення, сертифікацію, ліцензування і впровадження необхідних засобів технічного та програмного захисту інформації; створення спеціалізованих організаційних структур, завданням яких є забезпечення надійного функціонування засобів захисту, засобів генерації ключів та паролів, їхнього розподілу, контролю за використанням, зміною та знищенням; підготовку кваліфікованих кадрів для правоохоронних органів, а саме для органів дізнання та розшуку,

судів, служб безпеки комп'ютерних та телекомунікаційних мереж і систем.

Б. збройна /б. вооруженная/ [armed s.] — процес протиборства збройних сил воюючих держав. Вона є головною формою діяльності держави під час війни. Збройні сили використовуються державами для здійснення своєї політики, для продовження її в особливих умовах. Поряд з діями збройних сил, в ході війни ведеться боротьба економічна, дипломатична, ідеологічна і інформаційна. Всі ці форми боротьби, так же як і б. з., підпорядковуються політиці воюючих держав і спрямовуються нею.

Б. збройна фізична /б. вооруженная физическая/ — вид боротьби збройної, в якій використовуються переважно фізичні форми енергії для ураження противника і захисту від фізичного ураження противника своїх військ, зброї, військової техніки, об'єктів і середовища. В майбутніх війнах для фізичного ураження може знайти широке застосування енергія усіх достатньо відомих форм руху матерії — кінетичної; акустичної; електромагнітної; енергії елементарних часток; ядерної енергії; теплової і т.ін. Тобто, в залежності від форм енергії, у війнах і збройній боротьбі майбутнього у відповідних озброєннях будуть використовуватися різноманітні види кінематичного, акустичного, електромагнітного, радіаційного і теплового видів впливів.

Б. інформаційна /б. информационная/ [information s.] — 1) Боротьба з використанням спеціальних способів і засобів для впливу на сферу інформаційну (середовище) конфронтуючої сторони, а також для захисту власної інформаційної сфери в інтересах досягнення поставленої мети. Б. і. може бути як самостійним видом, так і складовою частиною будь-якого іншого різновиду боротьби (збройної, ідеологічної, економічної і т. ін.). Вона ведеться постійно, як в мирний, так і у воєнний час. Масштаби б. і. настільки великі, що її підготовка і ведення повинні носити плановий, систематичний характер, заснований на глибоких знаннях законів і закономірностей інформаційної боротьби. 2) Форма забезпечення інформаційної безпеки від загроз інформаційних навмисних. Ведеться державними органами інформаційної безпеки з формуваннями, що мають різноманітний (суспільний) стан (фізичні особи, юридичні особи, суб'єкти міжнародного права) і зловмисно створюють інформаційні загрози життєво важливим інтересам особистості, суспільства

і держави. Б. і. включає комплекс заходів забезпечення інформаційного, захисту інформаційного і протидії інформаційної, що здійснюються за єдиним замислом і планом з метою захоплення і утримання переваги інформаційної.

Б. політична /б. политическая/ [political s.] — змагання, суперництво, сутичка в політичному житті і діяльності конфронтуючих осіб, сил, партій, рухів, які відстоюють свої політичні погляди, позиції і устремління. Вважається, що б. п. повинна вестися цивілізованими прийомами і методами в рамках існуючого законодавства.

Б. радіоелектронна (РЕБ) /б. радиоэлектронная (РЭБ)/ [radio (electronic) warfare] — комплекс взаємопов'язаних заходів та дій з виявлення і подальшого придушення радіоелектронного або знищення засобів радіоелектронних та систем противника, а також відповідного захисту своїх радіоелектронних засобів та систем.

БРАНДМАУЕР /брандмауэр/ [brandmaurer] (нім. Brandmauer, від Brand — пожежа і Mauer — стіна) — 1) Вогнестійка капітальна стіна, що запобігає поширенню пожежі. 2) Метод (або принцип) захисту надійної мережі від загроз, що надходять від інших (менш надійних) мереж чи систем, за допомогою централізації доступу до мережі та контролю за ним апаратно-програмними засобами. Цей принцип захисту можна реалізувати за допомогою різних засобів таких як фільтруючий маршрутизатор, міжмережний екран, бастіонний вузол, подвійний шлюз, фільтруючий шлюз, проксі-шлюз, комбінований шлюз, ізольована підмережа, тощо. Іноді термін брандмауер використовують як синонім файерволу.

БРАУЗЕР /браузер/ [browser] (від англ. browse — переглядати) — програма-клієнт, що дає можливість користувачеві переглядати Web-сторінки, копіювати файли і т.ін. з IP-мереж. Найбільше популярні Microsoft Internet Explorer і Netscape Navigator.

БРОШУРА /брошюра/ [pamphlet] (франц. brochure) — книжкове видання обсягом більше 4, але не біль-

ше 48 сторінок. Засіб впливу психологічного друкованими засобами. Перевага над листівками в тому, що в них більше місця для тексту й ілюстрацій. В б. легше роз'яснювати неспроможність аргументів противника (докладно проаналізувати й прокоментувати їх). Б. особливо зручна для викриття таких тезисів, які підкріплені доводами формальної логіки або невірними статистичними даними, так як у даному випадку необхідно спростовувати пункт за пунктом, цифру за цифрою.

В

ВАКЦИНА /вакцина/ [vaccine] (лат. vaccinus — коров'ячий, від vacca — корова) — 1) Препарат, виготовлений з ослаблених чи вбитих мікроорганізмів і вірусів або з продуктів їхньої життєдіяльності. Застосовують для запобігання інфекційним хворобам та лікування цих хвороб. 2) В обчислювальній техніці — антивірус, заздалегідь введений (імплантований) у програму, яку захищають.

ВАРІООБ'ЄКТИВ /вариообъектив/ [auto-zoom lens, variofocal lens] (від лат. vario — змінюю і об'єктив) — об'єктив, створений за єдиною оптичною схемою, в якому зміна фокусної відстані здійснюється безперервним переміщенням однієї або декількох компонент уздовж оптичної осі.

ВБУДОВУВАННЯ /встраивание/ [add-in] — процес уставляння, приладжування якогось предмета, деталі і т.ін. усередину чого-небудь.

В. повідомлення /в. сообщения/ [embedded message] — процес стеганографічного перетворення контейнера і секретного повідомлення.

ВЕРБУВАННЯ /вербовка/ [enlistment, recruiting, recruitment] (від нім. werben — набирати, шукати) — залучення окремих осіб у якості агентів таємних.

В. в Інтернеті /в. в Интернете/ — залучення окремих користувачів Інтернету в якості агентів таємних.

ВЕРИФІКАЦІЯ /верификация/ [verification] (від лат. verus — істинний і лат. ... ficatio, від facio — роблю)

— 1) Процес перевірки достовірності інформації шляхом вивчення її джерел та їхньої надійності. 2) В програмуванні — доказ правильності програми. 3) Певна сукупність вимог із захисту засобів обчислювальної техніки від доступу несанкціонованого до інформації.

ВЗАЄМОДІЯ /взаимодействие/ [interaction, cooperation, coordination] — співдія, співдіяння. Взаємний зв'язок між предметами у дії, а також погоджена дія між ким-, чим-небудь.

В. вірусів /в. вирусов/ [virus i.] — модифікування кодів або блокування одного вірусу комп'ютерного іншим при одночасному знаходженні їх у пам'яті оперативній. В більш широкому розумінні — зміна функціонування одного комп'ютерного вірусу під впливом іншого.

ВИБІРКА /выборка/ [sample] — вибір елементів із деякої сукупності для дослідження таким чином, щоб його результати дали інформацію про аналогічні елементи, які не увійшли до вибірки.

В. аудиторська /в. аудиторская/ [audit s.] — в обчислювальній техніці — множина зроблених у хронологічному порядкові реєстраційних записів про події, пов'язані із зміною стану системи обчислювальної.

ВИБІРКОВІСТЬ /избирательность/ [selectivity] — здатність здійснювати відбір.

В. радіоприймача /и. радиоприемника/ [radio receiver s.] — здатність радіоприймача виділяти корисний сигнал із сигналів різноманітних частот, що приймаються антеною. В. р. оцінюється двома основними показниками: шириною смуги пропускання і коефіцієнтом прямокутності амплітудно-частотної характеристики радіоприймача, реальна форма якої має дзвонуватий вигляд.

ВИБУХ /взрыв/ [explosion] — 1) Миттєве руйнування чого-небудь, що супроводжується утворенням дуже нагрітих (високотемпературних), із високим тиском газів; звук, що супроводжує таке руйнування. 2) Переносно — раптовий сильний, гучний прояв чого-небудь.

В. інформаційний /в. информационный/ [information e.] — стрімке зростання загального обсягу ін-

формації, що створюється в межах будь-якої галузі діяльності або суспільства у цілому на певному етапі їхнього розвитку.

ВИКОРИСТАННЯ /использование/ — застосування, вживання чого-небудь із користю, користування чимось.

В. об'єкта повторне /и. объекта повторное/ [object reuse] — послуга безпеки, що забезпечує очищення пам'яті і призупинення дії повноважень щодо розділюваного об'єкта, який раніше використовувався одним користувачем або процесом, перед наданням його іншому користувачеві або процесу.

ВИМОГИ /требования/ [requirements] — норми, правила, яким хто-, що-небудь повинні підлягати.

В. безпеки /т. безопасности/ [security r.] — в "критеріях Загальних" — вимоги безпеки функціональні і вимоги гарантій безпеки.

В. безпеки функціональні (ФВБ) /т. безопасности функциональные (ФТБ)/ [security functional r.]— вимоги безпеки, які в "критеріях Загальних" регламентують функціонування компонентів продукту інформаційних технологій, що забезпечують безпеку, і визначають можливості засобів захисту. ФВБ декларуються у вигляді добре розробленої формальної структури. Набір ФВБ узагальнює усі існуючі раніше стандарти інформаційної безпеки і відрізняється всеосяжною повнотою й найдокладнішою деталізацією. ФВБ розділені на 11 класів ФВБ і 67 розділів ФВБ. Опис кожної вимоги будується за наступною схемою: назва [component identification], що містить унікальну назву вимоги, яка використовується для посилань на неї з профілю і проекту захисту; зміст вимоги [functional elements], де проводиться основна думка про те, що функціональний склад вимоги "Загальні критерії" дозволяють використовувати тільки без змін, що забезпечує їхню стандартизацію; сполучені вимоги [dependencies], що є необов'язковим пунктом, який містить список вимог різних розділів і класів, виконання яких розглядається як необхідна попередня умова

для реалізації даної вимоги.

В. гарантій безпеки (ВГБ) /т. гарантий безопасности (ТГБ)/ [security assurance r.] — вимоги безпеки, які в "критеріях Загальних" представляють собою характеристику продукту інформаційних технологій, що показує, наскільки ефективно забезпечується заявлений рівень безпеки, а також ступінь коректності реалізації засобів захисту. Як і вимоги безпеки функціональні, ВГБ детально структуровані та регламентують усі етапи проектування, створення й експлуатації IT-продукту дуже детально. Структура вимог гарантій аналогічна функціональним вимогам. Вона має 7 класів ВГБ і 26 розділів ВГБ. Структура в. г. б. складається з наступних елементів: назва вимоги [component identification]; мета [objectives]; опис застосування [application notes]; сполучені вимоги [dependencies]; елементи вимоги [assurance element]. Вимоги гарантій використовуються в ході аналізу кваліфікаційного IT-продукту відповідного рівня гарантій.

ВИПИТУВАННЯ /выспрашивание/ [questioning] — спосіб одержання інформації від людини шляхом задавання їй питань. Існують різноманітні способи випитування: від прихованого випитування до випитування під тортурами.

В. під тортурами /в. под пыткой/ [put to the question] — спосіб випитування, розрахований на швидке одержання інформації. Застосовується при відсутності часу на підготовку і проведення випитування прихованого. Найчастіше використовується кримінальними елементами.

В. приховане /в. скрытое/ [hiding q.] — випитування шляхом задавання невинних питань в будь-якій невимушеній обстановці (у ході бесіди на конференції, презентації, анкетування і т. ін.), відповіді на які для фахівця містять інформацію секретну або конфіденційну. Застосовується в усній або письмовій формі.

ВИПРОМІНЮВАННЯ /излучение/ [emission] — виділення променями теплової, електромагнітної та іншої енергії.

В. електромагнітне /и. электромагнитное/ [electromagnetic e.] — процес випромінювання хвиль еле-

ктромагнітних.

В. і наведення електромагнітні побічні (ПЕМВН) /и. и наводки электромагнитные побочные (ПЭМИН)/ [spurious elektromagnetic r. and breakthrough] — 1) Випромінювання електромагнітне і наведення паразитні, що виникають при функціонуванні будь-яких радіоелектронних і електричних пристроїв та приладів і утворюють джерела небезпечних сигналів, які можуть містити інформацію, що потребує захисту. 2) В обчислювальних мережах — електромагнітне випромінювання засобів мікропроцесорної та обчислювальної техніки, створення якого не є призначенням цих засобів, але яке має місце в процесі їхнього функціонування і може бути носієм інформації, зокрема, про процес оброблення даних. Здійснення реєстрації цієї інформації розглядається як загроза.

В. інфрачервоне /и. инфракрасное/ [InfraRed (IR, calorific e.)] — випромінювання оптичне, що характеризується довжинами хвиль, які розташовані в діапазоні $7,6 \cdot 10^{-7}$ — $2 \cdot 10^{-3}$ м.

В. немодульоване /и. немодулированное/ [unmodulated e.] — випромінювання, що не змінюється в часі за період його вимірювання. Як правило в інфрачервоній техніці рівень п. н. не є об'єктом вимірювання. При цьому постійну складову потоку випромінювання інфрачервоного називають фоном.

В. оптичне /и. оптическое/ [optical e.] — випромінювання електромагнітне, що характеризується довжинами хвиль, які розташовані в діапазоні $5 \cdot 10^{-9}$ — $2 \cdot 10^{-3}$ м. У зазначеному діапазоні електромагнітні хвилі найефективніше визначаються оптичними методами, для яких характерне формування керованих потоків електромагнітних хвиль за допомогою оптичних систем.

В. радіочастотне /и. радиочастотное/ [radio frequency e.] — електромагнітні коливання (хвилі) в діапазоні радіочастот, що поширюються (випромінюються) в просторі.

В. рівноважне /и. равновесное/ [balance e.] — випромінювання електромагнітне, що випромінюється

фізичною системою, яка знаходиться в термодинамічній рівновазі.

В. ультрафіолетове /и. ультрафиолетовое/ [ultraviolet e.] — оптичне випромінювання, що характеризується довжинами хвиль, які розташовані в діапазоні $5 \cdot 10^{-9} - 4 \cdot 10^{-7}$ м.

ВИПРОМІНЮВАЧ /излучатель/[radiator, emitter] — 1) Пристрій, за допомогою якого здійснюється випромінювання. 2) Випромінюючий елемент антени, зв'язаний з фідером.

В. небезпечних високочастотних сигналів /и. опасных высокочастотных сигналов/ [high-frequency compromising source emission, high-frequency tell-tale source emission] — джерела побічних високочастотних коливань, до яких відносяться: високочастотні генератори, що входять до складу багатьох радіотехнічних засобів; підсилювальні каскади, в яких при певних умовах виникають паразитні високочастотні коливання; нелінійні елементи, на які подаються гармонічні високочастотні коливання і електричні сигнали з мовною інформацією. У результаті акустоелектричних перетворень або інших інформаційних впливів на джерела побічних коливань (модуляції) модульовані коливання стають небезпечними сигналами, що можуть бути прийняті за межами зони контрольованої. Високочастотні коливання створюються не тільки функціональними або паразитними генераторами радіоелектронних засобів, але можуть бути підведені до них зловмисниками від зовнішнього генератора. Численні небезпечні високочастотні сигнали створюють працюючі ПЕОМ, особливо ті, що розташовані в пластмасових неметалізованих корпусах. Їхнє випромінювання має широкий діапазон: від одиниць до сотень МГц. Найбільш потужними інформативними джерелами електромагнітного випромінювання є відеопідсилювач і електронно-променева трубка монітора.

В. небезпечних низькочастотних сигналів /и. опасных низкочастотных сигналов/ [low-frequency compromising source emission, low-frequency tell-tale source emission] — джерела витоку інформації конфіденційної в звуковому діапазоні частот, що створюються при протіканні струмопроводами радіозасобів (проводами індуктивностей, монтажними і з'єднувальними проводами, доріжками друкованих плат) електричного струму й виникненні при цьому радіовипромінювання. Джерелами небезпечних низькочастотних

сигналів можуть бути телефонні апарати, пристрої гучномовного зв'язку, підсилювачі потужності, аудіо- і відеомагнітофони і т. ін.

ВИТІК /утечка/ [leakage] — процес виходу будь-чого з чого-небудь, з-під чогось назовні.

В. інформації /у. информации/ [information l.] — 1) Несанкціонований процес перенесення інформації від джерела до зловмисника. В. і. є можливим шляхом її розголошення людьми, втрати ними носіїв з інформацією, перенесення інформації за допомогою випромінювання, потоків елементарних часток, речовин в газоподібному, рідкому або твердому стані. В. і. у порівнянні з утратою (викраденням) матеріальних об'єктів має ряд особливостей, які необхідно враховувати при організації захисту інформації: в. і. може здійснюватися тільки при попаданні її до зацікавленого в ній несанкціонованого одержувача (зловмисника); при в. і. здійснюється її тиражування, яке не змінює характеристики носія інформації; ціна інформації при її витоку зменшується за рахунок тиражування; факт витоку інформації, як правило, виявляється через деякий час, за наслідками витоку, коли заходи забезпечення її безпеки можуть виявитися неефективними. В. і. здійснюється каналами витоку. 2) Просочування в засоби масової інформації відомостей із закритих або малодоступних джерел. Ці відомості можуть або слугувати на благо суспільним інтересам, або стати засобом маніпулювання суспільною думкою.

ВИЯВЛЕННЯ /обнаружение/ [detection, discovery, finding] — розшукування, знаходження, віднаходження.

В. несанкціонованих дій в мережі обміну інформацією /о. несанкционированных действий в сетях обмена информацией/ — один з основних аспектів забезпечення переваги над противником в інформаційній війні, що полягає в збиранні та підготовці відомостей про несанкціонований доступ для реалізації заходів протидії інформаційної. Одночасно проводяться заходи, спрямовані на зменшення часу безконтрольної присутності противника в мережі обміну інформацією з вирішенням завдання реагування простого та

протидії інтелектуальної.

В. об'єкта розвідки /о. объекта разведки/ [intelligence object d.] — виділення об'єкта розвідки (джерел і носіїв інформації, джерел сигналів) на фоні інших об'єктів шляхом пошуку за демаскуючими ознаками. Основу процесу виявлення складає процедура ідентифікації — порівняння поточних ознакових структур, що формуються в процесі пошуку, з еталонною ознаковою структурою об'єкта розвідки.

В. працюючого диктофону /о. работающего диктофона/ [bug(dictophone) d.] — установлення факту несанкціонованого (прихованого) запису мовної інформації на диктофон. Враховуючи конструктивні особливості диктофонів, призначених для прихованого запису, вони можуть бути виявлені за допомогою металодетекторів, або із застосуванням спеціальних виявників шляхом виявлення і аналізу змін параметрів полів, вимірюваних в місці розташування зловмисника. Накопичуючи зміни, вдається виділити регулярне поле двигуна диктофона на фоні навіть більш потужних випадкових полів інших джерел.

ВИЯВНИК /обнаружитель/ [detector] — пристрій для виявлення чого-небудь, а також узагалі те, за допомогою чого можна що-небудь точно визначити, встановити.

В. поля /о. поля/ [field d. (electromagnetic field d.)] — засоби радіоконтролю приміщень, призначені для виявлення радіовипромінювання пристроїв закладних в безпосередній близькості від джерела випромінювання. Найпростіші з них індикатори поля, які світловим або звуковим сигналом інформують оператора про наявність в місці розташування електромагнітного поля з напруженістю, вищою за фонову. Більш складні в. п. — частотоміри — забезпечують, крім того, вимірювання частоти коливань поля.

В. пустот /о. пустот/ — засоби пошуку невипромінюючих закладних пристроїв, що дозволяють виявляти можливі місця встановлення закладних пристроїв в пустотах стін або інших дерев'яних та цегляних конструкціях. Виявляти пустоти можуть різноманітні ультразвукові прилади, в тому числі медичного призначення, і спеціальні в. п. Спеціальні технічні засоби для виявлення пустот використовують: відмінності в

значеннях діелектричної проникності середовища і пустоти; різницю в значеннях теплопровідності повітря і суцільного середовища. Ефективним засобом виявлення пустот у стінах, нагрітих на декілька градусів вище температури повітря в приміщенні, є тепловізори.

ВІДБИВАЧ /отражатель/ [reflector] — пристрій або природна перепона, що змінює напрямок або інтенсивність світлових або теплових променів, електромагнітних хвиль, ядерних часток, а також твердих пружних тіл.

В. дипольні /о. дипольные/ [dipole r.] — радіовідбивачі, призначені для радіолокаційного маскування повітряних об'єктів. Д. в. являють собою смужки металізованого паперу або алюмінієвої фольги, металізовані скляні або нейлонові волокна, що розкидаються в зоні розташування об'єкта, який підлягає захисту. Довжина диполів і їхня товщина вибираються так, щоб забезпечити ефективне розсіювання радіохвиль по можливості у більш широкому діапазоні частот. В. д. упаковуються в пачки з десятків і сотень одиниць і при викиданні з літака у повітря створюють хмару відбивачів, що помалу опускається на землю. Відбиті від них сигнали спостерігаються на екрані РЛС у вигляді множини яскравих точок, що маскують відбитий від літака сигнал. Якщо послідовно скидати достатньо велику кількість пачок, то на екрані РЛС створюються засвітлені смуги, в яких важко виявити повітряні об'єкти.

В. кутиковий /о. уголковый/ [angle r., corner r.] — радіовідбивач, що складається з жорстко зв'язаних між собою перпендикулярних площин. Найважливішою властивістю в. к. є те, що значна частка енергії хвилі, що падає на нього в межах достатньо великого кута (біля 80 градусів), відбивається назад в бік опромінюючої РЛС. Тому в. к. навіть невеликих розмірів мають значну поверхню розсіювання ефективну. В. к. з трьох граней з розмірами 0,5 м при довжині хвилі РЛС 3 см створює ЕПР 290 м^2 (ЕПР літака-бомбардувальника В-52 — біля 100 м^2).

В. лінзові /о. линзовые/ [lens r.] — радіовідбивачі, що створюються на основі лінз Люнеберга. Лінза являє собою кулю із шарами матеріалів, що мають різноманітні значення діелектричної проникності. При

такій конструкції електромагнітні хвилі фокусуються на внутрішній поверхні кулі, покритої металевою радіовідбиваючою плівкою-екраном. Ширина діаграми розсіювання лінзи залежить від розмірів екрануючої поверхні і сягає 140 градусів. Л. в. діаметром 60 см і масою 40 кг на довжині хвилі λ=10 см має ЕПР більшу за 150 м^2, на λ=3 см більшу за 1800 м^2.

В.-антенна решітка /о.-антенная решетка/ — радіовідбивач, що має декілька горизонтальних і вертикальних рядів відбивачів дипольних, розташованих в одній площині на відстані чверті робочої довжини хвилі від відбиваючого екрана — металевої пластини. Дипольні пари розташовані дзеркально відносно центра екрана, з'єднуються між собою відрізками кабелю коаксіального або радіохвилеводу. Відбивні властивості в.-а. р. максимальні в напрямку, перпендикулярному її площині. При орієнтуванні диполів у певному порядкові створюється можливість забезпечення відбивних властивостей решітки незалежно від поляризації радіохвиль, що падають на неї. В деяких конструкціях в.-а. р. замість диполів застосовуються плоскі спіралі, нанесення яких на діелектричний лист здійснюється методом друкованих плат.

ВІДЕО... /видео.../ [video...] (від лат. video — дивлюся, бачу) — в складних словах указує на належність поняття до зображення телевізійних, радіолокаційних та інших складних електричних сигналів на екрані електронно-променевої трубки.

В. інтерактивне /в. интерактивное/ [interactive v.] — інтеграція відео- і комп'ютерної технології. Користувач здійснює вплив на розвиток сюжету.

ВІДЕОЗОБРАЖЕННЯ /видеоизображение/ [video image] (від відео... і зображення) — зображення, представлене сигналом електричним, наприклад, стандартним сигналом телевізійним.

ВІДЕОКАМЕРА /видеокамера/ [video camera, camera-recorder] (від відео... і камера) — пристрій для перетворення зображення у відеосигнал. Див. також камера телевізійна.

ВІДЕОПЕРЕХОПЛЕННЯ /видеоперехват/ (від відео... і перехоплення) — добування інформації шля-

хом застосування різноманітної відеоптичної техніки. В. має два різновиди: відеоперехоплення фізичне і відеоперехоплення електронне.

В. електронне /в. электронный/ — відеоперехоплення, що здійснюється за допомогою спеціальної відеоптичної техніки, що передбачає застосування різноманітних каналів зв'язку як постійних, так і таких, встановлюються тимчасово. Передавальний пристрій в даному випадку знаходиться на об'єкті, а приймальний — поза об'єктом. Для е. в. може використовуватися наступна спеціальна техніка: спеціальні відеомагнітофони, в тому числі з довготривалим записом; обладнання скритого відеознімання, включаючи цифрові електронні відеокамери, що мають повну адаптацію з комп'ютерними системами і різноманітними лініями зв'язку; телекомунікаційне обладнання з радіопередавальною апаратурою і різноманітними лініями зв'язку; прилади нічного бачення.

В. фізичне /в. физический/ — відеоперехоплення, що здійснюється за допомогою різноманітних засобів відеоапаратури, наприклад, підзорної труби, бінокля, приладу нічного бачення, оптичного прицілу, відеофотоапаратури з різноманітними оптичними насадками (об'єктивами) і т.ін. При. в. ф засоби відеоапаратури знаходяться безпосередньо в руках у особи, що здійснює відеоперехоплення.

ВІДЕОСИГНАЛ /видеосигнал/ [videosignal] (від відео... і сигнал) — сигнал електричний, призначений для створення зображення.

ВІДЕОТЕКС /видеотекс/ [videotex] (від відео... і англ. tex) — система доступу до баз даних через мережі зв'язку, яка забезпечує передавання текстів і зображень. Як приймач даних може використовуватися ПЕОМ або побутовий телевізор із спеціальним пристроєм.

ВІДКІТ /откат/ [rollback] — послуга безпеки, що забезпечує повернення об'єкта системи комп'ютерної до відомого попереднього стану після виконання над об'єктом певної операції або серії операцій.

ВІДМОВА /отказ/ [fault, failure] — утрата здатності системи (системи комп'ютерної) або її компоненти

виконувати певну функцію.

В. аварійна /о. аварийный/ [crash] — відмова системи, що вимагає для відновлення її нормального функціонування втручання оператора, а інколи і ремонтних робіт.

В. в доступі законному користувачеві /о. в доступе законному пользователю/ [authorization user rejection] — загроза, яка полягає у відмові системи захисту надання доступу до ресурсів інформаційно-обчислювальної системи користувачеві, який має на це законне право.

В. в обслуговуванні /о. в обслуживании/ [denial of service] — будь-яка дія або послідовність дій, що призводять будь-яку частину (компоненту) системи до виходу з ладу; нездатність системи виконувати свої функції (надавати декларовані послуги) внаслідок виходу з ладу якої-небудь компоненти або інших причин.

В. від авторства /о. от авторства/ [repudiation of origin] — заперечення причетності до утворення або передавання якого-небудь документа чи повідомлення.

В. від одержання /о. от получения/ [repudiation of receipt] — заперечення причетності до одержання якого-небудь документа чи повідомлення.

ВІДНОВЛЕННЯ /восстановление/ [recovery] — 1) Повернення до вихідного значення або повернення до нормального функціонування системи після збою або відмови. 2) Процес, за допомогою якого станція передавання даних розв'язує конфлікт або виправляє помилки, що виникають при передаванні даних.

В. баз даних /в. баз данных/ [database r.] — відтворення вмісту бази даних за резервною копією, що виконується у випадку машинних збоїв або програмних помилок для підтримання цілісності даних. Методи та засоби відновлення: копіювання, рестарт із контрольної точки, ведення журналу системного.

В. даних /в. данных/ [data r.] — процес відтворення даних із носія, що містить захищену копію даних,

на носій-оригінал у випадку порушення на ньому цілісності даних.

В. ключа /в. ключа/ [key r.] — процес одержання ключа арбітром для перетворення потоку зашифрованого тексту в його розшифрований еквівалент.

В. після відмови /в. после отказа/ [failure r.] — процедура поновлення роботи обчислювальної системи після відмови, що виключає вироблення системою неправильних результатів.

ВІДНОСИНИ /отношения/ [relations] — стосунки, зв'язки, взаємини між ким-небудь, контакти.

В. інформаційні /о. информационные/ [information r.] — 1) Відносини, що виникають при здійсненні процесів інформаційних. Основним предметом, із приводу якого або у зв'язку з яким виникають в. і., є інформація в усіх її видах і формах. В. і. людино-машинних об'єктів і систем в інформаційних середовищах пропонується розглядати як загальнотеоретичні (внутрішні і зовнішні) або прикладні. Серед прикладних виділяються два основні напрямки відносин — відносини інформаційної ізоляції і відносини інформаційної взаємодії. 2) Відносини (взаємодія) між діячами інформаційними. З інформатики відомо сім рівнів такої взаємодії в системах інформаційних: фізичний, канальний, мережний, транспортний, сеансовий, представницький, прикладний. В. і. бувають внутрішніми і зовнішніми. За характером інформаційного носія і. в. можуть бути розділені на три типи: об'єкт-об'єкт, суб'єкт-суб'єкт, суб'єкт-об'єкт. За метою функціонування діячів в умовах коаліцій або конфліктів в. і. розділяють на відносини інформаційні співробітництва і суперництва, дезорієнтування, дезінформування і дезорганізації з можливістю перетворення суб'єкта в об'єкт і навпаки. Сукупність конфліктних відносин суперництва, що організуються стороною-суб'єктом із метою зробити іншу сторону об'єктом бажаного управління у своїх інтересах, означає боротьбу інформаційну.

В. інформаційні внутрішні /о. внутренние информационные/ [internal information affairs] — відносини інформаційні в межах систем інформаційних.

В. інформаційні дезорієнтування /о. информационные дезориентирования/ — відносини інформа-

ційні сторін, коли дії однієї сторони збільшують інформаційну невизначеність іншої сторони. Причиною інформаційного дезорієнтування може бути ситуація, коли зменшення кількості інформації, що отримується однією стороною, ініціюється іншою стороною. Якщо перша сторона буде керувати цим процесом, то можливо примусить іншу сторону функціонувати в умовах дезінформації. При цьому протилежна сторона може розпочати адекватні дії і в цьому випадку перша сторона також опиниться в стані дезінформації.

В. інформаційні зовнішні /о. информационные внешние/ [external information r.] — відносини інформаційні системи інформаційної з іншими системами та із середовищем їхнього існування.

В. інформаційні конфліктні /о. информационные конфликтные/ — відносини інформаційні, спрямовані на забезпечення захисту інформаційного і інформаційного суперництва реальних систем інформаційних. Складають зміст боротьби інформаційної. Реалізуються інформаційно-ударними угрупованнями сил та засобів.

В. інформаційні співробітництва /о. информационные сотрудничества/ — відносини інформаційні в працездатних системах інформаційних, для яких апостеріорна інформаційна невизначеність стану в процесі функціонування зменшується.

В. інформаційні суперництва /о. информационные соперничества/ — антагоністичні відносини інформаційні, що відповідають безвихідним відносинам у непрацездатних системах, коли дії сторін збільшують невизначеність.

В. інформаційної взаємодії /о. информационного взаимодействия/ — відносини інформаційні, спрямовані на забезпечення інформаційного суперництва та співробітництва інформаційного реальних систем інформаційних.

В. інформаційної ізоляції /о. информационной изоляции/ — відносини інформаційні, спрямовані на

забезпечення інформаційного відокремлення і захисту інформаційного реальних систем інформаційних.

В. суспільні в галузі інформаційної безпеки /о. общественные в области информационной безопасности/ — відносини у суспільстві при створенні і застосуванні механізмів захисту життєво важливих інтересів особистості, суспільства, держави в інформаційній сфері (див. механізми інформаційної безпеки). Ці відносини зв'язані з цілим рядом прав, обмежень, обов'язків та відповідальністю: із правом на захист держави і суспільства від впливу недостовірної, хибної інформації; із правом на захист інформації документованої, ресурсів інформаційних та продукції інформаційної як речової власності; із правом на захист інформації та інших нематеріальних об'єктів як інтелектуальної власності; із правом на захист систем інформаційних, технологій інформаційних і засобів їхнього забезпечення як речової власності; із правом на захист особистості в умовах інформатизації; із обмеженням права на розкриття особистої таємниці, а також іншої інформації обмеженого доступу без санкцій її власника; із обов'язками — захисту держави і суспільства від шкідливого впливу інформації, захисту самої інформації, захисту прав особистості, захисту таємниці (особистої, державної і т.ін.); з відповідальністю — за порушення прав і свобод особистості, за порушення таємниці та інших обмежень доступу до інформації, за злочини комп'ютерні.

ВІДОМОСТІ /ведомости/ [list] — зведення, список яких-небудь даних.

В. особливої важливості /в. особой важности/ — відомості у галузі воєнної, зовнішньополітичної, економічної, науково-технічної, розвідувальної, контррозвідувальної та оперативно-розшукової діяльності, розповсюдження яких може нанести шкоду державі в одній або декількох із перелічених галузей.

В. таємні /в. секретные/ — відомості, що складають державну таємницю, за виключенням відмомостей особливої ваги та цілком таємних, розповсюдження яких може нанести шкоду підприємства, закладу або організації.

В. цілком таємні /в. совершенно секретные/ — відомості у галузі воєнної, зовнішньополітичної, еконо-

мічної, науково-технічної, розвідувальної, контррозвідувальної та оперативно-розшукової діяльності, розповсюдження яких може нанести шкоду інтересам міністерства (відомства) або галузей економіки держави в одній або декількох із перелічених галузей.

В. у галузі економіки, науки і техніки, які можуть складати державну таємницю /в. в области экономики, науки и техники, которые могут составлять государственную тайну/ — відомості в галузі економіки, науки і техніки, розповсюдження яких може заподіяти шкоду державі. До них можуть бути віднесені наступні відомості: про зміст планів підготовки держави та її окремих регіонів до можливих воєнних дій, мобілізаційні потужності промисловості стосовно виготовлення озброєння і воєнної техніки, про обсяги поставок і про запаси стратегічних видів сировини і матеріалів, а також про розташування і фактичні розміри державних матеріальних резервів; про використання інфраструктури держави в інтересах забезпечення її обороноздатності і безпеки; про сили і засоби цивільної оборони, дислокації, призначення і ступеня захищеності об'єктів адміністративного управління, забезпечення безпеки населення, про функціонування промисловості, транспорту і зв'язку в цілому по державі; про обсяги і плани (завдання) державного оборонного замовлення, випуск і поставки озброєння, воєнної техніки та іншої оборонної продукції, про наявність і нарощування потужностей їхнього випуску, зв'язок підприємств по кооперації, розробників і виготовлювачів озброєння, воєнної техніки і іншої оборонної продукції; про науково-дослідні, дослідно-конструкторські і проектні роботи, технології, що мають важливе оборонне або економічне значення, що впливає на безпеку держави; про державні запаси дорогоцінних металів і дорогоцінних каменів держави, її фінанси і бюджетну політику (окрім узагальнених показників, що характеризують загальний стан економіки і фінансів).

В. у галузі зовнішньої політики і економіки, які можуть складати державну таємницю /в. в области внешней политики и экономики, которые могут составлять государственную тайну/ — відомості про зовнішньополітичну і зовнішньоекономічну (торговельну, кредитну і валютну) діяльності держави,

передчасне розповсюдження яких може нанести шкоди її інтересам.

В. у галузі розвідувальної, контррозвідувальної і оперативно-розшукової діяльності, які можуть складати державну таємницю /в. в области разведывательной, контразведывательной и оперативно-разыскной деятельности, которые могут составлять государственную тайну/ — відомості в галузі розвідувальної, контррозвідувальної і оперативно-розшукової діяльності, розповсюдження яких може заподіяти шкоду державі. До них можуть бути віднесені наступні відомості: про сили, засоби, джерела, методи, плани і результати розвідувальної, контррозвідувальної і оперативно-розшукової діяльності, а також дані про фінансування цієї діяльності, якщо ці дані розкривають перелічені відомості; про осіб, що співпрацюють або співпрацювали на конфіденційній основі з органами, які здійснюють розвідувальну, контррозвідувальну й оперативно-розшукову діяльність; про систему урядового та інші види спеціального зв'язку, про державні шифри, методи і засоби їхнього аналізу; про методи і засоби захисту секретної інформації; про державні програми і заходи в галузі захисту державної таємниці.

В. у воєнній галузі, які можуть складати державну таємницю /в. в военной области, которые могут составлять государственную тайну/ — відомості воєнної галузі, розповсюдження яких може заподіяти шкоду державі. До них можуть бути віднесені наступні відомості: про зміст стратегічних і оперативних планів, документів бойового управління з підготовки та проведення операцій, стратегічного, оперативного і мобілізаційного розгортання військ, про їхню боєздатність і мобілізаційну готовність, про створення і використання мобілізаційних ресурсів; про напрями розвитку озброєння і воєнної техніки, зміст і результати виконання цільових програм, науково-дослідних і дослідно-конструкторських робіт, спрямованих на створення і модернізацію зразків озброєння і воєнної техніки; про кількість, будову і технології виробництва ядерної і спеціальної зброї, технічні засоби і методи його захисту від несанкціонованого застосування; про тактико-технічні характеристики і можливості бойового застосування зразків озброєння і воєнної техніки, властивості, рецептури або технології виробництва нових видів ракетного палива або вибухових речовин во-

єнного призначення; про дислокацію, призначення, ступені готовності і захищеності режимних і особливо важливих об'єктів, про їхнє проектування і будівництво, а також про відведення земель, надр і акваторій під ці об'єкти; про дислокацію, дійсні найменування, організаційну структуру, озброєння і чисельність об'єднань, з'єднань і частин збройних сил.

В. розвідувальні /в. разведывательные/ — результати спостереження за джерелами (об'єктами) розвідки. В. р. добуваються розвідниками або розвідувальними підрозділами. Збирання в. р. повинно задовольняти наступним основним вимогам: оперативність та цілеспрямованість подання в. р. у відповідності з поставленими розвідувальними завданнями; достовірність та відсутність спотворення в. р.; дублювання збирання найбільш важливих в. р.; можливість надходження в. р. у вигляді оригіналу; оброблення в. р. може бути як складовою частиною процесу добування, так і самостійним процесом перетворення, узагальнення в. р., який завершує виконання розвідувальних завдань.

В., що складають державну таємницю /в., которые составляют государственную тайну/ — відомості, розповсюдження яких може заподіяти шкоду державі. До таких відомостей можуть бути віднесені відомості: в воєнній галузі; в галузі економіки, науки і техніки; в галузі зовнішньої політики і економіки; в галузі розвідувальної, контррозвідувальної і оперативно-розшукової діяльності

В., які не підлягають засекречуванню /в., которые не подлежат засекречиванию/ — відомості, засекречення яких здатне спричинити шкоду суспільству, державі і громадянам. До них можуть бути віднесені наступні відомості: про надзвичайні події і катастрофи, що загрожують безпеці і здоров'ю громадян, і їхні наслідки, а також про стихійні лиха, їхні офіційні прогнози і наслідки; про стан екології, охорони здоров'я, санітарії, демографії, освіти, культури, сільського господарства, а також про стан злочинності; про привілеї, компенсації і пільги, що надаються державою громадянам, посадовим особам, підприємствам, закладам і організаціям; про факти порушення прав і свобод людини і громадянина; про розміри золотого запасу і державних валютних резервів держави; про стан здоров'я вищих посадових осіб держави; про

факти порушення законності органами державної влади і їхнім посадовими особами.

ВІДСТАНЬ /расстояние/ [distance] — вимір простору, який розділяє два пункти, предмети тощо; віддаль, відлеглість, дистанція.

В. однозначного визначення /р. однозначного определения/ [unicity d.] — щонайменша кількість символів вхідного тексту, за якими теоретично стає можливою атака криптоаналітична лише з відомим шифртекстом.

ВІЙНА /война/ [war, warfare]— 1) Організована боротьба збройна між державами, іноді всередині держави (війна громадянська). 2) Крайня ступінь жорстокої боротьби, ворожі відносини між будь-ким. Розрізняють види в.: світова, локальна; колоніальна, несправедлива, визвольна, справедлива, загарбницька; образно говорять — газетна, інформаційна, митна в. і т. ін. 3) Складне суспільно-політичне явище, що включає сукупність різноманітних видів боротьби: політичної; економічної; збройної; інформаційної і т. ін., які ведуть між собою держави або суспільні системи. Збройна боротьба є основною формою боротьби у в. Формула збройної боротьби у в. може бути представлена у вигляді чотирьох обов'язкових взаємозв'язаних елементів: ураження військ і об'єктів противника; захист своїх військ і об'єктів від ураження; всебічне забезпечення дій військ сторін; управління силами і засобами в збройній боротьбі. У в. поряд з усіма іншими формами боротьби обов'язково присутня інформаційна складова боротьби. Вона є в політичній, ідеологічній, економічній і власне збройній боротьбі. Масштаби протиборства інформаційного в усіх складових формах боротьби невпинно зростають і потребують високої організованості при його підготовці. На основі аналізу впливу зброї (озброєнь) і інформації на форми і способи ведення збройної боротьби можна виділити шість поколінь війн, із яких чотири покоління доядерних війн і воєнних конфліктів. Основні рубежі зміни поколінь таких в. співпадають, головним чином, з історичними якісними стрибками в розвитку економіки, які приводили до появи нових озброєнь, а це призводило до зміни форм і способів збройної боротьби. В доядерний період практично усі війни були інструментом політики, її продовженням силовим способом.

Ядерна ж в., у випадку її розв'язання, неминуче вийшла би за рамки політики, що породила її, і привела би до кінця всякої політики і до катастрофічних наслідків на планеті.

В. громадянська /в. гражданская/ [civil w.] — боротьба збройна всередині держави між її громадянами, підданими, їхніми угрупованнями.

В. електронна /в. электронная/ [electronic w.] — комплекс заходів із застосуванням засобів випромінювання електромагнітного, спрямованих на пониження ефективності або запобігання застосування противником електромагнітного спектру, а також на забезпечення ефективного використання електромагнітного спектра своїми військами. В. е. є основоположним елементом впливу як на системи управління противника в оперативній і тактичній ланках, так і в цілому на інфраструктуру інформаційну противника. В. е. включає три основних елементи: забезпечення електронне, атака електронна і боротьба з електронною протидією або контрпротидія електронна.

В. із засобами командування і оперативного управління /в. с средствами командования и оперативного управления/ [Command and Control W. (C^2W)] (ам.) — вид оперативного забезпечення, який реалізує на полі бою концепцію інформаційної війни. Передбачає проведення операцій психологічних, протидію розвідці противника та забезпечення безпеки дій своїх військ, введення противника в оману, ведення війни електронної, знищення (руйнування) пунктів управління противника і його систем зв'язку. Розвідка розглядається як один із найбільш важливих видів забезпечення заходів такої війни. Усі заходи реалізуються комплексно (інтегровано) та координуються у часі і по завданнях уже в мирний час, і на етапі підготовки операцій повинні забезпечити вплив на процес прийняття рішень командуванням противника у вигідному напрямку, а з початком воєнних дій зменшити ефективність або забезпечити руйнування системи управління противника, оволодіння і втримування інформаційного домінування.

В. інформаційна /в. информационная/ [information w.] — 1) Комплекс заходів і операцій, спрямованих на забезпечення переваги інформаційної по відношенню до потенційного або реального противника. В.

і. можна розглядати в двох аспектах: в широкому розумінні — як форму геополітичного суперництва сторін (протиборство інформаційне) і в більш вузькому значенні — стосовно галузі боротьби збройної (боротьба інформаційна). В. і. ведеться не тільки в фізичному просторі, де знаходяться фізичні системи інформаційні і засоби, але і в деякій віртуальній зоні (віртуальному або кібернетичному просторі). В. і. розширює простір ведення війн, який раніше обмежувався великими висотами в атмосфері (стратосфері) і великими глибинами у Світовому океані. До особливостей в. і. відноситься те, що вона ведеться як під час фактичних бойових дій, так і в мирний час, і в кризових ситуаціях без офіційного оголошення. Початок і. в. неможливо визначити однозначно. У в. і. відсутня лінія фронту; проведення противником операцій в. і. практично неможливо виявити, а якщо факти проведення таких операцій виявляються, вони залишаються анонімними. Які-небудь міжнародні юридичні і моральні норми ведення в. і. відсутні. Та чи інша країна може стати об'єктом інформаційної дії, не знаючи про це. Невисока вартість технічних засобів, які можуть бути використані у в. і., суттєво розширюють коло можливих її учасників. Ними можуть бути окремі країни та їхні органи розвідки, злочинні, терористичні і наркобізнесові угруповання, комерційні фірми і навіть особи, що діють без злочинних намірів. Усі форми в. і. зводяться до впливу на інфраструктуру інформаційну противника, його системи інформаційні і ресурси інформаційні з проведенням будь-яких дій, що мають за мету спотворення інформації, що одержується ним , позбавлення його можливостей одержання нової інформації або фізичне знищення його інформаційних засобів, а також до захисту інформації власних збройних сил від аналогічних дій противника. Як правило виділяють наступні форми в. і.: боротьба радіоелектронна; війна психологічна; війна з використанням засобів розвідки; війна кібернетична; війна з хакерами. 2) Відкриті та приховані цілеспрямовані впливи інформаційні систем інформаційних одна на одну з метою одержання певного виграшу в матеріальній сфері.

В. інформаційна громадянська /в. информационная гражданская/ [civil information w.] — великомасштабне інформаційне протистояння між суспільними групами або державами, яке має за мету змінити розподіл сил у суспільстві. В. і. г. може бути розв'язана терористами, наркотичними картелями, підпільни-

ми торгівцями зброєю масового знищення і т. ін.

В. інформаційна з використанням засобів розвідки /в. информационная с использованием средств разведки/ — застосування різноманітних систем і датчиків для спостереження і контролю обстановки на полі бою. Сучасні армії розробляють схеми використання інформації від датчиків у реальному або близькому до реального часі для управління бойовими діями і наведення зброї на цілі. Інформація від датчиків, встановлених безпосередньо в зоні бойових дій, зіставляється і суміщається з відеозображеннями, що отримуються від безпілотних розвідувальних літальних апаратів і літаків та даними розвідки агентурної для формування повної картини бойової обстановки.

В. кібернетична /в. кибернетическая/ [cybernetic w.] (ам.) — концепція ведення війни з використанням моделей і імітації. Так як багато об'єктів, проти яких проводяться операції інформаційної війни, не існують фізично, вони можуть бути подані тільки моделями. Розробка таких високоточних моделей є одною з функцій в. к. Ці моделі повинні відображати усі аспекти фактичної війни в реальному часі. Близьке до реальної дійсності кібернетичне моделювання бойової обстановки дозволяє не тільки заощадити кошти на навчання і тренування особового складу збройних сил, але і випробувати різноманітні сценарії бойових дій і тактичних прийомів без людських і матеріальних утрат. Операції і засоби інформаційної війни все більше застосовуються для імітаційного моделювання, від індивідуального навчання особового складу до підтримки широкомасштабних навчань і планування воєнних операцій.

В. криптографічна /в. криптографическая/ [cryptography w.] — процес боротьби між криптографом та криптоаналітиком.

В. психологічна /в. психологическая/ [psychological w.] — 1) Сукупність різноманітних форм, методів і засобів впливу на людей з метою зміни в бажаному напрямку їхніх психологічних характеристик (поглядів, думок, ціннісних орієнтацій, настроїв, мотивів, установок, стереотипів поведінки), а також групових норм, масових настроїв, суспільної свідомості в цілому. У в. п. впливи психологічні можуть здійснюва-

тися різними методи: власне психологічними засобами; воєнними засобами; використанням торговельних і фінансових санкцій; політичними засобами. 2) Діяльність спеціальних органів однієї держави, що здійснюють психологічний вплив на цивільне населення і (або) на військовослужбовців іншої держави заради досягнення своїх політичних, а також чисто воєнних цілей. Офіційно в. п. проти іноземних держав ведеться тільки із санкції президента, уряду або ради національної безпеки. Проте в країнах із слабкою виконавчою владою і загальним зневажливим ставленням до діючого законодавства в. п. здійснюється за допомогою засобів масової інформації цими чи іншими політичними угрупованнями або фінансово-промисловими групами (у тому числі транснаціональними). 3) Стихійне, некваліфіковане використання засобів спілкування і механізмів соціально-психологічного впливу одними людьми проти інших людей з метою підкорення їх собі або створення сприятливих умов для свого існування й діяльності. В цьому випадку термін п. в. може характеризувати: політичну діяльність окремих осіб, угруповань, партій, рухів; виборчі компанії кандидатів на різноманітні виборні посади; рекламну діяльність комерційних структур; боротьбу індивідів (і груп малих) у суперництві за лідерство у виробничих, наукових та інших колективах; політичне, економічне або культурне протистояння конфліктуючих між собою етносів; переговорний процес між конкуруючими фірмами або організаціями. 4) Сукупність різноманітних операцій психологічних і разових заходів, що мають за мету спотворення інформації, яку одержує політичне керівництво, командування і особовий склад збройних сил противника, і нав'язування їм фальшивої або беззмістовної інформації, яка позбавляє їх можливості правильно сприймати події або поточну обстановку і приймати правильні рішення; психологічне оброблення військ і населення; ідеологічні диверсії і дезінформацію; підтримку сприятливої суспільної думки; організацію масових демонстрацій під фальшивими гаслами; пропаганду і розповсюдження фальшивих чуток.

В. психотронна /в. психотронная/ — процес боротьби з масовим застосуванням зброї психотронної.

ВІНЧЕСТЕР /винчестер/ [winchester disk] (від назви системи рушниць з англ. м. Вінчестера) — ма-

логабаритний пакет дисків жорстких магнітних, що загерметизовані разом з головками запису-читання. Використовується як зовнішня незмінна пам'ять ЕОМ.

ВІРОГІДНІСТЬ /достоверность/ — те ж, що достовірність.

ВІРТУАЛІЗАЦІЯ /виртуализация/ [virtualization] — перехід на більш високий рівень абстракції у керуванні конкретними конфігураціями системи обчислювальної.

ВІРТУАЛЬНИЙ /виртуальный/[virtual] (від лат. virtualis — сильний, здібний) — 1) Можливий; той, що може або має проявитися. 2) Характеристика пристрою або об'єкта, що не існує насправді. Способи використання віртуальних пристроїв відрізняються від способів використання звичайних пристроїв чи об'єктів. Наприклад, користувач може працювати з віртуальним диском як з фізичним, але насправді цей диск є частиною комп'ютерної пам'яті.

ВІРУСИ /вирусы/ [viruses] (від лат. virus — отрута) — збудники інфекційних захворювань рослин, тварин і людини, які розвиваються лише в живих клітинах і мають надзвичайно дрібні розміри, проходять через бактеріальні фільтри.

В. вульгарний /в. вульгарный/ [v. vulgaris] — вірус комп'ютерний, програма якого написана єдиним блоком і достатньо легко виявляється фахівцями на самому початку її активних проявів за допомогою набору стандартних антивірусних програмних засобів.

В. завантажувальний /в. загрузочный/ [boot v.] — вірус комп'ютерний, призначений для ураження завантажувальних секторів машинної пам'яті. Зараження в. з. відбувається при завантажуванні комп'ютера з носія машинної інформації, що містить вірус. Зараження може відбутися як випадково, наприклад, користувач сам, не підозрюючи про наявність вірусу на носії, запустив його в комп'ютерну систему, так і навмисно, якщо зловмисник (злочинець) знав про його існування і наслідки, які настануть після запуску системи з вірусоносієм. Носій машинної інформації може і не бути системним, тобто не мати файлів

операційної системи.

В. комбінований /в. комбинированный/ [combiner v.] — вірус комп'ютерний, що має окремі ознаки інших вірусів у певній алгоритмічній сукупності.

В. комп'ютерний /в. компьютерный/ [computer v.] — спеціальна програма, що здатна самочинно розмножуватися, створюючи свої копії, і поширюватися, модифікуючи (заражаючи) інші програми шляхом приєднання до них для наступного одержання управління та відтворення нових копій. Після запуску заражених програм вірус може виконувати різні небажані дії, що порушують цілісність інформації та (або) режим роботи засобів обчислювальної техніки: псування файлів та каталогів, модифікування програмного забезпечення, спотворення результатів обчислень, засмічування або стирання пам'яті, створення завад при роботі ЕОМ, наприклад, різних аудіо- та відеоефектів. Програми вірусів складаються (виконуються, пишуться), в основному, на мові програмування "асемблер" і при виконанні не створюють ніяких аудіовізуальних відображень у комп'ютерній системі. В. к. переноситься при копіюванні програм або даних спеціального формату або розповсюджується по мережі обчислювальній. В. класифікуються на певній основі і розбиваються на декілька узагальнених груп: віруси завантажувальні (системні), віруси файлові і комбіновані віруси, або на дві групи, що мають підгруповий поділ, а саме: за способом зараження засобів комп'ютерної техніки поділяються на резидентні та нерезидентні; за алгоритмом їхньої побудови і виявлення на віруси вульгарні та роздроблені.

В. комп'ютерний бойовий /в. компьютерный боевой/ — вид зброї інформаційної, що відноситься до програм з потенційно небезпечними наслідками. Для в. к. б. принципове значення мають наступні класифікаційні ознаки: об'єкт впливу (зараження); спосіб зараження об'єкта; принцип маскування; деструктивні можливості. За видом об'єкта зараження к. в. б. поділяються на віруси завантажувальні, віруси файлові, віруси завантажувально-файлові, макровіруси. За способом зараження в. к. б. поділяються на резидентні і нерезидентні. За способом маскування — на вірусі поліморфні, віруси-невидимки (стелс-віруси) та віруси

комбіновані. За деструктивними можливостями — на безпечні віруси й віруси, що виконують деструктивні функції. Особливістю в. к. б. є його неспрямованість на конкретні програми та властивість самодублювання. В. к. б. можуть розмножуватися, впроваджуватися у програми, передаватися лініями зв'язку, мережами обміну інформацією, виводити з ладу системи керування і т. ін.

В. нерезидентний /в. нерезидентный/ [nonresident v.] — вірус комп'ютерний, який не залишається в оперативній пам'яті після завершення програми-переносника вірусу і є активним обмежений час, а потім "гине".

В. паразитичний /в. паразитический/ [parasitic v.] (франц. parasites, від грец. *παράσιτøς* — нахлібник, дармоїд) — вірус комп'ютерний, який при розповсюдженні своїх копій обов'язково змінює вміст програм, файлів або дискових секторів. До цього виду вірусів відносяться усі віруси, які не є "черв'яками" або "супутниками".

В. поліморфний /в. полиморфный/ [polymorphic v.] (грец. *πøλύμøρφς* — той, що буває в кількох формах) — вірус комп'ютерний, що змінює свою структуру.

В. резидентний /в. резидентный/ [resident v.] (від лат. residens (residentis) — той, що залишається на місці) — вірус комп'ютерний, який залишає в оперативній пам'яті ЕОМ після завершення програми свою резидентну частину — переносника вірусу, який потім перехоплює звернення операційної системи до об'єктів зараження і впроваджується в них. В. р. знаходиться в пам'яті і є активним аж до виключення або перезавантаження комп'ютерної системи. В. р. активізується після кожного ввімкнення комп'ютера.

В. роздроблений /в. раздробленный/ [shattered v.] — вірус комп'ютерний, програма якого розділена на частини, які на перший погляд не мають між собою логічного зв'язку. Ці частини містять інструкції, які вказують комп'ютерові, як їх зібрати разом, в якій послідовності і якому випадку або в який час відтворити

вірус і коли розмножити його (принцип "Троянського коня").

В. студентський /в. студенческий/ [student v.] — украй примітивний, простий вірус комп'ютерний, що містить велику кількість помилок в алгоритмі його побудови і викликає локальні "епідемії". Як правило, такі віруси не набувають широкого поширення, швидко виявляються і знищуються, проте, встигають заподіяти шкоду в місці свого розмноження.

В. файловий /в. файловый/ [file v.] — вірус комп'ютерний, призначений для зараження ЕОМ із запущеної на ній програми, яка вже містить вірус. В цьому випадку можливе зараження інших виконавчих файлів, в тому числі COM, EXE, SYS, BAT-файли і деякі інші. В. ф. можуть бути резидентними та нерезидентними.

В.-невидимка /в.-невидимка/ [stealth v.] — вірус комп'ютерний, що використовує спеціальні алгоритми, які маскують його присутність на диску (у деяких випадках і в оперативній пам'яті).

В.-привид (мутант) /в.-призрак (мутант)/ [mutant v.] (від лат. mutans (mutantis) — те, що змінює) — вірус комп'ютерний, здатний до самокодування. В.-п. містять у собі алгоритми шифрування-розшифрування, які виключають можливість повторення однакових ланцюжків байт вірусного коду у будь-яких двох файлах, інфікованих одним і тим же в.-п.

В.-супутник /в.-спутник/ [companion v.] — вірус комп'ютерний, який не змінює програмні файли. Алгоритми роботи таких вірусів полягають у тому, що вони створюють для командних файлів запуску файли-супутники, що мають те ж ім'я, але з розширенням більш високого командного порядку. Після запуску такого файла ЕОМ першою запускає файл, що має найвищий рівень порядку, тобто вірус, який потім запустить і командний файл.

В.-черв'яки /в.-черви/ [worm v.] — віруси комп'ютерні, що розповсюджуються в комп'ютерній мережі і так же як і віруси-супутники, не заражають "батьківські" програми, файли або сектори на дисках. В.-

ч. проникають у пам'ять комп'ютера з комп'ютерної мережі і після визначення адрес інших комп'ютерів, розсилають за цими адресами свої копії. Такі віруси іноді створюють робочі файли на дисках операційної системи, проте можуть і взагалі не звертатися до ресурсів обчислювальної системи (за винятком оперативної пам'яті).

ВІРУСОЛОГІЯ /вирусология/ [virology] (від вірус... і грец. *λόγος* — слово, вчення) — наука про віруси.

В. комп'ютерна /в. компьютерная/ [v., computer v.] — наука, що займається вивченням вірусів комп'ютерних.

ВІРУСОНОСІЙ /вирусоноситель/ — в обчислювальній техніці — програма, заражена вірусом комп'ютерним.

ВЛАДА /власть/ [authority, power] — 1) Здатність, право і можливість розпоряджатися будь-ким, будь-чим, здійснювати вирішальний вплив на долі, поведінку і діяльність, мораль і традиції людей за допомогою різного роду засобів — закону, права, авторитету, волі, суду, примусу. 2) Політичне панування над людьми, їхніми спільнотами, організаціями, над країнами і їхніми угрупованнями. 3) Система державних органів. 4) Особи, органи, наділені відповідними державними, адміністративними повноваженнями.

В. інформаційна /в. информационная/ [information p.] — здатність, право і можливість розпоряджатися будь-ким, будь-чим, здійснювати вирішальний вплив на будь-кого на основі зростання значення інформації і сили її впливу на політичні процеси, на процедури вироблення і прийняття важливих рішень, їхньої пропаганди і реалізації. Лідирує той, хто володіє повною і своєчасною інформацією. Цілеспрямована інформація важлива також для створення іміджу владі, політиці і політикам, вона здатна керувати поведінкою великих груп людей. Зростання ролі такої інформації привело до появи маркетингу політичного.

ВЛАСНИК /владелец/ [owner] — господар певних речей, майна і т.ін. на правах приватного або суспіль-

ного володіння.

В. інформації /в. информации/ — 1) Суб'єкт, що здійснює володіння і використання інформації та реалізує повноваження на розпорядження інформацією у межах прав, встановлених законом або особою, яка володіє інформацією. 2) Суб'єкт відносин інформаційних, який має право на володіння, розпорядження й користування ресурсом інформаційним за угодою з установою (особою), що володіє інформацією.

В. інформаційних ресурсів, інформаційних систем, технологій і засобів їхнього забезпечення /в. информационных ресурсов, информационных систем, технологий и средств их обеспечения/ — суб'єкт, який у повному обсязі реалізує повноваження володіння, користування, розпорядження ресурсами інформаційними, системами інформаційними, технологіями інформаційними і засобами забезпечення інформаційних технологій.

ВЛАСНІСТЬ /собственность/ [property, proprietary] — належність чогось кому-, чому-небудь із правом розпоряджатися.

В. інтелектуальна /с. интеллектуальная/ [intellectual p.] — належні будь-кому результати літературної, художньої, наукової, технічної та інших видів творчості.

ВОКОДЕР /вокодер/ [vocoder] (англ. vocoder, від voice — голос і code — шифр, код) — клас передавальних систем, що базуються на принципі аналізу і синтезу мовного сигналу. У передавальній частині вокодера з мовного сигналу виділяються інформаційні параметра спектра мови, що змінюються повільно, основний тон вокалізованих (дзвінких) звуків і переходи тон-шум глухих звуків. В. розрізняються в залежності від параметрів, що виділяються. Розповсюджені вокодери смугові і вокодери з лінійним передбаченням. В. для телефонного закритого зв'язку із швидкістю передавання 4800 біт/с забезпечують розбірливість складів до 93% (розбірливість слів сягає 99%) при задовільному упізнаванні абонента). В телефонних каналах низької якості швидкість інформаційного потоку на виході в. знижують до 2400 біт/с при збереженні достатньої

розбірливості, але низького упізнавання голосу абонента.

В. з лінійним передбаченням /в. с линейным предсказанием/ [linear predictive v.] — вокодери, у яких вхідний мовний сигнал апроксимується кусково-лінійною функцією, кожний поточний відлік якої є лінійною функцією n попередніх відліків. У цих вокодерах мовна інформація передається величиною амплітуди, значеннями коефіцієнта лінійного передбачення, періодом основного тону і рішенням про тон або шум. Швидкість передавання мовної інформації у розповсюджених вокодерах даного виду для n=10 складає 2400 біт/с, але існує можливість зниження її до 800 біт/с і менше з допустимою якістю мови.

В. смугові /в. полосовые/ [channel v.] — вокодери, в яких аналізується форма мовного сигналу з періодом аналізу 10–30 мс, виділяються і передаються телефонним каналом у цифровому вигляді: значення амплітуд обмеженого числа частотних смуг спектра мовного сигналу, величина періоду основного тону для вокалізованих звуків і рішення тон/шум, що відповідає наявності або відсутності вокалізованої ділянки в мовному сигналі. У приймальному вокодері синтезуються звуки з переданими параметрами. У більшості практичних випадків аналіз мовних сигналів здійснюється з періодом 20 мс для 16–20 частотних смуг, що виділяються смуговими фільтрами, а параметри мови передаються із швидкістю 2400 біт/с. При зниженні вимог до якості синтезованої мови швидкість передавання мовної інформації може бути зменшена до 1200–1800 біт/с.

ВОЛОКНО /волокно/ [fiber] — тонка непрядена нитка рослинного, мінерального або штучного походження.

В. багатомодове /в. многомодовое/ [multimode f.] — волокно оптичне, у якого діаметр світловодної жили складає 50–60 мкм, що робить можливим розповсюдження в ньому великої кількості променів.

В. одномодове /в. одномодовое/ [monomode f.] — волокно оптичне, у якого діаметр свотловідної жили

складає 8–10 мкм, по якій може розповсюджуватися тільки один промінь (одна мода).

В. оптичне /в. оптическое/ [optical f.] — нитка діаметром біля 100 мкм, виготовлена з кварцу на основі двоокису кремнію. Волокно складається із серцевини (світловодної жили) і оболонки з різними показниками заломлення. Волокно з постійним показником заломлення називається ступінчатим, із змінним — градієнтним. Для передавання сигналів застосовуються два види волокна: одномодове і багатомодове. В. о. характеризується двома основними параметрами: загасанням і дисперсією. Загасання визначається втратами на поглинання і розсіювання світла у в. о. і вимірюється в децибелах на кілометр (дБ/км). Кращі зразки волокна мають загасання 0,15–0,2 дБ/км, розроблюються ще більш "прозорі" волокна з теоретичним значенням загасання до 0,02 дБ/км для хвиль довжиною 2,5 мкм. При такому загасанні сигнали можуть передаватися на відстань у сотні км без ретрансляції. Дисперсія зумовлена різноманітністю фазових швидкостей окремих мод оптичного сигналу, спрямовуючими властивостями волокна і властивостями його матеріалу. Вона приводить до спотворення (розширення) форми сигналу при його розповсюдженні у волокні, що обмежує дальність передавання і верхнє значення частоти спектра сигналу. Дисперсія в. о. оцінюється величиною збільшення на 1 км довжини часового параметра оптичного сигналу або еквівалентної смуги частот пропускання.

ВПЛИВ /влияние/ [impact] — дія, здійснювана ким-, чим-небудь на кого-, що-небудь.

В. деструктивний /в. деструктивное/ [destructive i.] (від лат. destruo — ламаю, руйную) — дія, що здійснюється для руйнування ким-, чим-небудь кого-, що-небудь.

В. джерела інформації /в. источника информации/ — складова частина впливу переконуючого. Ефективність такого впливу залежить від того, як люди, що його сприймають, відносяться до джерела інформації. В ході війни психологічної джерелами інформації можуть бути: уряд і керівництво збройних сил своєї країни; особи, авторитетні для об'єкта переконуючого впливу; органи психологічної війни. Власний

уряд і воєнне керівництво використовуються як джерела інформації тоді, коли треба повідомити населенню й військам противника урядові заяви, ультиматуми або іншу важливу офіційну інформацію. Вплив таких джерел ефективний у випадку, коли інформаційно-пропагандистські матеріали доставляються вчасно. Крім того, заяви й заклики офіційних джерел найбільш дійові тоді, коли загальна політична ситуація заплутана, або противник не впевнений у сприятливому для нього закінчення війни. Авторитетними джерелами інформації можуть найрізноманітніші люди, наприклад, церковні діячі, популярні журналісти, військовополонені і т. ін. Представники органів психологічної війни як джерела інформації використовуються доволі рідко, за виключенням випадків, коли психологічний вплив здійснюється на населення союзних країн або в ході миротворчих операцій.

В. змісту інформації /в. содержания информации/ — складова частина впливу переконуючого, ефективність якої в певній мірі залежить від характеристик змісту інформації: доказовості і переконливості; підбору, побудови й подання аргументації; підбору й подання закликів; форми впливу.

В. інформаційний /в. информационное/ [information i.] — 1) Організоване застосування сил і засобів боротьби інформаційної для вирішення завдань завоювання (підтримки) переваги інформаційної над противником. 2) Вплив, який здійснюється із застосуванням засобів зброї інформаційної, які дозволяють здійснювати з інформацією, що передається, оброблюється, створюється, знищується і сприймається, задумані дії. В. і. буде допустимим, якщо він грубо не порушує прийняті у більшості систем інформаційних в даному інформаційному просторі норми і правила поведінки (вихідні результати).

В. інформаційний наступальний /в. (акция) информационное наступательное/ — активний, цілеспрямований, узгоджений за завданнями, місцем і часом вплив залучених до ведення боротьби інформаційної сил і засобів протягом певного часу в заданому районі по окремих інформаційних об'єктах системи управління противника або його ресурсу інформаційного в цілому. При цьому можуть здійснюватися рі-

зноманітні удари інформаційні. Див. також акція інформаційна наступальна.

В. інформаційний, заснований на викраденні (втраті) цінної інформації /в. информационное, основанное на похищении (потере) ценной информации/ — сукупність дій, що приводить до зниження ефективності власної діяльності або до підвищення ефективності діяльності противника, конкурента. Якщо об'єктом такого впливу є свідомість людей, то мова йде про розголошення таємниць державних, вербування агентів, спеціальні заходи і засоби для підслухування, використання детекторів брехні, медикаментозні, хімічні та інші впливи на психіку людини з метою розв'язати їй язика або забути будь-що. Безпеку від інформаційного впливу такого виду забезпечують контррозвідка та інші органи інформаційної безпеки. Якщо джерелом інформації служать технічні системи, то мова йде про розвідку технічну, або шпіонаж (перехоплення телефонних розмов, радіограм, сигналів інших систем комунікації), проникнення в комп'ютерні мережі, банки даних. Протидіють технічній розвідці органи контррозвідки, а також структури, що займаються теорією і практикою захисту комп'ютерних засобів, систем зв'язку.

В. інформаційний, заснований на впровадженні негативної інформації /в. информационное, основанное на внедрении отрицательной информации/ — сукупність дій, спрямованих не тільки на сприяння прийняття небезпечних, помилкових рішень, але і таких, що заставляють діяти на шкоду і можуть людину довести до самогубства, а суспільство — до катастрофи. Безпеку інформаційну проти впливів цього виду повинні забезпечувати спеціальні структури боротьби інформаційної, призначені для нейтралізації акцій дезінформації, переривання маніпулювання суспільною думкою, а також протидіяти силам і засобам РЕБ, ліквідувати наслідки комп'ютерних атак.

В. інформаційні небезпечні /в. информационные опасные/ [risky information i.] — дії, спрямовані на зниження рівня безпеки інформаційної. Вони можуть бути засновані як на викраденні (втраті) цінної інформації з об'єктів інформаційної безпеки, так і на впровадженні негативної інформації на об'єкти

інформаційної безпеки.

В. інформаційно-психологічний /в. информационно-психологическое/ — вплив психологічний словом, інформацією. Мета в. і.-п. — формування певних ідеологічних (соціальних) ідей, поглядів, уявлень, переконань, одночасно він викликає у людей позитивні або негативні емоції, почуття і навіть бурхливі масові реакції.

В. на ресурси противника /в. ресурсы противника/ — вид протидії інтелектуальної в мережах інформаційно-обчислювальних(ІОМ), що припускає поглинання ресурсів мережі і неефективне їхнє використання противником. До таких ресурсів відносять: час, що затрачається противником для досягнення мети нападу інформаційного; ресурси обчислювальних засобів, що затрачаються противником в ході атаки інформаційної і в процесі верифікації інформації, одержаної від об'єкта, що атакується; людські ресурси, що затрачаються в ході боротьби інформаційної; морально-психологічна стійкість осіб, що беруть участь в інформаційній боротьбі на стороні противника; ресурси інформаційні противника, що формуються в результаті інформаційних атак на ІОМ; зброя інформаційна противника й способи її застосування; матеріальні й фінансові витрати противника на ведення війни інформаційної.

В. нейролінгвістичний /в. нейролингвистическое/ — вид впливу психологічного, який змінює мотивацію людей шляхом уведення в їхню свідомість спеціальних лінгвістичних програм (програмування нейролінгвістичне). Основним об'єктом в. н. є нейрофізіологічна активність мозку та емоційно-вольовий стан, що виникає внаслідок активності мозку. Головний засіб впливу — спеціально підібрані вербальні (словесні) і невербальні програми, засвоєння змісту яких дозволяє змінювати в заданому напрямку переконання, погляди і уявлення людини (як окремого індивіда, так і цілих груп людей). Суб'єктом в. н. є спеціаліст (інструктор), який спочатку виявляє в психіці суперечливі (конфліктуючі) погляди і переконання, а також негативні емоційні стани (переживання, настрій, почуття), які турбують людей, а на наступному етапі за допомогою спеціальних прийомів допомагає усвідомити дискомфортність їхнього реального стану

(соціально-економічного, культурного, фізичного і як наслідок — психологічного) і вносить у свідомість зміни, які змушують людей по-іншому сприймати життєві ситуації і будувати відносини з іншими людьми.

В. переконуючий /в. убеждающее/ — вид впливу психологічного, заснований на використанні методів переконування. В. п. включає: вплив джерела інформації; вплив змісту інформації; вплив ситуації інформування. Для одержання максимального ефекту в. п. повинно відповідати певним вимогам: зорієнтованості й плановості; спрямованості на конкретний об'єкт; зорієнтованості переважно на інтелектуально-пізнавальну сферу психіки об'єкта; спрямованості на ініціювання певної поведінки. Основними принципами здійснення в. п. повинні бути: принцип повторювання; принцип досягнення первинності впливу; принцип забезпечення довіри до джерела інформації; принцип активізації психічних процесів сприйняття об'єктом змісту інформації.

В. психоаналітичний (психокорекційний) /в. психоаналитическое (психокоррекционное)/ — вплив психологічний на підсвідомість людини терапевтичними засобами, особливо в стані гіпнозу або глибокого сну. Існують також методи, що виключають свідомий опір як окремого індивіда, так і груп людей, які не сплять (комп'ютерний психоаналіз і комп'ютерна психокорекція).

В. психогенний /в. психогенное/ — вплив психологічний, який є наслідком фізичного впливу на мозок індивіда, результатом якого порушення нормальної нервово-психічної діяльності, або шокового впливу навколишніх умов або будь-яких подій (наприклад, картин масових зруйнувань, численних жертв і т. ін.) на свідомість людини, внаслідок чого вона не може раціонально діяти, втрачає орієнтацію у просторі, відчуває афект або депресію, впадає в паніку, в ступор і т.ін. Частковим випадком в. п. є вплив кольору на психофізичний і емоційний стан людини.

В. психологічний /в. психологическое/ — вплив на людей (на окремих індивідів і на групи), який здійснюється з метою зміни ідеологічних і психологічних структур їхньої свідомості і підсвідомості, транс-

формації емоційних станів, стимулювання певних типів поведінки. В. п. поділяють на наступні види: вплив інформаційно-психологічний, вплив психогенний, вплив психоаналітичний, вплив нейролінгвістичний, вплив психотронний, вплив психотропний. Для здійснення в. п., необхідно спочатку спровокувати збої і перекоси в функціонуванні окремих компонентів психіки об'єкта впливу. Динамічна рівновага між ними порушиться і він почне переживати стан дисонансу когнітивного. Після цього можна знову спонукати до відновлення душевної рівноваги за рахунок зміни своїх попередніх, звичних для нього поглядів, переконань і відносин, а потім і стереотипів поведінки. Результативність в. п. залежить від особливості механізмів трансформації переконань, стереотипів і установок людей. Виділяють три етапи в. п.: операційний, коли здійснюється діяльність його суб'єкта; процесуальний, коли має місце прийняття (схвалення) або неприйняття (несхвалення) впливу його об'єктом; заключний, коли проявляються реакції як наслідок перебудови психіки об'єкта впливу. Перебудова психіки може бути різноманітною як за широтою, так і за стійкістю у часі. У першому випадку розрізняють парціальні зміни, тобто зміни будь-якої однієї психологічної якості (наприклад, думки людини про конкретне явище), і більш загальні зміни психіки, тобто зміни ряду психологічних якостей індивіда (або групи). В іншому випадку зміни можуть бути короткочасними або довготривалими.

В. психологічний друкованими засобами /в. психологическое печатними средствами/ — психологічний вплив, що здійснюється шляхом розповсюдження друкованої продукції на іноземних мовах, а також публікації матеріалів в засобах масової інформації своєї країни і держав-союзників. Особливостями такого впливу є доступність, наочність, різноманітність, здатність впливати на різноманітні масові аудиторії. В. п. д. з. потребує достатньої кількості підготовлених творчих працівників і технічних фахівців, сучасної поліграфічної бази, достатнього запасу витратних матеріалів, а також технічні засоби доставки й розповсюдження друкованої продукції. Основними видами матеріалів, що використовуються при в. п. д. з. є:

листівки, газети, журнали, брошури.

В. психологічний образотворчими засобами /в. психологическое изобразительными средствами/ — вплив психологічний за допомогою наочних засобів, які несуть сильний емоційний заряд. Для цього використовують оформлені на художньому рівні плакати, карти, фотостенди, настінні газети і карикатури, спеціально організовані виставки, а також інші засоби, наприклад, наклейки, нашивки, сувеніри з відповідною символікою. Перевагами такого психологічного впливу є: використання ефекту багаторазового впливу; вплив через зорові рецептори, тобто через найбільш місткий канал передавання інформації в кору головного мозку; вплив зображення як на свідомість, так і на підсвідомість людини.

В. психологічний через радіо і телебачення /в. психологическое посредством радио и телевидения/ — вплив психологічний, який здійснюється шляхом передавання в ефір радіо- і телепередавачі спеціальних програм радіомовлення і мовлення телевізійного. Така форма війни психологічної дозволяє оперативно и ефективно охоплювати масові аудиторії в межах радіуса приймання радіо- або телевізійного мовлення конкретної станції.

В. психотронний /в. психотронное/ — вплив психологічний, який здійснюється шляхом передавання інформації через позачуттєве (позаусвідомлюване) сприйняття. Див. також психотроніка і зброя психотронна.

В. психотропний /в. психотропное/ — вплив на психіку людей за допомогою засобів психотропних (медичних препаратів, хімічних або біологічних речовин).

В. ситуації інформування /в. ситуации информирования/ — складова частина впливу переконуючого, що в певній мірі залежить від ситуації інформування.

В. сугестивний /в. суггестивное/ [suggestion i.] (лат. suggestio, від suggero — навчаю, навіюю) — вплив,

спрямований на формування у системи інформаційної із самонавчанням прихованих цілей.

В. у відповідь на інформаційний напад /в. источника информации/ — атака на мережу обміну інформацією віддалена, яка здійснюється після встановлення факту нападу інформаційного на об'єкти мережі та ідентифікації противника. Цей вид атак часто називають протидією (протидією інтелектуальною). Її відмітною особливістю є те, суб'єкт і об'єкт атаки міняються місцями. Атаки такого виду можуть бути організовані шляхом підміни суб'єктом атаки об'єкта атаки на хибний об'єкт і використання спеціальних програм протидії, що імітують роботу справжнього об'єкта атаки.

ВПРОВАДЖЕННЯ /внедрение/ [embedding, implementation] — таємне проникнення агента у ворожу організацію (або його вербування в цій організації) з метою добування її секретів.

ВТРАТА /потеря/ [loss] — дія, внаслідок якої хтось лишається без кого-, чого-небудь, втрачає когось, щось.

В. інформації /п. информации/ [information l.] — 1) Дія, внаслідок якої інформація в системі інформаційній перестає існувати для користувачів. 2) Неконтрольоване розповсюдження інформації, що веде до її несанкціонованого одержання.

ВУЗОЛ /узел/ [node] — 1) Точка в мережі даних, в якій один або декілька функціональних пристроїв об'єднують канали передавання даних або ланцюги даних. 2) Частина пристрою. 3) В Інтернеті — коротка назва моста, маршрутизатора, комутатора, шлюзу або хоста.

В. зв'язку /у. связи/ [communication n.] — елемент системи зв'язку, що забезпечує створення та комутацію групових трактів, каналів, повідомлень, пакетів, цифрових потоків, а також інших функцій в системі зв'язку.

В. інформаційний /у. информационный/ [information n.] — сукупність елементів і зв'язків найбільш інформативної частини інформаційного портрета. До в. і. відносяться принципово нові технічні, техноло-

гічні і образотворчі рішення та інші досягнення, які складають ноу-хау.

В. комутації каналів (повідомлень) /у. коммутации каналов (сообщений)/ [channel (message) switching center] — сукупність пристроїв, зосереджених в одному місці і об'єднаних загальним пристроєм управління, за допомогою яких здійснюється комутація каналів передавання даних (повідомлень).

В. мережного з'єднання /у. сетевого соединения/ [session n.] — набір розташованих поряд станцій робочих, скриньок поштових і кінцевих точок мережі транспортної.

Г

ГАЗЕТА /газета/ — періодичне, переважно щоденне (щоденник, тижневик, місячник, квартальник), друковане на великих аркушах паперу видання, яке містить різноманітні матеріали про поточні події суспільно-політичного, культурного та економічного життя. Г. — один з ефективних і розповсюджених видів друкованої пропагандистської продукції. До специфічних особливостей таких газет відносяться: передавання змісту на іноземній мові; характерні тільки для газети форми й способи подавання інформації; своєрідні структурно-композиційні й графічні елементи (які відповідають прийнятим у даній країні нормам і правилам); оригінальність мовного й стилістичного оформлення матеріалів, наявність особливих газетних жанрів і рубрик і т.ін. Г. як засіб психологічного впливу повинна відповідати наступним вимогам: відрізнятися актуальністю й інформативністю матеріалів, що публікуються; бути доступною за своїм структурно-композиційним і мовним оформленням; бути компетентною в усіх питаннях, що освітлюються на сторінках газети; враховувати склад читацької аудиторії, її інтереси й потреби; демонструвати бездоганне знання мови видання; подавати інформацію з урахуванням норм газетної журналістики, прийнятих у даній країні, стереотипів сприйняття її населення; додержувати правил поліграфічного оформлення, звичних для місцевої читацької аудиторії. В першу чергу треба враховувати типовий світогляд більшості читачів, їх соціальні, національні і релігійні особливості, інформаційні запити, загальне відношення до пропаганди противника.

ГАМА /гамма/ [gamma] — у криптографії — випадкові або псевдовипадкові послідовності чисел.

ГАММА-ПРОМІННЯ /гамма-излучение/ [gamma radiation] (грец. $\gamma\alpha\mu\mu\alpha$ — Г, γ) — проміння електромагнітне, що має надзвичайно малу довжину хвилі, меншу за 10^{-11} м, і внаслідок чого — яскраво виражені корпускулярні властивості, тобто є потоком часток — гамма-квантів. Г.-п. супроводжує радіоактивний розпад в тому випадку, коли створювані ядра знаходяться в збудженому стані.

ГАМУВАННЯ /гаммирование/[gamma] — метод перетворення криптографічного, який полягає в генерації гами шифру за допомогою датчика псевдовипадкових чисел та накладання одержаної гами на відкриті дані оборотним чином (наприклад, використовуючи додавання за модулем 2). Процес розшифровування здійснюється на основі повторної генерації гами шифру при відомому ключі та накладенні такої гами на зашифровані дані.

ГАРАНТІЯ /гарантия/ [guarantee, assurance] (франц. garantie) — 1) Порука, забезпечення. 2) В системі захисту інформації — оцінка міри довіри в тому, що система захисту відповідає конкретній системі автоматизованій та забезпечує виконання певної політики безпеки. Див. також рівень гарантій. Гарантії даються органом сертифікації при акредитації системи оброблення даних на підставі її сертифікації. 3) Сукупність вимог (шкала оцінки) для визначення міри упевненості, що система комп'ютерна коректно реалізує політику безпеки.

ГЕНЕРАТОР /генератор/ [generator] (від лат. generator — родоначальник) — пристрій, апарат чи машина, які виробляють якийсь продукт, електричну енергію або перетворюють один вид енергії на інший.

Г. випадкових паролів /г. случайных паролей/ [random-password g.] — програмно-апаратний засіб, що являє собою генератор випадкових чисел, які використовуються як паролі.

Г. випадкових сигналів /г. случайных сигналов/ [random signal g.] — пристрій, призначений для вироблення сигналів випадкових, величини яких мають цілком визначені ймовірнісні характеристики. Найбільш

розповсюджені г. в. с. з рівномірним законом розподілу на основі використання фізичних процесів, що мають випадкові характеристики: дробовий ефект, радіоактивний розпад і т.ін. При моделюванні випадкових процесів на ЕОМ випадкові числа з необхідними законами розподілу одержують за допомогою спеціальних пристроїв — датчиків випадкових чисел, що включають г. в. ч. Розрізняють датчики випадкових чисел, що використовують джерела фізичних випадкових процесів, а також датчики, які дають псевдовипадкові послідовності.

Г. випадкових чисел /г. случайных чисел/ [random number g.] — див. датчик випадкових чисел.

Г. завад /г. помех/ [noise g.] — засоби придушення закладних пристроїв, призначені для активної боротьби із закладками шляхом пониження відношення сигнал/шум до безпечних для інформації значень, що дозволяє забезпечити превентивний захист інформації без попереднього виявлення і локалізації закладних пристроїв. Розрізняють генератори завад із лінійним зашумленням і генератори завад із просторовим зашумленням.

Г. завад із лінійним зашумленням /г. помех с линейным зашумлением/ — генератор завад, виходи якого приєднуються до проводів телефонної лінії або електромережі і в них подаються електричні сигнали, що перекривають небезпечні сигнали по спектру і потужності.

Г. завад із просторовим зашумленням /г. помех с пространственным зашумлением/ — генератор завад, призначений для створення відповідного рівня електромагнітних завад у приміщенні і на вході приймача зловмисника. Для ефективного придушення сигналу закладки рівень завади (загороджувальної або прицільної) у смузі спектра сигналу повинен у декілька разів перевищувати рівень сигналу.

Г. псевдовипадковий /г. псевдослучайный/ — те ж, що генератор псевдовипадкових послідовностей.

Г. псевдовипадкових послідовностей /г. псевдослучайных последовательностей/ [random sequence g.] — алгоритм поліноміальний G, який випадковий паросток $x \in /0,1/^n$ перетворює у послідовність $G(x) \in$

$/0,1/^{l(n)}$, яка є нерозрізненим ансамблем від випадкової величини, рівномірно розподіленої на $/0,1/^{l(n)}$.

Г. псевдовипадкових послідовностей криптографічно надійний /г. псевдослучайных последовательностей криптографически надежный/ — те ж, що генератор псевдовипадкових послідовностей.

ГЕНЕРУВАННЯ /генерация/ [generation] (від лат. generatio — народження) — відтворення, вироблення.

Г. ключів /г. ключей/ [key g.] —- процес породження ключів або вибору відповідного ключа з множини усіх можливих ключів.

ГЕОПОЛІТИКА /геополитика/ [geopolitics] (від грец. $\gamma\tilde{\eta}$ — земля і політика) — політична концепція, яка використовує географічні фактори (територія, положення, природні особливості, клімат та інші особливості тих чи інших країн, держав, їхніх блоків і т. ін.) для обґрунтування тих чи інших планів і розрахунків: економічних, політичних (нерідко експансіоністських).

ГЕОФОН /геофон/ [geophone] (від грец. $\gamma\tilde{\eta}$ — Земля і $\varphi\omega\nu\acute{\eta}$ — звук) — приймач звукових хвиль, що розповсюджуються в верхніх шарах земної кори. Г. обладнані перетворювачами акустоелектричними, що перетворюють коливання ґрунту в коливання електричного струму.

ГЕТЕРОДИН /гетеродин/ [heterodyne, oscillator] (від грец. $\ddot{\varepsilon}\tau\varepsilon\rho\varnothing\varsigma\ldots$ — інший і $\delta\acute{\upsilon}\nu\alpha\mu\iota\varsigma$ — сила) — малопотужний генератор високої частоти. Застосовують у радіоприймачах і радіовимірювальних приладах для перетворення частоти.

ГЕТЕРОГЕННІСТЬ /гетерогенность/ [heterogeneity] (від грец. $\ddot{\varepsilon}\tau\varepsilon\rho\varnothing\varsigma$ — інший, що у складних словах означає різнорідність) — властивість системи інформаційного обслуговування, що виявляється у взаємному сполученні різнорідних, різноманітних за властивостями і складом форм забезпечення (наприклад, інформаційне та бібліотечно-бібліографічне) і засобів забезпечення (наприклад, реферування та синтезування), що діють на засадах взаємодоповнюваності.

ГІДРО... /гидро.../ [hydro...] (від грец. $\tilde{\upsilon}\delta\omega\rho$ — вода) — у складних словах відповідає поняттям “вода”, “водний простір”.

ГІДРОАКУСТИКА /гидроакустика/ [hydroacoustics] (від гідро... і акустика) — розділ акустики, що займається вивченням фізичних явищ, пов’язаних із розповсюдженням і прийманням хвиль звукових у водному середовищі. Є теоретичною базою для розроблення гідроакустичних засобів, засобів підводного спостереження і зв’язку.

ГІДРОЛОКАТОР /гидролокатор/ [hydrolocator] (від гідро... і локатор) — пристрій, призначений для визначення за допомогою хвиль звукових місцеположення у воді рухомих і нерухомих об’єктів.

ГІДРОЛОКАЦІЯ /гидролокация/ [hydrolocation, sonar](від гідро... і локація) — визначення місцеположення об’єктів, що знаходяться у воді, шляхом випромінювання у водне середовище акустичної енергії у вигляді звукових імпульсів (посилок) і приймання (реєстрації) відбитої енергії від об’єкта у вигляді луна-сигналу (активна г.). Напрямок на виявлений об’єкт визначається за положенням акустичної антени, а відстань до нього — за проміжком часу між посилкою і прийманням сигналу. При пасивній г. здійснюється тільки приймання звукових сигналів, що випромінюються самими об’єктами (див. шумопеленгування).

ГІДРОФОН /гидрофон/ [hydrophone] (від грец. $\tilde{\upsilon}\delta\omega\rho$ — вода і $\varphi\omega\nu\acute{\eta}$ — звук) — перетворювач акусто-електричний, який застосовується в гідроакустиці для прослуховування підводних сигналів і шумів, для вимірювальних цілей, а також входить до складу гідроакустичних антен. Найбільш розповсюджені г., що працюють на п’єзоелектричному ефекті; використовуються також г. електродинамічного та магнітострикційного типу. Застосовуються спеціальні заходи забезпечення герметичності і захисту чутливих елементів від дії гідростатичного тиску і впливу води.

ГІПЕРПОСИЛАННЯ /гиперссылка/ — в гіпертекстовому документі — фрагмент тексту або графічний об’єкт, в який вбудований невидимий для користувача покажчик на інший документ.

ГІПЕРТЕКСТ /гипертекст/ [hypertext] (від грец. *ὑπερ*..., префікса, що означає підвищення, надмірність і текст) — форма організації текстового матеріалу, в якої одиниці інформації представлені як система явно означених можливих переходів і зв'язків між ними. Слідуючи цим зв'язкам, можна читати матеріал у будь-якому порядку, утворюючи різні лінійні тексти. При достатньо просторовому матеріалі з великою кількістю зв'язків виникає гіпертекстовий простір — мережа, що обробляється за допомогою сучасних комп'ютерних технологій.

ГЛОБАЛІЗАЦІЯ /глобализація/ [globalization] (франц. global — загальний, всесвітній, від лат. globus — куля) — 1) Поширення на всю земну кулю. 2) Розповсюдження інформаційних матеріалів, зв'язків і систем у транснаціональних масштабах по всьому світу. Вважається, що г. збільшує можливості подальшого прогресу у галузі науки, культури і мирного співробітництва народів світу в умовах інформаційного суспільства. Проте критики г. мас медіа вважають, що г. продукції інформаційної призводить до нівелювання самобутніх культур у різних країнах й підпорядкування ЗМІ не гуманітарним, а комерційним цілям.

ГЛОБАЛІЗМ /глобализм/ [globalism] (франц. global — загальний, всесвітній, від лат. globus — куля) — система поглядів і діяльності, яка враховує положення справ на усій земній кулі.

Г. інформаційний /г. информационный/ [information g.] — сфера діяльності, що полягає в утворенні різноманітних міжконтинентальних комунікаційних каналів і мереж. Розвиток г. і. відбудеться за рахунок створення телетрансляційних транскордонних комп'ютерних і мегасупутникових систем зв'язку у сполученні з подальшим освоєнням космічного простору, сонячних і водних енергоресурсів, а також розвитком суперкорпоративних структур, адекватних сучасним напрямкам у науці, техніці і виробництві. Вважається, що розвиток таких тенденцій може супроводжуватися і небажаними соціальними процесами — наростанням екологічних проблем, перевантаженням інформаційним і необережним поводженням з електронними мас медіа.

ГОЛОГРАФІЯ /голография/ [holography] (від грец. *ὅλος* — весь, повний і *γράφω* — пишу) — спосіб записування просторової структури світлової хвилі й одержання об'ємного зображення об'єкта.

ГРА /игра/ [game] — ряд дій, спрямованих до певної мети; інтрига, таємний задум.

Г. оперативна /и. оперативная/ — передача фальшивої інформації противнику (і одержання у відповідь точних відомостей) співробітником розвідки, який видає себе за ворожого агента, або полоненим і перевербованим агентом. Це може здійснюватися, наприклад, через обмін даними по рації (радіогра).

ГРИФ /гриф/ [label] — нанесений на носій інформації умовний знак корисності інформації, що міститься на ньому, — гриф секретності або конфіденційності.

Г. конфіденційності /г. конфиденциальности/ [confidentiality classification l.] — гриф, що найчастіше застосовується для позначення ступеню конфіденційності інформації комерційної (інформації, що містить таємницю комерційну). Для грифування комерційної інформації застосовують різноманітні шкали, засновані на відповідному критерії. Розповсюджена шкала: "комерційна таємниця — суворо конфіденційно", "комерційна таємниця — конфіденційно", "комерційна таємниця". Відома також шкала "суворо конфіденційно — особливий контроль", "суворо конфіденційно", "конфіденційно". застосовується також шкала з двох рівнів: "комерційна таємниця" та "для службового використання".

Г. секретності /г. секретности/ [security classification l.] — реквізити, що свідчать про ступінь секретності відомостей, що містяться в їхньому носієві, і проставляються на самому носієві і (або) супроводжувальній документації на нього. Установлюється на основі відповідних законів та відомчих переліків відомостей, що складають таємницю державну. Для інформації секретної, цілком секретної інформації та особливої важливості вводяться грифи "секретно", "цілком секретно" та "особливої важливості", для несекретної інформації, що містить службову таємницю, вводять гриф "для службового використання". Див. також відомості особливої важливості, відомості цілком таємні, відомості таємні.

ГРОШІ /деньги/ — металеві та паперові знаки, що є мірою вартості при купівлі й продажу.

Г. електронні /д. электронные/ — серії наборів цифр, що представляють собою банківські купюри і монети. Реалізація г. е. може бути як апаратною у вигляді карток, в яких використовується спеціальне програмне забезпечення, нанесене в мікросхему або магнітну смугу. Для захисту і збереження конфіденційності використовуються методи захисту криптографічні. За допомогою г. е. можна купувати товари в режимі прямого доступу, сплачувати перегляд фільмів за вимогою в інтерактивних телевізійних системах. Вони можуть замінити готівку і чеки для щоденних покупок та інших витрат.

Г. цифрові /цифровые деньги/ [digital money] — електронний аналог готівки.

ГРАФ /граф/ [graph] (від грец. $\gamma\rho\acute{\alpha}\varphi\omega$ — пишу, креслю, зображую) — модель математична (графічна схема) системи зв'язків між об'єктами довільної природи. Задавання г. зводиться до вказування непустої множини вершин графа, множини ребер і так званого інцидентора, що встановлює відповідність між ребрами та парами вершин.

ГРУПА /группа/ [group] — сукупність людей, об'єднаних спільністю інтересів, професії, діяльності, а також сукупність предметів, об'єднаних спільністю ознак.

Г. агентурна /г. агентурная/ — група агентів і нелегалів, яких об'єднує одне завдання, один об'єкт розвідки і які знаходяться на зв'язку однієї людини, куратора або резидента. В кожній агентурній групі може існувати декілька осередків, відокремлених один від іншого. Таке подрібнення необхідне для того, щоб провал одного агента або одного осередку не привів до провалу всієї агентури. Див. також мережа агентурна.

Г. інженерів Інтернету робоча /г. инженеров Интенета рабочая/ [Internet Engineering Task Force (IETF)] — група у складі групи Інтернету консультативної технічної (IAB), яка обновлює існуючі стандарти Інтернету і створює нові. Члени IETF обмінюються матеріалами з дослідницькою групою Інтернету і

рекомендують стандарти для групи керування інженерами Інтернету [Internet Engineering Steering Group (IESG)], що співпрацює разом із IAB. IETF розроблює дев'ять напрямків: додатки, міжмережні служби, керування мережами, функціональні вимоги, маршрутизація, безпека, службові додатки, транспорти і послуги користувачам.

Г. Інтернету дослідницька /г. Интернета исследовательская/ [Internet Research Task Force (IRTF)] — проблемний підрозділ групи Інтернету консультативної технічної, який займається протоколами, додатками, архітектурою і технологіями Інтернету. Ним керують голова IRTF і група керування дослідженнями Інтернету [Internet Research Steering Group (IRSG)].

Г. Інтернету консультативна технічна /г. Интернета консультативная техническая/ [Internet Architecture Board (IAB)] — група у складі товариства Інтернету, яка наглядає за архітектурою і розвитком протоколів Інтернету, створює стандарти, керує серією документів RFC і готує різноманітні періодичні видання. IAB співпрацює також з іншими організаціями, що займаються технічними питаннями і стандартами Інтернету. До складу IAB входять дві основні підпорядковані групи — група інженерів Інтернету робоча і група Інтернету дослідницька.

Г. керування дослідженнями Інтернету /г. управления исследованиями Интернета/ [Internet Research Steering G. (IRSG)] — див. група Інтернету дослідницька.

Г. керування інженерами Інтернету /г. управления инженерами Интернета/ [Internet Engineering Steering G. (IESG)] — див. група інженерів Інтернету робоча.

Г. соціальна /г. социальная/ — спільність людей, що існує в масштабах суспільства, та розвивається відповідно до соціально-психологічних закономірностей прояву масової психіки. Див. також соціальна психологія. Розрізняють наступні види соціальних груп: за розміром — великі, середні, малі групи та мікрогрупи; за суспільним статусом — формальні (офіційні) і неформальні (неофіційні); за стійкістю взаємозв'язків

членів групи — реальні (контактні) і умовні (формально виділені за будь-якою ознакою); за рівнем розвитку — дифузні, асоціації, корпорації, колективи; за значимістю для членів — референтні (еталонні) і нереферентні.

Г. соціальна велика /г. социальная большая/ — спільність людей, що існує в масштабах суспільства, та розвивається відповідно до соціально-психологічних закономірностей прояву масової психіки і на відміну від груп соціальних малих не припускає обов'язкових особистих контактів. В г. с. в., як правило, створюються загальноприйняті норми поведінки, культурні цінності і традиції, суспільна думка і масові рухи. До г. с. в. відносяться класи, соціальні прошарки, етноси (нації, народності), релігійні конфесії, партії і суспільні організації, вікові групи і т. ін.

Г. соціальна мала /г. малая социальная/ — невелика спільність людей, між членами якої існують безпосередні контакти, а також ієрархічні відносини верховенства (лідерства, популярності, авторитетності, симпатії/антипатії) і підпорядкування. До малих груп відносяться сім'ї, невеликі військові підрозділи, сусіди, дружні компанії і т.ін. Кожна група має певну структуру, що складається під впливом як зовнішнього середовища, так і внутрішньогрупових міжособистістних відносин. Розрізняють групи соціальні формальні і неформальні малі. У групах, де встановлюються дуже міцні міжособистістні зв'язки (екіпаж літального апарату, бойової машини, обслуга РЛС і т. ін.), спостерігається надто високий рівень спільності поглядів, вкрай рідко відмічаються будь-які окремі думки (а тим більше дії), що йдуть врозріз із думкою більшості. Установлено, проте, що лідери малих груп більше підпадають впливу ззовні, ніж рядові члени.

Г. соціальна неформальна /г. социальная неформальная/ — група соціальна мала, яка сама створює свою структуру. Вона складається на основі особистих симпатій і антипатій.

Г. соціальна формальна /г. социальная формальная/ — група соціальна мала, що має задану структуру і функціонує у відповідності із заздалегідь установленими, офіційно фіксованими метою, завдання-

ми, інструкціями, статутами. Характерно, що в г. с. ф. також мають місце неформальні відносини між її членами, тому успіх діяльності г. с. ф. в багатьох випадках залежить від того, наскільки співпадають її формальна формальна й неформальна структури.

Д

ДАЛЬНІСТЬ /дальность/ [distance, range] — відстань між двома певними точками.

Д. радіорозвідки /д. радиоразведки/ — максимальна відстань до джерела радіовипромінювання, при якому виявляється його робота засобами радіорозвідки або розвідки радіотехнічної. Д. р. у вільному просторі визначається за формулою

$$D_{ri} = \frac{\lambda}{4\pi}\sqrt{\frac{P_s g g_s \gamma \eta}{\nu P_{rmin}}},$$

де P_s — потужність, що випромінюється джерелом радіовипромінювання, Вт; g — коефіцієнт підсилення антени джерела радіовипромінювання в напрямку на засіб розвідки; g_s — коефіцієнт підсилення антени засобу розвідки; γ — коефіцієнт, що враховує неспівпадання поляризації антен засобу розвідки і джерела радіовипромінювання (при розрахунках приймається рівним 0,5); ν — коефіцієнт передавання потужності сигналу з антени на вхід радіоприймача засобу розвідки (при розрахунках приймається рівним 0,5); P_{rmin} — гранична чутливість радіоприймача, яка визначається потужністю його власних шумів, віднесених до входу; ν — коефіцієнт перевищення сигналу над рівнем шумів радіоприймача, необхідний для надійного спрацьовування апаратури засобу розвідки. Приведена формула не враховує загасання при розповсюдженні радіохвиль в атмосфері, яке особливо сильно проявляється в міліметровому і короткохвильовій частині сантиметрового діапазону. Для уточнення д. р. в даному випадку враховують коефіцієнт поглинання електромагнітної енергії на одиницю шляху в атмосфері, виражений, наприклад, у Дб/км. Для хвиль міліметрового, сантиметрового і дециметрового діапазонів, де явище рефракції виражене вкрай слабо, ма-

ксимальна д. р. обмежується дальністю прямої видимості. Дальність прямої видимості при нормальній атмосферній рефракції визначається за формулою

$$D_{max} = 4,1(\sqrt{h_s} + \sqrt{h_{ri}}),$$

де D_{max} — у км; h_s — висота антени джерела радіовипромінювання в м; h_{ri} — висота антени засобу розвідки над земною поверхнею в м.

Д. розповсюдження носіїв інформації /д. распространения носителей информации/ — максимальна відстань, на якій можливе добування інформації дистанційне.

ДАНІ /данные/ [data] — факти і ідеї, подані у формалізованому вигляді, що дозволяє передавати або оброблювати ці факти і ідеї за допомогою деякого процесу (за допомогою технічних засобів). Див. оброблення даних автоматичне, система оброблення даних, база даних.

Д. вірчі (мандат) /д. верительные/ [credentials] — дані для встановлення істинності особи, за яку видає себе користувач ресурсу обчислювальної системи.

Д. з обмеженим доступом /д. с ограниченным доступом/ [confidential d.] — закриті дані, коло користувачів якими визначається відповідними нормативними документами.

Д. закриті (захищені) /д. закрытые (защищенные)/ [restricted d.] — дані, доступні обмеженому колу користувачів. Як правило, обмеження доступу досягається системою паролів.

Д. зашифровані /д. зашифрованные/ [black d., enciphered d., cryptographically protected d.] — інформація, до якої застосована операція зашифровування.

Д. колективного користування /д. коллективного использования/ [public d.] — загальнодоступна інформація: дані, доступні великій кількості користувачів як у пакетному, так і в інтерактивному режимах.

Д. особисті (індивідуальн, приватні) /д. личные (индивидуальные, частные)/ [private d.] — дані,

власником і користувачем яких є окрема особа (обмежена група осіб, окрема установа).

Д. персональні /д. персональные/ [personal d.] — див. інформація особиста.

Д. розвідувальні /д. разведывательные/ [intelligence d.] — оброблені відомості розвідувальні, що містять висновки про діяльність джерел (об'єктів) розвідки.

Д. секретні /д. секретные/ [confidential d.] — дані закриті, яким наданий певний гриф (ступінь) секретності.

Д., що зберігаються /сохраняемые д./ [stored d.] — дані, розташовані на зовнішньому носії або в hyperlinkp8112пристрої запам'ятовуючому постійному.

ДАТЧИК /датчик/ [generator, measuring transducer] — пристрій, який перетворює фізичну величину в сигнали для оброблення технічними засобами.

Д. випадкових чисел /д. случайных чисел/ [random number g.] — пристрій для одержання послідовності незалежних випадкових чисел із розподілом імовірностей, який є близьким до рівномірного розподілу в інтервалі від 0 до 1), при якому ймовірність попадання випадкової величини в будь-який відрізок, що входить у даний інтервал, дорівнює довжині цього відрізка.

ДАХ /крыша/ — організація (заклад), роботою в якому розвідник прикриває свою діяльність розвідувальну (контррозвідувальну).

ДЕЗІНФОРМАЦІЯ /дезинформация/ [misleading information, misinformation] (від франц. des... та інформація) — 1) Свідоме поширення неправильної інформації. 2) Навмисне поширення неправильних відомостей про власні збройні сили і плани воєнних дій, щоб увести в оману противника. 3) Спосіб захисту інформації технічного, що полягає у формуванні свідомо хибної (фальшивої) інформації для виключення несанкціонованого одержання істинної.

ДЕЗІНФОРМУВАННЯ /дезинформирование/ [deception message] — 1)Метод інформаційного приховування інформації, який полягає в перетворенні (трансформації) вихідного портрета інформаційного в новий, такий що відповідає фальшивій інформації семантичній або фальшивій структурі ознаковій, та "нав'язуванні" нового портрета органу розвідки або зловмисникові. Д. відноситься до числа найбільш ефективних способів захисту інформації. Д. надає власникові інформації, що потребує захисту, запас часу, який зумовлений перевіркою розвідкою достовірності одержаної інформації. Наслідки рішень, прийнятих противником на основі фальшивої інформації, можуть бути для нього гіршими у порівнянні з рішеннями, що приймаються при відсутності інформації. Основна проблема д. полягає в забезпеченні достовірності фальшивого інформаційного портрета. Д. здійснюється шляхом підгонки ознак інформаційного портрета об'єкта, що потребує захисту, під ознаки інформаційного портрета фальшивого об'єкта, який відповідає раніше розробленій версії. Розрізняють наступні способи Д.: дезінформування заміною реквізитів інформаційного портрета; дезінформування ознаками з різних інформаційних портретів реальних об'єктів; дезінформування сполученням істинних і фальшивих ознак; дезінформування зміною інформаційних вузлів. Як правило, використовуються різноманітні комбінації способів д. 2) Спосіб впливу психологічного, що полягає в намірі подання противникові такої інформації, яка вводить його в оману відносно справжнього положення справ. Д. включає в себе використання явно фальшивих даних і відомостей. В цьому випадку воно стає обманом. Заходи з д. повинні здійснюватися за єдиним замислом; із ретельним погодженням пропорцій правди й брехні (при максимальному використанні правдоподібної інформації); з обов'язковим приховуванням справжніх намірів, мети й завдань, що вирішуються військами. Д. широко застосовується в усіх видах стратегічних операцій.

Д. заміною реквізитів інформаційного портрета /д. заменой реквизитов информационного портрета/ — спосіб дезінформування, який використовується у випадку, коли портрет інформаційний об'єкта захисту схожий на інформаційні портрети інших "відкритих" об'єктів і не має специфічних інформативних

ознак. В цьому випадку обмежуються розробленням і підтримуванням версії про інший об'єкт, видаючи за його ознаки об'єкта, що потребує захисту.

Д. зміною інформаційних вузлів /д. заменой информационных узлов/ — спосіб дезінформування, що полягає у зміні тільки вузлів інформаційних із збереженням незмінною всієї іншої частини інформаційного портрета.

Д. ознаками з різних інформаційних портретів реальних об'єктів /д. признаками из разных информационных портретов реальных объектов/ — спосіб дезінформування, спрямований на підтримування версії з ознаками, що беруться з різних портретів інформаційних реальних об'єктів. Шляхом різноманітних сполучень таких ознак можна нав'язати протилежній стороні фальшиве уявлення про об'єкти, що потребують захисту, без імітації додаткових ознак.

Д. правильне /д. правильное/ — передавання органу керування неспотвореної інформації про неправдиву обстановку.

Д. противника в інформаційно-обчислювальній мережі /д. противника в информационно-вычислительной сети/ — санкціоноване розповсюдження в ІОМ інформації про плани, способи дій і наміри керівництва корпорації, яка не відповідає дійсності.

Д. сполученням істинних і фальшивих ознак /д. соединением истинных и ложных признаков/ — спосіб дезінформування, заснований на заміні фальшивими ознаками незначної, але найбільш цінної інформації, що відноситься до об'єкта, який потребує захисту, та їхнє використання поряд із рештою істинних ознак.

ДЕЗОРГАНІЗАЦІЯ /дезорганизация/ [disorganization] (від франц. désorganisation — розлад) — відсутність організованості, порушення порядку, дисципліни, нормальної діяльності, розладнаність, розвал.

Д. противника в інформаційно-обчислювальній мережі /д. противника в информационно-

вычислительной сети/ — дії, спрямовані на дезорієнтацію противника відносно об'єкта атаки, що цікавить його (інформаційного ресурсу, інформаційної системи, елемента ІОМ), а також дії з руйнування технологічно взаємозв'язаних засобів інформаційної війни, що застосовуються противником в ІОМ.

ДЕЙТАГРАМА IP /дейтаграмма IP/ [IP datagram] — базова одиниця даних, що пересилаються в мережах Інтернету. Д. IP складається із заголовка і даних, які часто називають корисним навантаженням (payload). Заголовок д. містить адреси відправника і одержувача.

ДЕКОДЕР /декодер/ [decoder] (від франц. decoder — розшифровувати) — 1) Пристрій чи стандартна програма, що перетворює закодовані дані у первинну форму. Це іноді також означає заміну одного коду на інший. 2) Логічний пристрій, який формує один або більше виділених вихідних сигналів, що базуються на комбінації вхідних сигналів, які він одержує.

ДЕКОДУВАННЯ /декодирование/ [decoding] — перетворення кодованих даних у форму, яку вони мали до кодування; операція, обернена кодуванню.

ДЕМАСКУВАННЯ /демаскирование/ (від франц. demasquer — зняти маску) — порушення маскування, розкривання, виділення об'єктів, що потребують захисту, перед противником.

ДЕМОДУЛЯЦІЯ /демодуляция/ [demodulation] (від лат. de... і модуляція) — 1) Виділення низькочастотних коливань із високочастотних модульованих коливань. 2) Процес, зворотний модуляції. Полягає у відновленні модулюючого сигналу.

ДЕПОНУВАННЯ /депонирование/ [deposit] (від лат. depono — кладу) — здійснення внесків, вкладів.

Д. ключів /д. ключей/ [key escrow] — див. криптосистеми з депонуванням ключів.

ДЕПРЕСІЯ /депрессия/ [depression] — афективний емоційний стан, що характеризується негативним фоном. Людина в стані д. зазнає важких, нестерпних переживань пригніченості, туги, відчаю. Її потяги,

мотиви, вольова активність, самооцінка різко знижені. Зміненим виявляється і відчуття часу, який тече нестерпно довго. Для поведінки людей у стані д. характерні уповільненість, безініціативність, швидка втомлюваність, що в сукупності призводить до різкого падіння продуктивності діяльності.

ДЕРЖАВА /государство/ [State, country, nation] — сукупність офіційних органів влади в цій чи іншій країні, основний заклад і спосіб політико-правової організації життя суспільства на чолі з одноосібним або колективним правителем, органами виконавчої та інших видів влади і вертикальною системою управління, за допомогою якої здійснюється влада, охороняється існуючий лад, забезпечується нормальне життя людей. Устрій д. оформлюється і закріплюється в конституціях і відповідних нормах права. Основні ознаки д.: наявність особливої системи органів і закладів (механізм д.), що здійснюють владні функції (внутрішні і зовнішні); право, що закріплює певну систему норм, санкціонованих д.; певна територія з населенням, на яку розповсюджується юрисдикція даної д.

ДЕСКРЕМБЛЕР /дескремблер/ [descrambler] (від лат. de... і скремблер) — пристрій для виділення з прийнятого сигналу скрембльованого вхідного повідомлення. Див. скремблювання, скремблер.

ДЕТЕКТОР /детектор/ [detector] (лат. detector — відкривач, від detego — виявляю) — 1) Пристрій для детектування електричних коливань. 2) Прилад для виявлення різних фізичних явищ, частинок і випромінювання.

Д. брехні /д. лжи/ [stress analyzer] — 1) Засіб, призначений для перевірки правдивості людей. Визначення брехні засновується на тому факті, що людина, яка говорить неправду, відчуває в цей момент деякий психологічний стрес, що викликає, в свою чергу, певні фізіологічні зміни в її організмі. Існують три основні типи д. б.: поліграф (polygraph, psychological stress evaluator), сигналізатор психологічного стресу (psychological stress signalizer) і аналізатор стресу за голосом (vocal stress analyzer). 2) Алгоритм роботи деякого людино-машинного комплексу, який дозволяє організувати інформаційну взаємодію з об'єктом, що досліджується, таким чином, щоб у процесі цієї взаємодії виявити наявність у об'єкта, що досліджується,

прихованих знань із певної теми.

Д. руху системи відеоконтролю /д. движения системы видеоконтроля/ [motion d.] — пристрій, призначений для сповіщення оператора системи відеоконтролю або вмикання відеомагнітофона при зміні картинки на одній або декількох камерах телевізійних. Детектори руху випускаються у вигляді окремих блоків, що сполучаються з іншими елементами системи відеоконтролю, або ними можуть обладнуватися мультиплексори. Ступінь зміни зображення (швидкість руху зловмисника), що викликає сигнал тривоги, встановлюється оператором за допомогою регулятора порога спрацьовування.

ДЕШИФРАТОР /дешифратор/ [decipherer] (від франц. déchiffrer — розбирати, відгадувати) — 1) У криптології — пристрій, призначений для перетворення шифрограм у вихідні повідомлення. Зворотну функцію виконує шифратор. 2) В обчислювальній техніці [decoder] (інша назва декодер) — комбінаційна схема, яка реалізує систему з 2^n булевих функцій, кожна з яких є конституентою одиниці від n змінних. Наприклад, дешифратор адресу [address decoder] реалізує вибір комірки пам'яті за сигналами на адресній шині.

ДЕШИФРУВАННЯ /дешифрование/ [deciphering] (від франц. déchiffrer — розбирати, відгадувати) — 1) Читання (розшифровування) тексту, написаного умовними знаками (шифром), тайнописом. 2) Процес перетворення шифртексту у відкритий текст без знання ключа та, можливо, при невідомому алгоритмі шифрування; процес, зворотний процесу зашифровування (див. також Розшифровування).

Д. зображень /д. изображений/ [interpretation] — виявлення, розпізнавання або оцінка об'єктів (цілей) за їхніми зображеннями (фотографічному, телевізійному, тепловому, радіолокаційному, голографічному і т. ін.).

ДЖЕРЕЛО /источник/ [source] — те, що дає початок чому-небудь, звідки виходить що-небудь.

Д. відкриті /и. открытые/ — джерела інформація, доступні широкому загалу, головним чином, засоби

масової інформації (преса, телебачення, і радіо). Див. також інформація з відкритих джерел.

Д. даних /и. данных/ [data origin] — людина або пристрій, які здійснюють формування і введення даних в ЕОМ.

Д. дестабілізуючих факторів /и. дестабилизирующих факторов/ [destabilizing factor s.] — див. фактори дестабілізуючі.

Д. загроз інформаційно-психологічній безпеці /и. угроз информационно-психологической безопасности/ — потенційні джерела впливу деструктивного на психіку людей. До таких джерел можна віднести: джерела інформування (наприклад, засоби масової інформації); програми для ЕОМ; генератори фізичних полів і випромінювання; фізичні особи, що мають від природи здатність несвідомого впливу на інших осіб, і об'єднання цих осіб; зони геопатогенні; зони антропогенні.

Д. звуку /и. звука/ [audio s.] — будь-які явища, що викликають локальну зміну тиску або механічної напруги. Широко розповсюджені д. з. у вигляді твердих тіл, що коливаються (наприклад, дифузори гучномовців і мембрани телефонів, струни і деки музичних інструментів); в діапазоні ультразвукових хвиль — це пластинки і стрижні з матеріалів п'єзоелектричних або матеріалів магнітострикційних. Цілий клас д. з. складають перетворювачі акустоелектричні.

Д. інформації /и. информации/ [information s.] — в безпеці інформаційній — суб'єкти і об'єкти, від яких інформація (дані і відомості) може поступати до несанкціонованого одержувача (зловмисника). Цінність такої інформації визначається інформативністю д. і. Основними д. і. є наступні: люди; документи; продукція; вимірювальні датчики; інтелектуальні засоби оброблення інформації; чернетки і відходи виробництва; матеріали і технологічне обладнання.

Д. надійне /и. надежный/ — стандартне, активно використовуване джерело розвідувальних відомо-

стей, надійність якого не потребує перевірки.

Д. небезпечного сигналу /и. опасного сигнала/ [insecure signal s.] — джерело, від якого можуть розповсюджуватися несанкціоновані сигнали з інформацією, що належить захисту. Д. н. с. можуть виникати випадково (за рахунок побічного випромінювання і наведень) або створюватися зловмисниками. Д. н. с. є радіо і електротехнічні елементи і пристрої будь-яких радіоелектронних засобів і систем. Існує велика різноманітність таких засобів і систем. За призначенням їх можна розділити на основні засоби і системи (такі, що забезпечують оброблення, зберігання і передачу інформації, яка потребує захисту) і допоміжні засоби та системи (такі, що забезпечують оброблення, зберігання і передачу всієї іншої інформації). За фізичними властивостями засобів д. н. с. можна класифікувати наступним чином: перетворювачі акусто-електричні; випромінювачі низькочастотних сигналів; випромінювачі високочастотних сигналів; паразитні зв'язки і наведення. Джерела функціонального сигналу відносяться до небезпечних у випадку, коли вони цікавлять зловмисника або противника і до них не застосовані заходи безпеки інформації.

Д. повідомлень /и. сообщений/ [message origin] — частина комунікаційної системи, яка породжує повідомлення; пристрій, програма або система, що формує повідомлення.

Д. розвідувальних відомостей /и. разведывательных сведений/ [intelligence s.] — суб'єкти і об'єкти, від яких інформація (дані і відомості) може поступати до розвідників або розвідувальних підрозділів.

Д. сигналу /и. сигнала/ [signal s.] — складова частина об'єкта, що випромінює сигнал. Д. с. містить інформацію про ознаки сигналу (див. інформація ознакова). Якщо об'єкт відбиває поля зовнішніх джерел, то він одночасно стає джерелом інформації про об'єкт і д. с. В цьому випадку сигнал містить інформацію про ознаки об'єкта видові або сигнальні.

Д. функціонального сигналу /и. функционального сигнала/ [functional signal s.] — джерело сигналу, створене для забезпечення зв'язку між санкціонованими абонентами. До д. ф. с. відносяться: передавачі си-

стем електрозв'язку; передавачі систем радіотехнічних; випромінювачі акустичних систем гідролокаторів; сигнали умовні.

ДИКТОФОН /диктофон/ [dictaphone] (від лат. dicto — диктую і грец. *φωνή* — звук, голос) — див. аудіомагнітофон.

ДИРЕКТОР /директор/ [director] (франц. directeur — від лат. dirigo — спрямовую, керую) — 1) Керівник підприємства, установи. 2) В деяких країнах — керівник служби розвідувальної (наприклад, директор Агентства національної безпеки США, директор агентства урядового зв'язку та інформації Федерального РФ і т. ін.).

Д. центральної розвідки /д. центральной разведки/ [d. of central intelligence] — назва посади керівника управління розвідувального Центрального США. Див. також. управління розвідувальне Центральне, Агентство національної безпеки.

ДИСК /диск/ [disk] (грец. *δισκός* — 1) Плоский круг, кругла пластина. 2) Носій інформації, що являє собою круглу пластину, яка покрита шаром матеріалу, здатного запам'ятовувати і відтворювати інформацію. Місцем розташування інформації є концентричні доріжки. Розрізняють диски магнітні, магнітооптичні і оптичні.

Д. віртуальний (тимчасовий, електронний) /д. виртуальный (временный, электронный)/ [virtual d.] — 1) Логічний підрозділ фізичного пакета дисків, що має свій особистий віртуальний адрес. 2) Програмне подання (імітація) фізичного диска магнітного у віртуальній системі операційній.

Д. магнітний гнучкий (ГМД) /д. магнитный гибкий (ГМД)/ [floppy d.] — змінний диск магнітний на гнучкому носії. Використовується як пам'ять зовнішня прямого доступу. Випускаються диски діаметром

133 мм (5,25 дюйма) і 76 мм (3,5 дюйма).

Д. жорсткий (твердий) /д. жесткий (твердый)/ [hard d.] — диск магнітний на металевій основі.

Д. змінний /д. сменный/ [exchange d. store] — диск (пакет дисків магнітних), який можна знімати з нагромаджувачів, замінюючи його іншим диском.

Д. логічний /д. логический/ [logical d.] — частина вінчестера, яка має окреме ім'я (C, B, D і т. ін.) і використовується як самостійний диск магнітний.

Д. магнітний /д. магнитный/ [magnetic d.] — диск, поверхня якого покрита феромагнітним шаром.

Д. магнітооптичний /д. магнитооптический/ [magnetooptic d.] — диск, в якому для зберігання і пошуку інформації використовується магнітооптичний ефект: запис даних виконується лазерним променем й магнітним полем, зчитування даних — лазерним променем, стирання даних — лазерним променем, який розмагнічує відповідні ділянки поверхні, розігріваючи їх до температури вище точки Кюрі.

Д. оптичний /д. оптический/ [optical d.] — диск, призначений для запису і зчитування інформації за допомогою лазерного променя. Стирання та зміни інформації не передбачено. Відомі диски типу CD-ROM (від Compact Disk — Read-Only Memory — компакт-диск-ПЗУ) та диски типу DVD-ROM (від Digital Video Disk — цифровий відеодиск).

Д. системний /д. системный/ [system d.] — диск, на якому розташовані модулі системи операційної і з якого здійснюється її запуск.

Д. фіксований /д. фиксированный/ [fixed d.] — пристрій запам'ятовуючий на дисках магнітних з носієм, який не можна зняти.

ДИСКЕТА /дискета/ [diskette] — див. диск магнітний гнучкий (флоппі-диск).

Д. ключова /д. ключевая/ [key d.] — дискета, що містить ключі системи захисту інформації.

Д. системна /д. системная/ [system d.] — див. диск системний.

ДИСКОВОД /дисковод/ [disk drive] — механізм для встановлення дисків магнітних і роботи з ними. Є одним з вузлів нагромаджувача на дисках магнітних.

ДИСКОМФОРТ /дискомфорт/ — (від грец. $\delta\upsilon\sigma$..., лат. dis... — префікса, що надає поняттю, до якого додається, негативного або протилежного змісту і комфорт) — незручність, відсутність належних умов, потрібних для нормальної життєдіяльності людини, виконання певної роботи; невигода.

ДИСКУРСИВНИЙ /дискурсивный/ [discursive] (лат. discursivus, від discursus — міркування, довід, аргумент) — той, що здійснюється шляхом логічних міркувань, розсудковий, опосередкований. Часто застосовується поняття дискурсу [discurse], що має багато значень: лекція, промова, трактат, розмова, бесіда, висловлювання, надфразна єдність, текст. В комунікативістиці ідея дискурсивності синомізується з поняттям комунікабельності тексту як тканини, фактури і структури різноманітних мов інформації у їхньому розмовному прояві в різних соціокультурних контекстах.

ДИСЛОКАЦІЯ /дислокация/ [stationing, distribution (of troops)] (від дис... і лат. locus — місце) — розміщення (розквартирування) військових частин, з'єднань і установ збройних сил.

ДИСОНАНС /диссонанс/ (франц. dissonance, від лат. dissonans — різноголосий, різнозвучний) — відсутність у чомусь гармонії, невідповідність слів або поведінки когось настроям, переконанням інших людей.

Д. когнітивний /д. когнитивный/ — неузгодженість, суперечливість між інтелектуально-пізнавальними і всіма іншими (споживчо-мотиваційними, емоційно-вольовими, комунікаційно-поведінковими) компонентами психіки людини. Наявність д. к. викликає у людини прагнення зменшити

його або хоча б перешкодити його подальшому збільшенню. Прояв цього прагнення: недовірливе відношення до нової інформації, або зміна поведінки у відповідності з новою інформацією, або переосмислення попередньої інформації в новому ракурсі.

ДИСПЕТЧЕР /диспетчер/ [dispatcher] (англ. dispatcher, від dispatch — швидко виконувати) — оперативний розпорядник, який забезпечує виконання виробничих графіків, координує за допомогою системи організаційно-технічних заходів взаємодію всіх ланок підприємства.

Д. доступу /д. доступа/ [security monitor] — 1) Реалізація концепції абстрактного автомата, яка забезпечує дотримання правил розмежування доступу і характеризується такими трьома особливостями: забезпечує безперервний і повний контроль за доступом, захищений від модифікації і має невеликі розміри. 2) Технічні, програмні і мікропрограмні компоненти комплексу засобів захисту інформації, що реалізують деяку абстрактну машину, яка виконує функції посередника при всіх зверненнях суб'єктів до об'єктів; ядро захисту.

ДИСПЛЕЙ /дисплей/ [display] (англ. display, букв. — показ, демонстрування) — пристрій для відображення інформації в ЕОМ. Розрізняють дисплеї алфавітно-цифрові і графічні.

Д. алфавітно-цифровий /д. алфавитно-цифровой/ [alpha-numeric d.] — дисплей, який забезпечує введення і відображення алфавітно-цифрових знаків — букв, цифр та інших знаків.

Д. графічний /д. графический/ [graphic d.] — дисплей, призначений для відображення інформації, яка подається в графічній або графічній і алфавітно-цифровій формі одночасно.

Д. кольоровий /д. цветной/ [color d.] — дисплей з екраном кольорового зображення.

Д. монохромний /д. монохромный/ [monochrome d.] — однокольоровий дисплей, наприклад, з чорно-

білим (black-and-white) зображенням.

Д. плазмовий /д. плазменный/ [plasma-panel d.] — дисплей, зображення на екрані якого створюється з точкових розрядів, які виникають між електродами.

ДІАГРАМА /диаграмма/ [diagram] (від грец. *διάγραμμα* — малюнок, фігура, кресленик) — графічне зображення співвідношень між різними величинами, які порівнюються.

Д. спрямованості антени /д. направленности антенны/ [antenna direction d.] — графічне зображення рівня сигналу антени (випромінюваного або того, що приймається) в залежності від кута обернення антени в горизонтальній і вертикальній площинах. Д. с. а. зображуються в прямокутних і полярних координатах. Діаграми спрямованості можуть мати різноманітний покраяний характер, який визначається механічною конструкцією і електричними параметрами. Пелюстка д. с. а. з максимумом потужності випромінюваного або того, що приймається, електромагнітного поля називається головною або основною пелюсткою, а решта — боковими і задніми. Співвідношення між величинами потужності основної пелюстки у порівнянні з рештою пелюсток характеризує спрямовані властивості антени. Ширина головної пелюстки вимірюється кутом між прямими, проведеними з початку полярних координат до значень д. н. а., які відповідають половині максимальної потужності випромінювання або 0,707 напруги електричного сигналу приймальної антени. Чим вужча ширина д. с. а., тим вищий її коефіцієнт спрямованої дії.

ДІАПАЗОН /диапазон/ [range, band, bandwidth] (від грец. *διάπασῶν* — всеструнний інтервал, октава) — 1) Звуковий обсяг голосу, музичного інструмента, звукоряду, мелодії тощо. 2) Смуга частот (довжин радіохвиль), на яких здійснюється радіоприйом або радіопередача. 3) Межі зміни деякого параметра.

Д. динамічний /д. динамический/ [signal dynamic r.] — відношення найбільшого і найменшого миттєвих значень потужності або напруги сигналу, яких він реально може набувати в процесі вимірювання. Як

правило, використовують логарифм цього відношення.

Д. динамічний радіоприймача /д. динамический радиоприемника/ [broadcasting receiver dynamic r.] — величина, яка характеризує можливості приймача приймати радіосигнали різної потужності. Оцінюється логарифмом відношення максимального рівня потужності сигналу, що приймається, до його мінімального рівня. Для підвищення д. д. р. застосовується пристрій автоматичного регулювання підсилення приймального тракту, який змінює його коефіцієнт підсилення у відповідності до рівня сигналу, що приймається.

Д. радіохвиль /д. радиоволн/ [wave r., wave b.] — визначена ділянка довжин радіохвиль, якій присвоєна умовна назва. За довжиною радіохвиль виділяють такі д. р.: декамегаметрових (10–100 Мм), мегаметрових (1–10 Мм), гектокілометрових (100–1000 км), міріаметрових (10–100 км), кілометрових (1–10 км), гектометрових (100–1000 м), декаметрових (10–100 м), метрових (1–10 м), дециметрових (10–100 см), сантиметрових (1–10 см), міліметрових (1–10 мм) та децимініметрових (0,1–1 мм) радіохвиль. В залежності від особливостей розповсюдження, а також генерування, випромінювання і приймання радіохвиль виділяють такі д. р.: наддовгих (довжиною понад 10 км), довгих (1–10 км), середніх (100–1000 м), коротких (10–100 м) та ультракоротких (довжиною до 10 см) радіохвиль.

Д. радіочастот /д. радиочастот/ [frequency b.] — означений безперервний інтервал радіочастот, в якому коливання та хвилі мають порівняні властивості і умовну назву. За частотою радіохвиль виділяють такі д. р.: вельминизьких (3–30 Гц), наднизьких (30–300 Гц), інфранизьких (0,3–3 кГц), дуже низьких (3–30 кГц), низьких (30–300 кГц), середніх (0,3–3 МГц), високих (3–30 МГц),дуже високих (30–300 МГц), ультрависоких (0,3–3 ГГц), надвисоких (3–30 ГГц), вельмивисоких (30–300 ГГц) та гіпервисоких (0,3–3 ТГц) радіочастот.

Д. частот радіоприймача /д. частот радиоприемника/ — інтервали радіочастот, в яких радіоприймач здійснює прийом радіосигналів. Д. ч. р. забезпечується шириною смуги пропускання селективних елементів вхідних фільтрів та інтервалом частот гетеродина. Настройка приймача на необхідний діапазон

або піддіапазон частот здійснюється шляхом переключення елементів вхідних контурів і контуру гетеродина, а настройка на частоту всередині діапазону (піддіапазону) — шляхом змінювання частоти гетеродина. В сучасних приймачах як гетеродин використовується пристрій — синтезатор частот, який створює множину (сітку) гармонічних коливань на стабілізованих фіксованих частотах з інтервалом, відповідно до кроку настройки приймача.

ДІЇ /действия/ [action, operation] — 1) Робота, діяльність, здійснення чого-небудь. 2) Операції, пов'язані з боротьбою збройною.

Д. з інформаційного захисту (акції з інформаційного захисту) /д. по информационной защиты (акции по информационной защите)/ — оборонні дії (акції) інформаційні, узгоджені за завданнями, місцем і часом застосування залучених до ведення боротьби інформаційної сил і засобів з метою забезпечення стійкості функціонування системи управління військами (силами) в умовах впливу інформаційного противника.

Д. інформаційні (акції інформаційні) /д. информационные (акции информационные)/ [information a.] — сукупність узгоджених за метою, завданнями, місцем і часом заходів, що проводяться силами і засобами, залученими для ведення боротьби інформаційної, протягом певного часу в певному районі (напрямку). Під час д. і. можуть здійснюватися удари інформаційні. Д. і. можна класифікувати за видами (наступальні і оборонні), масштабом (стратегічні, оперативно-стратегічні, оперативні, оперативно-тактичні і тактичні) і об'єктами впливу (інформаційні системи, морально-психологічний стан особового складу та їхня комбінація). До наступальних д. і. відносяться вплив інформаційний (акція інформаційна) та блокада інформаційна, до оборонних — дії (акції) з інформаційного захисту.

Д. несанкціонована /д. несанкционированное/ [unauthorized o.] — будь-яка недозволена дія, яка ви-

конується користувачем.

Д. несанкціонована в інформаційно-обчислювальній мережі /д. несанкционированное в информационно-вычислительной сети/ — вплив інформаційний на ресурси інформаційні, персонал, інформаційні системи мережі інформаційно-обчислювальної (ІОМ), елементи ІОМ і ІОМ у цілому, а також підготовка цього впливу.

ДІЯЛЬНІСТЬ /деятельность/ [action, activities, activity, work] — 1) Специфічна людська форма активного відношення до навколишнього світу, зміст якої складає його доцільна зміна і перетворення. 2) Робота, заняття в якій-небудь галузі. 3) Робота будь-яких закладів, органів влади. Типи, види і форми д. різноманітні: д. законодавча, парламентська, політична, адміністративна, організаторська, виховна освітня, наукова, інформаційна, військова, міжнародна, дипломатична і т. ін.

Д. безпечна /д. безопасная/ [safety a.] — для будь-якого підприємства або організації — діяльність, у процесі якої забезпечується фізична безпека (захист від посягань на життя персоналу), безпека економічна, безпека інформаційна та матеріальна безпека (збереження матеріальних цінностей від різного роду посягань, починаючи від крадіжок і закінчуючи загрозами пожежі або іншого стихійного лиха).

Д. інформаційна /д. информационная/ [information a.] — сукупність процесів збирання, накопичення, аналізу, перетворення, зберігання, пошуку і розповсюдження інформації (а також інших допоміжних процесів, що забезпечують ці основні процеси), що систематично здійснюються будь-якою організацією (установою, підрозділом, групою осіб і т. ін.).

Д. інформаційно-аналітична /д. информационно-аналитическая/ — сукупність процесів діяльності інформаційної, спрямованих на забезпечення керівництва відомостями, необхідними для прийняття рішень, а також опрацювання концептуальних пропозицій. Д. і.-а. є основним видом діяльності служб

інформаційно-аналітичних.

Д. науково-інформаційна /д. научно-информационная/ [scientific information a.] — галузь діяльності щодо задоволення потреб суспільства у науково-технічній інформації. До поняття д. н. і. входять збирання, перероблення аналітико-синтетичне, зберігання, пошук, розповсюдження науково-технічної інформації.

Д. патентно-інформаційна /д. патентно-информационная/ [patent information a.] — діяльність інформаційна, спрямована на забезпечення фахівців та організацій відомостями про результати науково-технічних досліджень і проектно-конструкторських розробок, заявлених чи визнаних винаходами, а також відомостями про характер та обсяг прав винахідників і проектувальників — власників патентів.

Д. розвідувальна /д. разведывательная/ — діяльність, основним змістом якої є добування, оброблення та доведення споживачам інформації, необхідної для прийняття рішень.

ДІЯЧ /деятель/ [figure, leader, statesman] — особа, яка відзначається своєю активністю та енергійністю на якій-небудь роботі, в якійсь галузі життя.

Д. інформаційний /д. информационный/ [information f.] — носій інформації, здатний вступати в відносини інформаційні (взаємодії) з іншими носіями інформації. Д. і. можна розглядати людину і комп'ютер, якщо вони мають відповідні інформаційні відносини. У структурі інформаційних відносин активний д. і. є суб'єктом (наприклад, орган керування), а пасивний — об'єктом (наприклад, об'єкт керування). При цьому структурованого д. і. (діяча-систему) називають інформаційною стороною.

ДОБРОЗИЧЛИВЕЦЬ /доброжелатель/ [well-wisher] — особа, яка добровільно пропонує свої шпигунські послуги противнику. Свого роду прихований перебіжчик і потенційний агент ворожої розвідки. Така людина, як правило, сама приходить в іноземне посольство або представництво іноземної спеціальної служби без попереднього встановлення зв'язку з ними і без вербування.

ДОБУВАННЯ /добывание/ [getting, procuring] — дія, спрямована на діставання, роздобування кого-,

що-небудь.

Д. даних і відомостей /д. данных и ведомостей/ [data p.] — активні дії сил та засобів органів розвідки, спрямовані на пошук об'єктів (джерел) інформації та її носіїв, виявлення їх, встановлення з ними контакту розвідувального, одержання даних і відомостей.

Д. інформації /д. информации/ [information p.] — сукупність заходів і дій, спрямованих на забезпечення контакту розвідувального з джерелом інформації та одержання від нього даних і відомостей. В найбільш загальному випадку д. і. являє собою процес, який починається з моменту поставлення завдання її споживачами до моменту подання даних і відомостей в органи збирання і оброблення інформації або безпосередньо користувачу. Д. і. здійснюється постійно легальними способами (див. добування інформації легальне) на основі принципів добування інформації, а при недостатності одержаної цими способами інформації — шляхом проведення таємних операцій (див. добування інформації нелегальне, операція розвідувальна).

Д. інформації без порушення державного кордону /д. информации без нарушения государственной границы/ — одержання інформації з носіїв, що розповсюджуються за межі зони контрольованої держави — державного кордону. В цьому випадку добувається тільки та інформація, носії якої можуть легально або нелегально перетинати кордон (див. носії інформації через державний кордон). У випадку носіїв-випромінювання з інформацією, добування інформації можливе наземними засобами добування інформації, розташованими за межами державного кордону (наприклад засоби радіо- і радіотехнічної розвідки, що перехоплюють радіосигнали з семантичною і ознаковою інформацією), засобами добування інформації зверху, розташованими на космічних апаратах або штучних супутниках Землі (засоби фото, телевізійного, радіолокаційного спостереження, радіо- і радіотехнічної розвідки), а також засобами добування інформації, розташованих на літальних апаратах (літаках-розвідниках, безпілотних літальних апаратах) і

кораблях, що літають та плавають вздовж повітряних і морських кордонів.

Д. інформації без фізичного проникнення в контрольовану зону /д. информации без физического проникновения в контролированную зону/ — одержання інформації з носіїв, що розповсюджуються за межі контрольованої зони. Для забезпечення добування інформації дистанційного органи добування застосовують найбільш чутливу апаратуру для приймання носія і добування з нього інформації (див. наземні засоби добування інформації), яка за своїми параметрами перевищує параметри кращих зразків апаратури побутового і навіть військового призначення.

Д. інформації дистанційне /д. информации дистанционное/ [remote data p.] — одержання інформації з носіїв, що розповсюджуються за межі зони контрольованої (приміщення, будівлі, території і т. ін.). Д. д. і. здійснюється в результаті спостереження, підслухування, перехоплення, збору носіїв інформації у вигляді матеріальних тіл (бракованих вузлів, деталей, демаскуючих речовин і т. ін.) за межами контрольованої зони.

Д. інформації легальне /д. информации легальное/ — одержання даних і відомостей з відкритих джерел інформації.

Д. інформації нелегальне /д. информации нелегальное/ — одержання даних і відомостей в результаті проведення таємних заходів спеціальними службами і органами розвідки (див. також шпіонаж, шпіонаж промисловий, шпіонаж технологічний. Н. д. і. застосовується для одержання найбільш цінних даних і відомостей.

ДОВЕДЕННЯ /доказательство/ [proof, proving] — 1) Дія за значенням довести, доводити. 2) Логічна форма встановлення істинності будь-якого судження на підставі інших суджень, істинність яких перевірена практикою.

Д. з нульовим знанням (без розголошення) /д. с нулевым знанием (без разглашения)/ [zero

knowledge p.] — протокол криптографічний для доведення одним з учасників протоколу іншому факту володіння певними секретними даними без розкриття цих даних. При цьому учасник, якому доводиться факт володіння, не отримує жодної інформації про секретні дані, якими володіє інший учасник.

ДОВІДКА-ДОСЬЄ /справка-досье/ — систематизована за тематикою і часом добірка матеріалів на одну тему. В залежності від обсягу наявної інформації вона може поділятися на рубрики (розділи). Для зручності користування розділи (рубрики) позначаються порядковими номерами, шифрами, назвами. Див. також досьє.

ДОКАЗОВІСТЬ /доказательность/ — характеристика змісту інформації підтверджувати істинність, правильність чого-небудь фактами, незаперечними доводами (див. вплив змісту інформації). Вона визначається логічністю, правдоподібністю і несуперечністю викладеного матеріалу. Складовою частиною д. є переконливість.

ДОКТРИНА /доктрина/ [doctrine] (лат. doctrina — вчення) — наукова або філософська теорія, політична система, керівний теоретичний або політичний принцип (наприклад, воєнна доктрина) або нормативна формула.

Д. влади /д. власти/ [d. of power] — один з найважливіших видів доктрин, що викладає систему уявлень про владу або погляди самої влади по цій чи іншій важливій для держави проблемі.

Д. воєнна /д. военная/ [military d.] — система офіційних поглядів і положень, що встановлюють напрям воєнного будівництва, підготовки держави і збройних сил до війни, способи і форми її ведення; розробляється політичним керівництвом держави. Основні положення д. в. зв'язані з характером суспільного устрою, державною політикою, рівнем розвитку виробничих сил, наукових досягнень і уявленнями про можливу війну.

ДОКУМЕНТ /документ/ [document] (від лат. documentum — повчальний приклад, взірець, доказ) —

матеріальний об'єкт із зафіксованою на ньому інформацією у вигляді тексту, звукозапису або зображення, призначений для передавання у часі і просторі з метою збереження і суспільного використання. До д. відноситься службова інформація, наукові публікації у відкритих і закритих виданнях, статті в газетах і журналах про діяльність організації або її співробітників, конструкторська і технологічна документація і т.ін. Документи — найбільш інформативні джерела інформації, так як вони містять, як правило, достовірну інформацію в обробленому і стисненому вигляді, особливо, коли вони підписані або затверджені. Що стосується інформативності різноманітних публікацій, то вони мають достатньо широкий діапазон оцінок: від дуже високої, коли описується відкриття, до навмисної або ненавмисної дезінформації.

Д. Internet-Drafts /д. Internet-Drafts/ — серія технічних документів про Інтернет, яка в основному використовується робочими групами групи Інтернету дослідницької. Ці чорнові документи мають силу тільки протягом шести місяців, після чого їх поновлюють, міняють, або виводять з обігу. Такі документи не нумерують, як документи RFC, їм присвоюють унікальні імена файлів.

Д. RFC /д. RFC/ [Request for Comments (RFC)] — серія технічних документів Інтернету, в яких докладно описані мережні протоколи і інтерфейси, а також розкриті інші теми Інтернету. Документи RFC пронумеровані. Наприклад, RFC 2000 — це "Internet Official Protocol Standard" від групи Інтернету консультативної технічної.

Д. архівний /д. архивный/ [archive d.] — документ, що зберігається або підлягає збереженню внаслідок його значимості для суспільства, а також такий, що має цінність для його власника.

Д. аудіальний /д. аудиальный/ [audio d., sound record] — документ, що містить запис фонетичної інформації і призначений для звукового відтворення інформації. Наприклад, диск оптичний, магнітна стрічка із записаною інформацією і т. ін.

Д. аудіовізуальний /д. аудиовизуальный/ [audio-visual d.] — документ, що містить одночасно запис

звуку та видимого зображення і призначений для аудіовізуального повідомлення. Наприклад, кінострічка.

Д. системи захисту інформації /д. системы защиты информации/ [data protection d.] — документи, що визначають структуру і алгоритм функціонування системи захисту інформації організації. Розрізняють документи системи захисту інформації керівні, нормативні і методичні.

Д. системи захисту інформації керівні /руководящие д. системы защиты информации/ [data protection low] — документи системи захисту інформації, що визначають порядок забезпечення захисту інформації і обов'язки посадових осіб по захисту інформації. Типовими керівними документами є: інструкція по захисту інформації в організації; положення про підрозділ організації, на який покладаються завдання забезпечення безпеки інформації; інструкції по роботі з грифованими документами; інструкції по захисту інформації про конкретні вироби.

Д. системи захисту інформації нормативні /д. системы защиты информации нормативные/ [data protection normative d.] — документи системи захисту інформації, які визначають перелік відомостей, що складають державну, воєнну, комерційну або будь-яку іншу таємницю. Такі документи є основними нормативними документами. Інші нормативні документи визначають максимально допустимі значення рівнів полів з інформацією і концентрації демаскуючих речовин на межах зони контрольованої, які забезпечують необхідний рівень безпеки інформації. Ці норми розроблюються відповідними відомствами, а для комерційних структур, які виконують недержавні замовлення, — фахівцями цих структур.

Д. електронний /д. электронный/ [electronic d.] — сукупність даних в пам'яті ЕОМ, призначених для сприйняття людиною з допомогою відповідних програмних і засобів апаратних. Може включати крім текстової, графічну і звукову інформацію та має нелінійну структуру.

Д. інформаційний розвідки /д. информационный разведки/ — доповідь, складена офіцером інформації (розвідником) для подання керівництву. Найважливіші критерії цінності д. і. р. — корисність та

своєчасність подання інформації.

Д. інформаційні органів психологічної війни /д. информационные органов психологической войны/ — сукупність спеціальних документів, що складаються в ході вивчення об'єктів психологічної війни. До таких документів відносяться: довідки-досьє, картотеки, формуляри на конкретні підрозділи і частини збройних сил противника. Крім того складаються інформаційні документи про ідеологічну (соціально-політичну) ситуацію в окремих країнах (регіонах), морально-політичний стан особового складу збройних сил і населення, політичне лице воєнних і державних діячів. На додаток до них накопичуються й узагальнюються відомості про поточні події в зарубіжних країнах, які можуть подаватися у формі зведень поточної інформації зарубіжних агентств, тематичних реферативних оглядів, вибіркових реферативних оглядів, довідкових матеріалів.

Д. нормативний /д. нормативный/ [normative d.] — офіційний документ, який містить певні правила, стандарти, нормалі, нормативи і умови.

Д. програмний /д. программный/ [program d.] — документ, який містить відомості, необхідні для розробки, виготовлення, експлуатації і супроводження забезпечення програмного.

ДОКУМЕНТАЦІЯ /документация/ [documents, documentation] — сукупність документів, ділових паперів, оформлених за єдиними правилами. Обґрунтування чого-небудь за допомогою документів. Існують різноманітні види д.: державна, цивільного призначення, графічна, інформаційного забезпечення, міжнародна, нормативна, програмна, робоча, секретна, експлуатаційна і т. ін.

Д. експлуатаційна /д. эксплуатационная/ [maintenance (service) d.] — документація конструкторська, яка містить відомості, необхідні для експлуатації виробу (використання за прямим призначенням, з технічного обслуговування, транспортування і зберігання). До д. е. відносяться технічні описи, інструкції з експлуатації, технічного обслуговування, монтажу, пуску, регулювання і обкатки виробу, формуляри, па-

спорти, відомості запасного майна і приладдя, відомості експлуатаційних документів і т. ін.

Д. інформаційного забезпечення /д. информационного обеспечения/ [information support d.] — частина документації проектної, яка містить рішення з інформаційної бази, системи класифікації і кодування та технологічного процесу оброблення інформації.

Д. ключова /д. ключевая/ [key d.] — сукупність документів, які містять відомості щодо створення, застосування і знищення ключів.

Д. конструкторська /д. конструкторская/ [design d.] — сукупність документів, які розроблюються і використовуються в ході проектування виробу, виготовлення дослідного зразка і при організації серійного виробництва виробу.

Д. математичного забезпечення /д. математического обеспечения/ [mathematical support d.] — частина документації проектної, яка містить опис алгоритмів, що застосовуються.

Д. нормативна (нормативно-технічна) /д. нормативная (нормативно-техническая)/ [normative d.] — вид документації технічної, що встановлює норми, правила, технічні і організаційно-методичні вимоги, обов'язкові або рекомендовані до застосування. Включає всі категорії і види стандартів, тактико-технічні (технічні) завдання, технічні умови, норми і правила, інструкції, методичні вказівки і т. ін. В залежності від категорії д. н. затверджується Держстандартом, міністерствами (відомствами) і підприємствами.

Д. організаційно-розпорядча /д. организационно-распорядительная/ [documents about organization and instruction] — найбільш загальна категорія керівницьких документів. Система д. о. р. включає організаційну, розпорядчу і довідково-інформаційну документацію. В організаційній документації реалізується такий вид організаційно-розпорядчого впливу, як установлення норм (правил), регулюючих діяльність системи управління. До організаційної документації відносяться положення, статути, правила, посадові інструкції. Організаційні документи встановлюють права органів керування та керівників видавати розпо-

рядчі документи: рішення, постанови, розпорядження, накази, вказівки.

Д. організаційного забезпечення /д. организационного обеспечения/ [organization d.] — частина документації проектної, яка містить рішення про організаційну структуру і інструкції персоналу.

Д. програмна /д. программная/ [software d.] — частина документації проектної, яка містить рішення із застосування програм і забезпечення програмного в цілому. Призначена для користувачів.

Д. програмного забезпечення /д. программного обеспечения/ [software d.] — те ж, що документація програмна.

Д. проектна /д. проектная/ [design d.] — частина документації технічної, яка містить проектні рішення на створення і експлуатацію системи, що створюється.

Д. технічна /д. техническая/ [hardware d.] — система текстових і графічних документів, що містять інформацію про технічні вироби (деталі, зразки, комплекси), технічні і технологічні процеси, затверджені встановленим порядком. Основні види д. т.: конструкторська, нормативно-технічна, технологічна.

Д. технічного забезпечення /д. технического обеспечения/ [hardware d.] — те ж, що документація технічна.

Д. технологічна /д. технологическая/ — документація технічна, що визначає технологічний процес виготовлення або ремонту виробу, комплектацію деталей, матеріалів, оснастки, технологічних документів і маршрут проходження виробу цехами (службами) підприємства. До т. д. відносяться технологічні карти, відомості і інструкції. Т. д. регламентується стандартами Єдиної системи технологічної документації.

ДОМЕН /домен/ [domain] (франц. domaine, від лат. dominium – володіння) — 1) Ділянка. 2) Частина адреси доменної, відділена крапками. Приклади: доменна адреса www.kubstu.ru, містить три д.: д. верхнього рівня ru (Росія), вкладений д. kubstu (КубГТУ) і вкладений у нього www (WWW-сервер). До інших

д. верхнього рівня відносяться: com — комерційні, gov — урядові, edu — навчальні, org — громадські організації, net — телекомунікаційні мережі, і національні д. різних держав: ru — Росія, jp — Японія, fr — Франція і т.ін. Звичайно для підтримки кожного д. (крім найнижчого рівня) використовується окремий сервер DNS. У такий спосіб утворюється ієрархія серверів DNS. На кожному DNS-сервері ведеться база даних про адреси IP (DNS-серверів їхніх вкладених доменів або кінцевих персональний комп'ютерів мережі). Д. ru керує спеціально створена для цього некомерційна організація RIPN у Москві.

Д. комп'ютерної системи /д. компьютерной системы/ [domain] — ізольована логічна область системи комп'ютерної, що характеризується унікальним контекстом, усередині якої об'єкти комп'ютерної системи володіють певними властивостями, повноваженнями і зберігають певні відносини між собою.

ДОПИТ /допрос/ [interrogation, examination, questioning] — спосіб одержання від полонених, перебіжчиків, біженців відомостей про противника, місцевість і т.ін. в інтересах виконання бойового (розвідувального) завдання.

Д. анкетний /д. анкетный/ — метод опитування, що проводиться за заздалегідь складеним переліком питань — анкетою, в якій допитуваний дає відповіді на питання в тому чи іншому вигляді. Д. а. може бути відкритим і анонімним. Питання анкет повинні формулюватися чітко і конкретно, бути зрозумілими, виключати можливість альтернативних відповідей. Особливість анонімних анкет полягає в тому, що опитуваний не вказує своє прізвище, ім'я і т.ін. Учасники анонімного опитування дають більш об'єктивну інформацію.

Д. груповий /д. групповой/ — метод опитування, який реалізують, як правило, через брак часу для проведення допитів індивідуальних. Д. г. дозволяє в короткий термін охопити значну кількість допитуваних, проте в ході його важко (а іноді і неможливо) одержати відповіді з найбільш важливих пунктів, тому

що допитувані в такій обстановці не завжди наважуються говорити відверто.

Д. індивідуальний /д. индивидуальный/ — найбільш ефективний метод опитування. Дозволяє встановити безпосередній контакт з допитуваним, фіксувати його психологічні реакції і т.ін. Разом з тим в ході д. і. можуть бути допущені елементи суб'єктивізму, що призводить до похибок при оцінці того чи іншого явища. Тому після проведення д. і. потрібна ретельна перевірка показань.

Д. письмовий /д. письменный/ — метод опитування, який використовується тоді, коли показання полоненого мають особливо важливе значення. Він ефективний у двох випадках: коли показання дають допитувані, які мають необхідні знання і кругозір; коли показання дають особи, що добровільно виявили готовність повідомити відомості, що являють певний інтерес.

ДОПУСК /допуск/ [clearance] — дія, що надає змогу або дозволяє кому-небудь увійти кудись, підійти до кого-, чого-небудь.

Д. до державної таємниці /д. к государственной тайне/ [secret (top secret) c.] — процедура оформлення права громадян на доступ до відомостей, що складають таємницю державну, підприємств, закладів і організацій — на проведення робіт з використанням таких відомостей. Допуск посадових осіб і громадян до державної таємниці здійснюється у добровільному порядку і передбачає відповідну процедуру допуску до державної таємниці. При цьому встановлюються три форми допуску, які відповідають ступеням секретності відомостей, що складають державну таємницю: до відомостей державної важливості, цілком секретних і секретних.

ДОСТОВІРНІСТЬ /достоверность/ [validity, adequacy] — 1) Форма існування істини, обґрунтованої яким-небудь способом (наприклад, експериментом, логічним доказом) для об'єкта, що пізнається (вивчається). 2) Властивість інформації бути правильно сприйнятою; ймовірність відсутності помилок.

Д. даних /д. данных/ [data v.] — ступінь відповідності даних, що зберігаються у пам'яті ЕОМ або

документах, реальному стану відображених ними об'єктів предметної області.

Д. добутої інформації /д. добытой информации/ — ступінь відповідності отриманої інформації дійсній обстановці. Д. д. і. досягається: позначенням часу здійснення подій, відомості про які отримують; ретельним вивченням та порівнянням даних, отриманих з різних джерел; перевіркою сумнівних відомостей; своєчасним викриванням дезінформаційних та маскувальних заходів противника; виключенням спотворення інформації, що передається за допомогою технічних засобів зв'язку. Для оцінки д. д. і. використовують наступні часткові показники: достовірність повідомлень (відносно відсутності неправдивих повідомлень і даних); розбірливість мови; імовірність помилкового або неспотвореного прийому дискретної одиниці (біта, символу, цифри, букви, слова).

Д. оброблення інформації /д. обработки информации/ [data processing v.] — функція ймовірності помилки, тобто події, яка полягає у тому, що інформація в системі не збігається у межах заданої точності з деяким її істинним значенням. Забезпечення необхідного рівня д. о. і. є однією з основних умов ефективного функціонування автоматизованої системи. Необхідна д. о. і. досягається використанням різноманітних методів, реалізація яких потребує введення в системи оброблення даних надмірності інформаційної, часової або структурної. Достовірність даних досягається шляхом контролю достовірності та виявлення помилок у вихідних і виведених даних, їхня локалізація і виправлення. Умова підвищення достовірності — понижения долі помилок до допустимого рівня. В конкретних системах необхідна достовірність встановлюється з врахуванням небажаних наслідків, до яких може привести помилка, що виникла, і тих затрат, які необхідні для її попередження.

Д. передавання інформації /д. передачи информации/ [data transmission v.] — ступінь відповідності прийнятого повідомлення переданому.

Д. розвідувальної інформації /д. разведывательной информации/ — ступінь відповідності отриманої інформації розвідувальної дійсній обстановці. Д. р. і. досягається: позначенням часу здійснення подій,

відомості про які отримують; ретельним вивченням та порівнянням даних, отриманих із різних джерел; перевіркою сумнівних відомостей; своєчасним викриванням дезінформаційних та маскувальних заходів противника; виключенням спотворення інформації, що передається за допомогою технічних засобів зв'язку.

ДОСТУП /доступ/ [access] — 1) Взаємодія між суб'єктом і об'єктом доступу, що забезпечує обмін даними між ними. 2) У фізичній безпеці — можливість входу на територію, що знаходиться під захистом.

Д. алгоритмічний /д. алгоритмический/ [algorithmic a.] — доступ, що базується на обчисленні адреси за деяким алгоритмом.

Д. до відомостей, що складають державну таємницю /д. к ведомостям, которые составляют государственную тайну/ [secret (top secret) clearance] — санкціоноване повноважною посадовою особою ознайомлення конкретної особи з відомостями, що складають таємницю державну.

Д. до даних /д. к данным/ [a. to data] — надання даних системі оброблення даних чи одержання їх від неї шляхом виконання операцій пошуку, читання та (або) записування даних.

Д. до інформації /д. к информации/ [a. to information] — 1) Ознайомлення з інформацією, її оброблення, а саме, копіювання, модифікація або знищення інформації. 2) Наближення органів розвідки (агентів, технічних засобів) до джерел (або носіїв) інформації для забезпечення з ними контакту розвідувального. 3) В мережах обчислювальних — можливість одержання, оброблення та (або) порушення цілісності інформації. 4) Вид взаємодії двох об'єктів комп'ютерної системи, внаслідок якого створюється потік інформації від одного об'єкта до іншого і (або) відбувається зміна стану об'єкта.

Д. до файла /д. к файлу/ [file a.] — перегляд, модифікування, заміна або вилучення файла, а також перегляд і маніпулювання його атрибутами.

Д. за ключем /д. по ключу/ — те ж, що доступ ключовий.

Д. ключовий /д. ключевой/ [keyed a.] — спосіб доступу, при якому для звернення до запису в базі даних необхідно вказати ключовий атрибут.

Д. колективний (груповий) /д. коллективный (групповой)/ [shared a.] — спільне використання си-

стеми обчислювальної двома або більше користувачами в пакетному чи інтерактивному режимах.

Д. локальний /д. локальный/ [local a.] — доступ за допомогою локального пристрою вводу-виводу ЕОМ.

Д. множинний /д. множественный/ [multiple a.] — в мережах передавання даних доступ багатьох станцій до широкомовного каналу, що дозволяє усунути змагання шляхом виявлення конфлікту і виконання повторного передавання.

Д. монопольний /д. монопольный/ [exclusive a.] — доступ програми (запиту) до даних в режимі, при якому всі інші програми (запити) в цей момент не мають доступу до цих же даних і знаходяться в режимі очікування.

Д. несанкціонований (неавторизований) /д. несанкционированный (неавторизованный)/ [unauthorized (illegal) a.] — навмисне звернення користувача до даних, доступ до яких йому не дозволений, з метою їхнього читання, оновлення або руйнування.

Д. несанкціонований до апаратури /д. несанкционированный к аппаратуре/ [unauthorized (illegal) a. to hardware] — дії порушника, спрямовані на здійснення доступу до внутрішнього монтажу, ліній зв'язку, технологічних органів управління з метою: зміни та руйнування принципової схеми обчислювальної системи і апаратури; приєднання стороннього пристрою; зміни алгоритму роботи обчислювальної системи шляхом використання технологічних пультів і органів управління; завантаження сторонніх програм і внесення комп'ютерних вірусів у систему; використання терміналів системи і т. ін.

Д. несанкціонований до інформації /д. несанкционированный к информации/ [unauthorized a. to information] — доступ до інформації під час якого порушуються встановлені правові норми і порядок його здійснення (правила розмежування доступу). У системі комп'ютерній доступ несанкціонований (НСД) може здійснюватися як з використанням штатних засобів (сукупністю програмно-апаратного забезпечення, включеного до складу системи розробником під час розроблення або адміністратором системи в процесі експлуатації), що входять в затверджену конфігурацію комп'ютерної системи, так і з використанням

програмно-апаратних засобів, включених до її складу зловмисником. До основних способів НСД відносяться: безпосереднє звертання до об'єктів комп'ютерної системи з метою одержання певного виду доступу; створення програмно-апаратних засобів, що виконують звернення до об'єктів в обхід засобів захисту; модифікація засобів захисту, що дозволяє здійснити НСД; впровадження в комп'ютерну систему програмних або апаратних механізмів, що порушують структуру й функції системи і дозволяють здійснити НСД.

Д. санкціонований до інформації /д. санкционированный к информации/ [authorized a. to information] — доступ до інформації, під час якого не порушуються встановлені правові норми і порядок його здійснення (правила розмежування доступу).

Д. шахрайський /д. мошеннический/ [a. fraud] — несанкціоноване використання послуг стільникового зв'язку шляхом навмисного або ненавмисного втручання, маніпулювання або перепрограмування серійних або ідентифікаційних номерів стільникових апаратів.

ДОСТУПНІСТЬ /доступность/ [availability] — 1) Можливість проникнення куди-небудь. 2) Властивість ресурсу системи (комп'ютерної системи, послуги, об'єкта комп'ютерної системи, інформації), яка полягає в тому, що користувач і (або) процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, і в той час, коли він йому необхідний.

Д. даних /д. данных/ [data a.] — властивість даних, що полягає у можливості їхнього читання користувачем або програмою. Визначається рядом факторів: можливістю працювати за терміналом, володінням паролем, знанням мови запитів і т. ін.

Д. ресурсу /д. ресурса / [resources a.] — властивість ресурсу, що полягає у можливості його використання за вимогою користувача, який має відповідні повноваження.

ДОСЬЄ /досье/ [dossier] (франц. dosser) — сукупність документів, матеріалів, що стосуються певного питання, справи, особи, а також папка, в якій містяться ці матеріали.

ДУБЛЮВАННЯ /дублирование/ [doubling] (франц. doubler — подвоювати) — виготовлення будь-чого у двох екземплярах, повторювання; паралельне з будь-ким виконання схожої, однакової роботи.

Е

ЕКВІВАЛЕНТ /эквивалент/ [equivalent] (від лат. aequivalens (aequivalentis) — рівноцінний) — рівноцінне, рівносильне, рівнозначне; предмет або кількість, що відповідає іншим предметам або кількостям, може їх замінювати або виражати.

Е. антени /э. антенны/ [antenna e.] — електричне коло або пристрій, що імітує антену. Складається з резисторів, котушок індуктивності і конденсаторів так, що його імпеданс дорівнює імпедансові антени (в діапазонах від кілометрових до декаметрових хвиль) або являє собою відрізок коаксіальної лінії з навантаженням у вигляді поглинача енергії електромагнітних хвиль (в діапазоні дециметрових хвиль). Застосовується при настроюванні і випробування радіоприймачів і радіопередавачів без приєднання реальних антен.

ЕКОЛОГІЯ /экология/ [ecology] (від грец. *οἶκος* — оселя, середовище і ...логія, що від грец. *λόγος* — слово, вчення) — наука про зв'язок організмів із середовищем.

Е. культурна /э. культурная/ [cultural e.] — концепція комунікативістики, спрямована збереження й розвиток культурно-просвітницької функції засобів масової інформації шляхом звільнення їх від пресингу зі сторони інформаційно-розважальних монополій, що відносяться до інформації як до товарної маси. Завданням е. к. проголошується захист ідей справді гуманної комунікабельності ЗМІ, що відкриває шлях до міцного миру й взаєморозуміння між людьми та їхніми об'єднаннями, між країнами та регіонами.

Е. соціальна /э. социальная/ [social e.] — в комунікативістиці — напрям дослідження соціально-культурних аспектів інформаційної діяльності і комунікаційного простору з урахуванням можливих змін, що порушують збалансовану комунікабельність гуманістичних духовних цінностей, суспільних структур і систем. Е. с. займає критичну позицію по відношенню до тотальної комерціалізації ЗМІ і підпорядкуван-

ню їх принципам конс'юмеризму. На основі такої позиції розвивається концепція комунікації як екології культурної.

ЕКОНОМІКА /экономика/ [economy] (грец. *øìκøνøμική*, від *øìκøς* — житло і *νόμøς* — закон) — 1) Сукупність суспільно-виробничих відносин. 2) Господарське життя, стан господарства. 2) Наука, що вивчає фінансово-матеріальну сторону будь-якої галузі матеріальної діяльності.

Е. інформатизації /э. информатизации/ [informatization e.] — стан і правові механізми забезпечення виробництва, розподілу, обліку, споживання ресурсів інформаційних і ресурсів інформатизації.

Е. інформаційна /э. информационная/ — термін, що характеризує сучасну тенденцію розвитку світової економіки, зв'язану із збільшенням ролі індустрії інформаційної, знань в економічному житті суспільства. Див. також економіка постіндустріальна. Проблемними питаннями і. е. можуть бути: формування економічних показників для суспільства інформаційного; вивчення темпів створення і ліквідації робочих місць в інформаційному суспільстві; методи пониження соціальної напруги; вихід на домінуючі позиції високоінтелектуальних робіт тощо. Результатом функціонування і. е. є продукція інформаційна і послуги інформаційні, а рівень їхнього споживання є мірилом її розвиненості. Комплексні послуги з надання інформації й розваг в режимі прямого доступу є бізнесом, що швидко зростає. Див. також ринок інформаційний.

Е. постіндустріальна /э. постиндустриальная/ — економіка, в якій промисловість за показниками зайнятості і своєї долі в національному продукті поступається місцем сфері послуг, а сферою послуг переважно є оброблення інформації. В суспільстві з п. е. найбільше потенційне джерело багатства — національніресурси інформаційні, що викликає необхідність розвивати нову галузь економіки — економіку інформаційну.

ЕКРАН /экран/ [screen, shield] (франц. *écran*, буквально заслон, ширма) — пристрій з поверхнею, що відбиває, знищує або перетворює випромінювання різних видів енергії з метою захисту чи використання.

Е. міжмережні /э. межсетевые/ [firewall] — засоби, що дозволяють ізолювати внутрішню мережу і комп'ютери від Інтернету і обмежити доступ користувачів Інтернету до внутрішньої інформації і систем.

Усі е. м. поділяють на три категорії: фільтри пакетні (фільтри без пам'яті); фільтри канальні; фільтри прикладного рівня.

ЕКРАНУВАННЯ /экранирование/ [screening, shielding] — дія, спрямована на реалізацію захисту кого-, що-небудь екраном від зовнішнього впливу, шкідливого діяння і т. ін.

Е. електричного поля /э. электрического поля/ — локалізація поля електричного шляхом нейтралізації зарядів в металевому заземленому екрані, викликаних джерелами цього поля. Унаслідок екранування напруженість електричного поля за екраном зменшується. Для стікання зарядів з екрана необхідно забезпечити його заземлення з малим (менше 4 Ом) опором.

Е. електромагнітне /э. электромагнитное/ [electromagnetic s.] — об'єднання способів екранування високочастотних електричних і магнітних полів. Для виготовлення екранів застосовують наступні матеріали: сталь листова декапована товщиною 0,35–2 мм; сталь тонколистова оцинкована товщиною 0,51–1,5 мм; сітка сталева тканa з номерами 0,4–2,5; сітка сталева плетена з номерами 3–6; сітка з латунного проводу марки Л-80 з номерами 0,25–0,25; металізовані тканини. Матеріал екрана вибирають на основі оцінки необхідного коефіцієнта послаблення ПЕМВН екраном, для чого на місці, де передбачається встановлення екрана, вимірюється рівень поля.

Е. магнітного поля /э. магнитного поля/ [magnetic insulation] — локалізація і шунтування поля магнітного за допомогою спеціальних екранів. Для ефективного екранування низькочастотних полів застосовуються екрани, виготовлені з феромагнітних матеріалів (пермалою або сталі) з великою відносною магнітною проникністю. В такому екрані лінії магнітної індукції проходять його стінками, які мають малий магнітний опір порівняно з опором повітря поза екраном. В результаті цього магнітне поле шунтується екраном. Якість екранування залежить від магнітної проникності екрана і опору магнітопроводу, яке буде тим менше, чим товстіший екран і менше у ньому стиків і швів, розташованих поперек напряму ліній магнітної індукції. Екранування високочастотного магнітного поля ґрунтується на використанні явища магнітної індукції, що створює в екрані вихрові струми (струми Фуко). Магнітне поле цих струмів спрямоване назустріч збуджу-

ючому полю, в результаті чого збуджуюче магнітне поле витісняється екраном. Із-за поверхневого ефекту щільність вихрових струмів і напруженість змінного магнітного поля по мірі заглиблення в метал падає по експоненціальному закону. Ефективність е. м. п. залежить від частоти його коливань і від електричних властивостей матеріалу екрана. Для високих частот, починаючи з діапазону середніх хвиль, екран з будь-якого матеріалу товщиною 0,5–1,5 мм є достатньо ефективним. При е. м. п. заземлення екрана не змінює величини збуджуваних в екрані струмів і не впливає на його ефективність екранування.

Е. побічних полів /э. побочных полей/ — локалізація побічних полів, що породжуються при роботі радіоелектронних засобів, в межах зони контрольованої шляхом екранування джерел поля. Розрізняють наступні способи екранування: екранування електричного поля; екранування магнітного поля; екранування електромагнітне.

Е. приміщення /э. помещения/ — спосіб екранування електромагнітного, достатнього для проведення у приміщенні закритих заходів. Розміри екранованого приміщення вибирають виходячи з його призначення і вартості. Металеві листи або полотнища сітки повинні бути між собою міцно, з малим електричним опором, з'єднані по всьому периметру. Двері приміщень також повинні бути екрановані і при закриванні забезпечувати надійний електричний контакт із стінками приміщення (дверною рамою) по всьому периметру не рідше ніж через 10–15 см. Для цього може бути застосована гребінка з фосфористої бронзи, яку закріплюють по внутрішньому периметру дверної рами. Вікна (якщо вони є) затягуються одним або двома шарами мідної сітки з розмірами комірки 2х2 мм з відстанню між шарами сітки не менше 50 мм. Обидва шари повинні мати хороший контакт із стінками приміщення (рамою) по всьому периметру (по аналогії з дверима). Для покращення екрануючих властивостей неекранованих приміщень застосовуються додаткові засоби, в тому числі: струмопровідні лакофарбові покриття або струмопровідні шпалери; штори з металізованої тканини; металізоване скло, встановлене в металеві або металізовані рами; струмопровідні плівки, що наклеюються на вікна.

Е. проводів /э. проводов/ [conductor s.] — спосіб захисту інформації від витоку лініями зв'язку і кабе-

лями електроживлення, що виходять за межі контрольованої зони. Досягається розташуванням проводів в металевих оболонках. Необхідна умова е. п. — їхнє заземлення. Найкращий захист забезпечують екранований трифіляр (три скручені разом проводи, один з яких використовується як екран), триаксіальний кабель (ізольований коаксіальний кабель, розташований в електричному екрані), екранований плоский кабель у вигляді плоского багатопроводового кабелю, покритого з однієї або з обох сторін мідною фольгою.

ЕКСПЕРТ /эксперт/ [expert] — (від лат. expertus — досвідчений) — фахівець, який здійснює експертизу.

Е. з кваліфікації /э. по квалификации/ — фахівець, що займається аналізом кваліфікаційним.

ЕКСПЕРТИЗА /экспертиза/ [(expert) examination] (франц. expertise, від лат. expertus — досвідчений) — 1) Розгляд, дослідження експертом певних справ, питань, що потребують спеціальних знань. 2) Процес опитування експертів, збирання і первинний аналіз експертної інформації.

Е. психоекологічна /э. психоекологическая/ — встановлення відповідності неусвідомлюваного впливу інформаційного до стандартів інформаційно-психологічної безпеки і допустимості його застосування у визначених законом випадках.

ЕКСПОРТ /экспорт/ [export] (англ. export, від лат. exporto — виношу, виводжу) — 1) Вивіз товарів або капіталів за кордон; протилежне імпорт. 2) Загальна кількість або загальна вартість товарів, що вивозяться за кордон.

Е. інформації /э. информации/ [information e.] — виведення інформації з-під керування комплексу засобів захисту назовні.

ЕЛЕКТОРАТ /электорат/ [electorate] (англ. elect — обирати, від лат. eligo — обираю) — виборці, настрої й рішення яких на сучасному етапі системи демократичних виборів у більшості випадків залежать від знайомства з кандидатами через мас-медіа. Поведінка кандидатів під час телевізійних дебатів, їхня зовнішність, голос, манери, що проявляються у виступах на телебаченні або в інших ЗМІ, створюють іміджі, здатні відволікати увагу публіки від суті політичних програм, що висуваються.

ЕЛЕКТРО... /электро.../ [electro...] (від грец. $\tilde{\eta}\lambda\varepsilon\kappa\tau\rho\phi\nu$ — янтар) — у складних словах означає “електри-

чний".

ЕЛЕКТРОАКУСТИКА /электроакустика/ [electroacoustics] (від електро... і акустика) — розділ акустики, зміст якого складає теорія, методи розрахунку і конструювання перетворювачів електроакустичних.

ЕЛЕКТРОЗВ'ЯЗОК /электросвязь/ [electric(al) communication] (від електро... і зв'язок — будь-яке передавання сигналів електричних, що відображають знаки, текст, зображення, звуки або знання будь-якої природи за допомогою проводових, радіо, оптоелектронних та інших електромагнітних пристроїв (систем).

Е. документальний /э. документальная/ — вид електрозв'язку, за якого здійснюється передавання документальних повідомлень: літеро-цифрового тексту, цифрових даних і графічних зображень.

ЕЛЕКТРОННИЙ БІЗНЕС /электронный бизнес/ [e-business] — сукупність електронної комерції та комплексної автоматизації внутрішньої діяльності організації.

ЕЛЕКТРОННИЙ ГАМАНЕЦЬ /электронный кошелек/ [electronic purse] — електронний інтелектуальний пристрій, який зберігає в своїй пам'яті деяку суму грошових кошт, дозволяє здійснювати покупки в системі електронної комерції, при здійсненні операцій відразу зменшує сальдо на суму транзакції.

ЕЛЕКТРОННА КОМЕРЦІЯ /электронная коммерция/ [e-commerce] — різновид комерційної діяльності, в якої взаємодія між її учасниками на всіх або деяких етапах здійснюється в електронний спосіб, одна із двох складових електронного бізнесу.

ЕЛЕКТРОННИЙ УРЯД /электронное правительство/ [e-government] — назва концепції та моделі державного управління в суспільстві інформаційному. Під цим терміном також розуміють узагальнену назву програм розвитку автоматизації діяльності урядових структур країни від найпростішого - інформування громадян про діяльність уряду, до найскладнішого - автоматизації управління та контролю суспільства за діяльністю уряду.

ЕЛЕМЕНТ /элемент/ [element, item] — (від лат. elementum — первісна речовина) — складова частина будь-чого цілого.

Е. інформації /э. информации/ [information i.] — інформація на носії з достатньо чіткими межами, що

задовольняє наступним вимогам: належить конкретному джерелу (документу, людині, зразка продукції і т. ін.); міститься на окремому носії; має конкретну ціну.

ЕМЕРДЖЕНТНІСТЬ /эмерджентность/ [emergence] (англ. — раптова поява) 1) Особливість систем, яка полягає в тому, що властивості системи не зводяться до сукупності властивостей частин, з яких вона складається, та не виводяться з них; 2) Внутрішня цілісність систем.

ЕМОЦІЇ /эмоции/ [emotion] (франц. *èmotion* — хвилювання, від лат. emoteo — хвилюю, збуджую) — душевні переживання, почуття гніву, печалі, страху, радощів і т. ін.

ЕНДОСКОП /эндоскоп/ [endoscope] (від грец. *ἐνδον* — всередині і *σκοπέω* — спостерігаю, розглядаю) — прилад візуально-оптичний для спостереження через малі отвори діаметром 6–10 мм. Створюється на базі волоконно-оптичних світловодів. Типовий е. складається: з окулярної частини, через яку здійснюється спостереження, робочої частини у вигляді волоконно-оптичного кабелю довжиною 600–1500 мм, дистальної частини, що містить об'єктив, і освітлювального джгута для підсвічування об'єкта спостереження. Е. комплектуються мережними або акумуляторними освітлювачами з джерелами світла — галогенними лампами потужністю 20–150 Вт. В е. забезпечується можливість відхилення дистальної частини на 180° у вертикальній і горизонтальній площинах. Кут поля зору об'єктива складає 40–60°, фокусування об'єктива забезпечує спостереження як поблизу (від 1 мм і більше), так і "в нескінченності" (на відстані більше 5 м).

ЕНТРОПІЯ /энтропия/ [entropy] (від грец. *ἐν* — в і *τροπή* — поворот, зміна, перетворення) — 1) Міра хаосу, кількісна міра безладу в системі інформаційній. Надлишок зв'язків, потенційно здатних створювати хаос в прийнятті рішення. 2) В теорії інформації — усереднена міра невизначеності стану об'єкта або деякої ситуації (випадкової величини) з кінцевим числом виходів. Використовується для визначення кількості інформації в повідомленні. При рівній імовірності всіх повідомлень кількість інформації визначається як математичне сподівання невизначеності повідомлення за формулою $H = k \cdot \log_2 m$, де H — ентропія, k — число знаків в повідомленні, m — число знаків в алфавіті. 3) В математиці — міра невизначеності випадкової функції.

ЕОМ /ЭВМ/ [computer] — комплекс технічних засобів, призначений для автоматичного оброблення інформації в процесі вирішення задач обчислювальних і завдань інформаційних.

Е. персональна (ПЕОМ) /э. персональная (ПЭВМ/ [personal (one-on-one) c. (PC)] — ЕОМ, призначена для індивідуального використання.

Е. персональна професійна (ППЕОМ) /э. профессиональная персональная (ППЭВМ)/ [Personal Professiooriented C. (PPC)] — універсальна мікрокомп'ютерна система, призначена для використання в автономному режимі, локальних обчислювальних мережах і системах телеоброблення даних для вирішення завдань різноманітної професійної орієнтації; ЕОМ, що використовується як робоче місце фахівця і призначена для вирішення його професійних завдань.

ЕТАП /этап/ [halting place, stage] (від франц. etape — перегін, перехід) — 1) Частина шляху — дистанція. 2) Відрізок часу, відзначений певними подіями.

Е. вивчення об'єктів психологічної війни /э. изучения объектов психологической войны/ — послідовність основних заходів вивчення об'єктів психологічної війни: здійснення збирання, оброблення і накопичення вихідної інформації про країну, її збройні сили, соціально-політичне життя, національно-психологічні особливості населення, культуру, побут, вдачу, звичаї, традиції і т. ін.; здійснення загальної оцінки й прогнозування соціально-психологічної обстановки в країні, морально-психологічного стану військовослужбовців і цивільного населення як в цілому, так і по конкретних регіонах; визначення пріоритетних об'єктів психологічного впливу, тобто найбільш уразливих або схильних до сприйняття інформації, що розповсюджується органами психологічної війни. На цьому ж етапі визначають також оптимальні шляхи й способи психологічного впливу на них; підготовка інформаційно-довідкових і пропагандистських матеріалів для здійснення психологічних операцій і заходів проти виділених об'єктів; уточнення вихідних відомостей, звірення матеріалів оцінок і прогнозів з реальним розвитком подій, виявлення конкретних результатів психологічного впливу на противника.

Е. підготовки й проведення психологічних операцій і заходів психологічної війни /э. подго-

товки и осуществления психологических операций и мероприятий психологической войны/ — послідовність основних заходів підготовки й ведення війни психологічної: планування; формулювання мети операцій (заходів); визначення й вивчення об'єктів впливу; вибір конкретних видів, форм, методів, способів і прийомів здійснення психологічних впливів; розроблення змісту (технології застосування основних складових) психологічних впливів; визначення комунікативних контурів і умов здійснення психологічних впливів, а при необхідності й створення їх; контроль за ефективністю проведення конкретних психологічних операцій і заходів.

Е. підготовки програм усного мовлення /э. подготовки программ устного вещания/ — послідовність основних заходів підготовки й виготовлення програм усного мовлення: вироблення загальної концепції (замислу) передачі, визначення мети, теми й основної ідеї, вибір виду передачі й способу його підготовки; здійснення розрахунку часу всіх робіт (загальна тривалість передачі, розподіл часу на музику, текст, сигнали і шуми), підбір диктора, розроблення варіантів тактики застосування звукомовної станції з конкретною програмою; підготовка власне програми (написання тексту, підбір музики, шумів, сигналів, затвердження програми у керівництва, узгодження дій диктора та інших учасників передачі, запис її на магнітну плівку і, якщо потрібно, розмноження); аналіз ефективності програми після проведення сеансу й виявлення змін і доповнень, які потрібно в неї внести.

Е. системного аналізу /э. системного анализа/ — послідовність основних складових аналізу системного: постановка задачі системного аналізу (визначення границь системи, цілей її функціонування і основних показників оцінки); проведення структуризації системи, виявлення складових елементів (основних об'єктів і процесів), які визначають досягнення цілей, що стоять перед системою, з врахуванням умов впливу зовнішнього середовища у вигляді характеристик, що відображають його вплив на елементи системи; складання математичної моделі системи, тобто визначення параметрів системи, допустимих інтервалів зміни і залежностей між параметрами (математичний опис системи) та формування і розрахунок цільової функції; удосконалення (коригування) складу, структури, організації процесів оброблення, керування в системі за

результатами математичного моделювання і розрахунків за цільовою функцією стосовно до умов оптимального функціонування, а також оптимальне планування функціонування системи і керуючих впливів до неї, у відповідності до параметрів, виведених у цільовій функції.

ЕТИМОЛОГІЯ /этимология/ [etymology] (від грец. *ἐτυμολογία*, від *ἔτυμον* — істина і *λόγος* — слово, вчення) — 1) Розділ мовознавства, що вивчає походження слів. 2) Пояснення походження якогось слова зіставленням його з спорідненими словами тієї або іншої мови.

ЕТНОС /этнос/ [ethnic group] (від грец. *ἔθνος* — народ)— спільність людей (плем'я, народність, нація), що склалася в ході соціально-історичного розвитку.

ЕФЕКТ /эффект/ (лат. effectus — виконання, дія, від efficio — дію, виконую) — 1) Результат, наслідок яких-небудь причин, заходів, дій. 2) Сильне враження, спричинене ким-небудь або чим-небудь. 3) Засіб, що має на меті справити сильне враження, викликати здивування.

Е. міжгрупової дискримінації /э. межгрупповой дискриминации/ (лат. discriminatio від discrimino — розрізняю, розділяю) — встановлення відмінностей між власною і іншою групою (див. група соціальна). В певних умовах міжгрупові відмінності можуть штучно підкреслюватися або перебільшуватися. Міжгрупова дискримінація — явище не тільки психологічне, в основі якого лежать пізнавальні механізми встановлення тотожності й відмінності, але також і соціальне. Результати міжгрупової дискримінації проявляються у вигляді двох тенденцій: встановлення відмінностей, що оцінюються позитивно, на користь власної групи; встановлення відмінностей, що оцінюються позитивно, на користь іншої групи. В першому випадку спостерігається пріоритет свого групового членства над співпаданням поглядів з представниками чужої групи, тобто, індивід в ситуації вибору швидше віддасть перевагу навіть таким членам "своєї" групи, з якими він не згідний, ніж тим членам "чужої" групи, з якими його об'єднує подібність точок зору. Друга тенденція веде до послаблення внутрішньогрупових зв'язків, девальвації внутрішньогрупових цінностей і дезінтеграції групи як такої. Як правило, на це й орієнтовані впливи психологічні.

Е. новизни /э. новизны/ — психологічний ефект, що виникає при сприйнятті людьми один одного.

Полягає в тому, що по відношенню до знайомої людини найбільше значення має остання, тобто більш нова інформація про неї, а по відношенню до незнайомої людини більше значення має перша інформація.

Е. ореолу /э. ореола/ (франц. auréole — сяяння, від лат. aureolus — золотий) — психологічний ефект, що полягає в розповсюдженні первинної загальної оцінки людини (людей) на сприйняття її (їх) вчинків і особистих якостей. Так, якщо перше враження про людину (людей) в цілому прихильне, то в подальшому вся її (їхня) поведінка, риси і поступки починають переоцінювати в позитивну сторону. В них виділяють і перебільшують тільки позитивні моменти, а негативні як би недооцінюють або взагалі не помічають. Якщо ж загальне перше враження про будь-яку людину (людях) виявилося негативним, то навіть позитивні її (їхні) якості й поступки в подальшому не помічають, або недооцінюють на фоні гіпертрофованої уваги до недоліків.

Е. первинності /э. первичности/ — психологічний ефект, суть якого в тому, що ймовірність пригадування декількох перших елементів однорідного матеріалу більш висока, ніж середніх (при цьому, чим більший обсяг пред'явленого матеріалу і чим вищий темп його подавання, тим менша кількість перших елементів запам'ятовується).

Е. стереотипності /э. стереотипности/ — психологічний ефект, що виражається у спрощеному й схематичному, але стійкому уявленні про будь-що (або будь-кого). Стереотипи стихійно формуються в умовах дефіциту інформації, або нездатності індивіда інтерпретувати її адекватно. Стереотип ніколи не буває істинним, він завжди містить тенденційні, наперед задані характеристики явища, тому завжди неадекватний йому. Стереотип узагальнює явища за принципом зовнішньої подібності або випадкового збігу, проте не аналізує його глибинну сутність.

ЕФЕКТИВНІСТЬ /эффективность/ [efficiency] (від лат. effectus — виконання, дія) — 1) Результат, наслідок будь яких причин, сил, дій. 2) Ступінь співвідношення результатів з затратами; система показників, що характеризують рівень використання потужностей різноманітних систем. Розрізняють е. технічну і економічну. В обчислювальній техніці технічна ефективність — це швидкість обробки одиниці інформації, питомі

затрати на обробку одиниці інформації.

Е. добування інформації /э. добывания информации/ — ступінь виконання завдань, поставлених перед органом добування інформації. Для об'єктивного визначення ефективності використовується група загальносистемних показників кількості і якості інформації: повнота інформації, що добувається; своєчасність добування інформації; достовірність інформації; точність вимірювання розвідувальних ознак; сумарні витрати на добування інформації.

Е. економічна /э. экономическая/ — показник економії праці в результаті застосування певних заходів; ступінь віддачі виробництва, машин, апаратів.

Е. економічної розвідки /э. экономической разведки/ — відношення прибутків від діяльності розвідувальної до витрат на її проведення.

Е. захисту інформації /э. защиты информации/ [data protection e.] — здатність системи захисту інформації забезпечити достатній рівень її безпеки.

Е. інформаційної боротьби /э. информационной борьбы/ — ступінь реалізації мети інформаційної боротьби. Стосовно до боротьби збройної можна виділити два рівні е. і. б. — е. і. б. у війнах і збройних конфліктах в цілому та е. і. б. в операціях (бойових діях) та розділити (на кожному рівні) на дві частини: загальну е. і. б., яка призначена для оцінки власне інформаційної боротьби (як самостійного виду боротьби) і спеціальну е. і. б., призначену для оцінки дій, в інтересах яких ведеться інформаційна боротьба.

Е. психологічного впливу /э. психологического влияния/ — ступінь реалізації мети психологічної війни. Залежить від цілого ряду факторів, які поділяються на передумови сприйняття психологічного впливу і передумови засвоєння змісту психологічного впливу.

Ж

ЖИВУЧІСТЬ /живучесть/ [liveness; viability] — термін, що означає життєздатність, витривалість, стій-

кість, тривале збереження.

Ж. програмного виробу /ж. программного изделия/ [program v.] — показник якості програмного виробу, що характеризує його здатність зберігати нормальне функціонування при машинних збоях або частковому виходу обладнання з ладу.

Ж. системи /ж. системы/ [system v.] — здатність системи до збереження своїх основних функцій, навіть при пониженій ефективності системи, при дії факторів катастрофічного характеру — на відміну від надійності як здатності системи виконувати свої функції в нормальних, наперед заданих умовах.

ЖОВТОГАРЯЧА КНИГА /оранжевая книга/ [orange book] — див. критерії безпеки комп'ютерних систем.

ЖУРНАЛ /журнал/ [journal, log] (франц. journal, від jour — день) — 1) Періодичне видання, один із засобів масової інформації і пропаганди, що впливає на громадську думку, формуючи її відповідно до інтересів певних суспільних угруповань і політичних партій. Може використовуватися як засіб впливу психологічного друкованими засобами. 2) В обчислювальній техніці — набір даних (файл), що використовується операційною або іншою системою для збирання і обліку статистичної інформації, різних повідомлень та інших даних.

Ж. відновлення /ж. восстановления/ [recovery l.] — журнал, що забезпечує можливість відновлення бази даних або файла. Містить інформацію про всі зміни в базі даних (файлі) з того моменту, коли було встановлено, що дані достовірні і була зроблена остання копія резервна. В загальному випадку ж. в. може бути використаний одним із двох способів: відтворенням усіх змін, зроблених з моменту одержання останньої резервної копії (якщо база даних або файл зруйновані); знищенням усіх неправильних змін (якщо джерело помилок — в самих цих змінах).

Ж. змін /ж. изменений/ [after-look j.] — журнал, в який заносяться нові значення змінених записів. Використання цього журналу дозволяє повторити зміни.

Ж. контрольний /ж. контрольный/ [audit j., event j.] — журнал, в якому реєструються події, що

мають відношення до забезпечення безпеки обчислювальної системи, зокрема, звернення до захищених даних. Перегляд цього журналу дозволяє виявити спроби доступу несанкціонованого і ідентифікувати осіб, які роблять такі спроби.

Ж. помилок /ж. ошибок/ [error l.] — файл, в який система записує інформацію про збої.

Ж. реєстрації /ж. регистрации событий/ — упорядкована сукупність реєстраційних записів, кожний з яких заноситься комплексом засобів захисту за фактом здійснення контрольованої події. Див. також журнал контрольний.

Ж. реєстрації подій /ж. регистрации событий/ — те ж, що журнал контрольний.

Ж. системний /ж. системный/ [system j.] — набір даних, в який операційна система записує інформацію, що характеризує хід обчислювального процесу (виконання завдань, опис подій, заміну носіїв, повідомлення операторові і т. ін.).

ЖУРНАЛІЗАЦІЯ /журнализация/ [journalizing] — процес записування до журналу системного інформації про повідомлення, запити, виконувані програми, використані набори даних і т. ін.

З

ЗАБЕЗПЕЧЕННЯ /обеспечение/ [support] — сукупність методів, засобів і заходів, необхідних для нормального функціонування того чи іншого об'єкта, процесу і т. ін.

З. автоматизованих систем організаційне /о. автоматизированных систем организационное/ [organization support] — сукупність заходів, які регламентують функціонування і використання ЕОМ та систем автоматизованих.

З. апаратне (технічне) /о. аппаратное (техническое)/ [hardware] — комплекс технічних засобів, що включає ЕОМ, зовнішні пристрої, термінали і абонентські пункти, засоби зв'язку, необхідні для функціонування цієї чи іншої системи.

З. безпеки інформації /о. безопасности информации/ [provide information security] — запобігання або

виключення доступу несанкціонованого до інформації або ненавмисного, але недозволеного руйнування інформації. Див. також захист.

З. безпеки інформації в локальній обчислювальній мережі програмне спеціальне /о. безопасности информации в локальной вычислительной сети программное специальное/ [local area network security software] — забезпечення програмне засобів контролю і керування захистом інформації в локальній обчислювальній мережі (ЛОМ). Може включати наступні програми: уведення списків ідентифікаторів користувачів мережі; генерації і введення кодів ключів-паролів; уведення і контролю повноважень користувачів; реєстрації і відображення повідомлень про факти НСД (незбіг кодів-паролів, порушень повноважень із позначкою часу, місця і дати події); реєстрації звернень до інформації, що зберігається у файл-сервері і робочих станціях із позначкою автора звернення, часу і дати видачі інформації; ведення журналу обліку і реєстрації доступу до інформації; формування і видачі необхідних довідок про НСД; контролю цілісності програмного забезпечення ЛОМ; контролю конфігурації ЛОМ; керування шифруванням інформації; періодичного тестування і контролю функціонування функцій захисту; документування функцій захисту; ведення статистики НСД.

З. безпеки інформації в мережі обміну інформацією /о. безопасности информации в сети обмена информацией/ — один з основних аспектів забезпечення переваги над противником в інформаційній війні, що полягає в забезпеченні безпеки інформації при доступі та забезпеченні безпеки інформації при передаванні.

З. безпеки інформаційних систем організаційне /о. безопасности информационных систем организационное/ [organization support for information system secure] — регламентація виробничої діяльності і взаємовідносин виконавців на нормативно-правовій основі таким чином, що розголошення, витік, несанкціонований доступ до конфіденційної інформації стає неможливим або істотно утруднюється за рахунок проведення організаційних заходів.

З. безпеки інформаційних систем правове /о. безопасности информационных систем правовое/

[data protection legislation] — сукупність законодавчих актів, нормативно-правових документів, положень, інструкцій, настанов, вимоги яких є обов'язковими в межах сфери їхньої дії в системі захисту інформації.

З. безпеки інформації при доступі /о. безопасности информации при доступе/ — складова частина забезпечення безпеки інформації в мережі обміну інформацією, що полягає в запобіганні доступу несанкціонованого на територію, у приміщення і до носіїв даних та запобіганні несанкціонованого доступу до компонентів мережі обміну інформацією.

З. безпеки інформації при передаванні /о. безопасности информации при передаче/ — складова частина забезпечення безпеки інформації в мережі обміну інформацією, що полягає в запобіганні активному та пасивному перехопленню інформації.

З. електронне /о. электронное/ [electronic s.] — елемент війни електронної, який передбачає проведення заходів пошуку, перехоплення випромінювання в електромагнітному спектрі та визначення місцеположення джерел випромінювання для оцінки ступеня можливої загрози і прийняття рішення командирами усіх рангів, а також виконання додаткових функцій, таких як ухилення від загрози з боку противника і високоточний цілевказ системам озброєння.

З. інформаційне /о. информационное/ [information s.] — сукупність єдиної системи класифікації і кодування інформації, систем уніфікованих документації і масивів інформаці, які використовуються в системі автоматизованій. Розрізняють інформаційне забезпечення зовнішнє і внутрішнє.

З. інформаційне внутрішнє /о. информационное внутреннее/ [internal information s.] — вид забезпечення інформаційного, який являє собою методи і засоби перетворення зовнішнього подання даних в машинне, організації машинних масивів інформації, перетворення даних із машинних у зовнішні.

З. інформаційне зовнішнє /о. информационное внешнее/ [external information s.] — вид інформаційного забезпечення, який являє собою сукупність єдиної системи класифікації і кодування інформації та уніфікованої системи документації. Це методи і засоби ідентифікації об'єктів, подання їх у вхідних доку-

ментах.

З. інформаційне сил та засобів в умовах інформаційної боротьби /о. информационное сил и средств в условиях информационной борьбы/ — комплекс заходів добування інформації про противника в умовах протиборства, збирання інформації про свої сили і засоби, оброблення інформації і обмін нею між органами керування з метою організації і ведення бойових дій. Результативність інформаційного забезпечення залежить від багатьох факторів і умов, які кінець-кінців здійснюють вплив на два основних елементи: інформування органу керування і сприйняття одержаної ним інформації.

З. інформаційного відокремлення /о. информационного отделения/ — сукупність заходів інформаційно-розрахункового забезпечення функціонування системи інформаційної та забезпечення необхідної якості інформації, що циркулює в системі, на основі застосування технологій інформаційних спеціальних.

З. інформаційного захисту /о. информационной защиты/ [provide information security] — сукупність заходів, спрямованих на маскування і прикривання реальних систем інформаційних.

З. інформаційного збирання /о. информационного сбора/ — сукупність заходів забезпечення інформаційного суперництва, спрямованих на добування достовірної інформації про супротивну систему інформаційну: розвідка; контррозвідка; верифікація інформації з різних джерел; тестування системи управління конфронтуючою системою.

З. інформаційного маскування /о. информационного маскирования/ — сукупність заходів, спрямованих на приховування фактів обміну інформацією в системах інформаційних або її змісту: захисні семантичні перетворення інформації (необоротні — на основі спеціальної апаратури і оборотні — кодування і шифрування); організація замаскованого інформаційного обміну в інформаційно-розподільних мережах систем управління; застосування широкосмугових інформаційних сигналів і т. ін.

З. інформаційного прикривання /о. информационного прикрытия/ — сукупність заходів, спрямованих на захист діями свої сил та засобів: захист радіоелектронний; блокування цінної інформації; обмеже-

ння допуску до засобів і інформаційно-програмних ресурсів систем; контроль потенційних загроз і каналів витоку інформації; організація технологічних процесів захищеного (достовірного і конфіденційного) перероблення інформації в інформаційних системах; контроль і керування доступом до ресурсів систем.

З. інформаційного співробітництва /о. информационного сотрудничества/ — сукупність заходів інформаційного обміну і інформаційної інтеграції, спрямованих на реалізацію відносин інформаційних співробітництва на основі створення і застосування загальних технологій інформаційних (ЗІТ): телекс, телетекст, пошта електронна, відеотекс, телеконференції і т. ін. та єдиного середовища інформаційного (ЄІС) — Internet і т. ін.

З. інформаційного суперництва /о. информационного соперничества/ — сукупність заходів, спрямованих на реалізацію відносин інформаційних суперництва в реальних системах інформаційних на основі забезпечення інформаційного збирання і інформаційної протидії.

З. інформаційної безпеки /о. информационной безопасности/ [information security s.] — сукупність заходів, призначених для досягнення стану захищеності потреб особистостей, суспільства і держави в інформації. Держава здійснює свої заходи через відповідні органи, а громадяни, суспільні організації і об'єднання, що мають відповідні повноваження, у відповідності із законодавством. В основу з. і. б. держави повинні бути покладені наступні принципи: законність, дотримання балансу інтересів особистості, суспільства і держави; взаємна відповідальність суб'єктів забезпечення інформаційної безпеки; інтеграція систем національної і міжнародної безпеки. Специфічними принципами з. і. б. є: превентивний характер проведення її заходів по відношенню до заходів інших видів безпеки; інформованість адекватна об'єктів безпеки, в тому числі і міжнародних. В залежності від виду загроз інформаційних, що є наслідком навмисних або ненавмисних дій суб'єктів інформаційного процесу, з. і. б. здійснюється відповідно у формах патронату інформаційного і кооперації інформаційної або у формі боротьби інформаційної.

З. інформаційної безпеки інформаційне /о. информационной безопасности информационное/ [information s. information security] — сукупність заходів, що включають збирання (добування) відомостей

про фактори дестабілізуючі та загрози інформаційні, їхнє оброблення, обмін інформацією між органами керування і силами та засобами системи інформаційної безпеки. Його основу складає збирання (добування) необхідних відомостей, здійснюване в процесі розвідувальної, контррозвідувальної, оперативно-розшукової і оперативно-інформаційної діяльності.

З. інформаційної протидії /о. информационного противодействия/ — сукупність заходів забезпечення інформаційного суперництва, спрямованих на протидію конфронтуючій системі інформаційній: придушення радіоелектронне, інфільтрація дезінформації, в тому числі інформація для впливу на психіку персоналу конфронтуючої сторони (інформація психологічної боротьби) і інформація для здійснення дезорганізації функціонування системи управління противника; інфільтрація вірусів комп'ютерних в систему управління противника; блокування інформаційних процесів в системі управління противника; руйнування інформаційно-програмного забезпечення систем керування автоматизованих противника.

З. кадрове /о. кадровое/ [personal, cadre] — штати і персонал центру обчислювального, адміністрація системи автоматизованої, які виконують передмашинне оброблення інформації, зберігання носіїв, програмування і взаємодію з користувачами, а також інженерно-технічні працівники, які здійснюють експлуатацію і ремонт обчислювальної техніки та засобів захисту інформації.

З. лінгвістичне /о. лингвистическое/ [linguistic s.] — сукупність термінів і мов штучних, правил формалізації мови природної, що використовуються в техніці обчислювальній.

З. математичне /о. математическое/ [mathematical s.] — сукупність методів, правил, математичних моделей і алгоритмів вирішення задач.

З. математичне загальне /общее математическое о./ — забезпечення математичне функціонування програмного забезпечення загального.

З. математичне прикладне (спеціальне) /о. математическое прикладное (специальное)/ [application (special) mathematical software] — забезпечення математичне вирішення задач прикладних.

З. міжмережного обміну /о. межсетевого обмена/ [internetwork software, firmware and hardware] —

сукупність програмних і технічних засобів, в тому числі засобів захисту інформації, які використовуються для з'єднання двох або більше мереж передавання даних.

З. національної безпеки /о. национальной безопасности/ [enforcement (national) security] — проведення єдиної державної політики у сфері безпеки і системи заходів економічного, політичного або іншого характеру, адекватних загрозам життєво важливим інтересам особистості, суспільства і держави, спрямованих на виявлення і попередження загроз. Див. також безпека національна.

З. організаційне /о. организационное/ [organization s.] — сукупність заходів, які регламентують функціонування і використання ЕОМ та систем автоматизованих.

З. переваги над противником в інформаційній війні /о. превосходства над противником в информационной войне/ — сукупність оборонних дій інформаційних, що забезпечують ефективність боротьби інформаційної з противником в мережі обміну інформацією. Передбачає реалізацію усіх трьох аспектів таких дій: забезпечення безпеки інформації в мережі обміну інформацією; виявлення несанкціонованих дій в мережі обміну інформацією; протидія противникові в мережі обміну інформацією інформаційна.

З. програмне /о. программное/ [software] — сукупність програм системи оброблення даних і програмних документів, необхідних для експлуатації цих програм. Розрізняють забезпечення програмне загальне і прикладне.

З. програмне загальне /о. программное общее/ [general software] — сукупність керуючих і обробляючих програм, призначених для планування і організації обчислювального процесу, автоматизації програмування і налагодження програм розв'язування прикладних задач. В нього входить система операційна, система програмування, програми технічного обслуговування.

З. програмне криптографічне /о. программное криптографическое/ [encryption software, cryptographic protection software] — сукупність програм, призначених для реалізації захисту криптографічного інформації як програмним, так і апаратно-програмним способом.

З. програмне прикладне (спеціальне) /о. программное прикладное (специальное)/ [application

(special) software] — частина забезпечення програмного, що складається з окремих програм прикладних і пакетів прикладних програм, які забезпечують вирішення прикладних задач.

З. програмне системне /о. программное системное/ [system software] — забезпечення програмне, яке призначене для експлуатації і технічного обслуговування ЕОМ, для організації обчислювальних робіт і автоматизації розробки програм прикладних.

З. програмне стеганографічне /стеганографическое программное о./ [steganography software] — сукупність програм, які дозволяють приховувати інформацію на графічних, звукових та інших як би "чистих" носіях за допомогою методів стеганографії.

З. проектування системи захисту інформації методичне /о. проектирования системы защиты информации методическое/ [metodical support for security system design] — у відповідності до алгоритму проектування системи захисту інформації сукупність заходів і засобів забезпечення моделювання об'єкта захисту, виявлення і моделювання загроз безпеці інформації, розроблення заходів захисту інформації.

З. цілісності /о. целостности/ [data integrity provide] — процес, що забезпечує підтримку функціонування механізмів системи захисту інформації та об'єктів системи обчислювальної в такому стані, який визначений прийнятою стратегією захисту інформації.

ЗАВАДИ /помехи/ [interference, noise] — 1) Те, що порушує нормальну роботу будь-чого. 2) В техніці — різноманітна галузь явищ, що заважають нормальному функціонуванню різних технічних засобів і викликають відхилення параметрів їхньої роботи. Наприклад, у військовій техніці з. затрудняють виявлення, розпізнавання, визначення координат, селекцію і супроводження цілей, а також порушують зв'язок і т.ін. З. можуть створюватися: спеціальними технічними пристроями і організованими діями противника (завади навмисні); при одночасній роботі різних технічних засобів або від ненавмисних власних дій (завади ненавмисні); природними джерелами (завади природні). З. розрізняють: за фізичними полями, що несуть з. (електричні, магнітні, електромагнітні, акустичні, гравітаційні та вібраційні); джерелом виникнення (штучні і природні); середовищем розповсюдження (космічні, атмосферні, гідроакустичні, сейсмічні,

геофізичні); галуззю і способами використання, діапазонами частот та іншими ознаками.

З. активні /п. активные/ [active i.] — завади радіоелектронні, що виникають в результаті випромінювання хвиль електромагнітних технічними пристроями та системами (штучні з. а.) або джерелами електромагнітного випромінювання природного походження (природні з. а.). З. а. можуть бути навмисними (що створюються спеціальними передавачами) та ненавмисними (взаємні завади від роботи інших передавачів), завади індустріального походження (див. завади промислові), природне електромагнітне випромінювання (див. завади природні).

З. гідроакустичні /п. гидроакустические/ [hydroacoustic i.] — хвилі акустичні, що впливають на гідроакустичну антену і заважають прийманню повідомлень. До з. г. відносяться: шуми моря, корабля; шуми кавітації гвинтів двигуна; реверберація.

З. загороджувальні /п. заградительные/ [barrage] — завади радіоелектронні, ширина спектра частот яких значно перевищує ширину спектра корисного сигналу, що дозволяє придушувати сигнал без точної настройки на його частоту.

З. імітуючі /п. имитирующие/ [imitation i.] — активні завади радіоелектронні, які за своєю структурою є близькими до корисних сигналів і при передаванні можуть ввести в оману одержувача.

З. маскуючі /п. маскирующие/ [masking i.] — завади радіоелектронні, призначені для створення фону, на якому утрудняється або робиться неможливим виявлення і розпізнавання корисних сигналів.

З. навмисні /п. умышленные/ [intended i.] — завади, що створюються спеціальними технічними пристроями і організованими діями противника.

З. ненавмисні /п. неумышленные/ [unintentional i.] — завади, що виникають при одночасній роботі різних технічних засобів або будь-яких власних дій (див. також завади промислові).

З. пасивні /п. пассивные/ [passive i.] — завади радіоелектронні, що створюються за рахунок відбивання власного випромінювання радіолокаційних станцій від різних відбивачів (металізована паперова стрічка,

скловолокно, куткові відбивачі та інші засоби, а також земна і водна поверхня, гідрометеоутворення).

З. природні /п. естественные/ [natural n.] — завади, що викликаються наступними природними явищами: електричними грозовими розрядами, як правило, на частотах менше 30 МГц; переміщенням заряджених електрикою часток хмар, дощів, снігу і т. ін.; виникненням резонансних електричних коливань між землею і іоносферою; тепловим промінням Землі і будівель в діапазоні більше 30–40 МГц; електромагнітним промінням Сонця, Місяця, інших планет (на частотах більше 1 МГц); тепловими шумами в елементах і ланцюгах радіоприймачів. В містах до з. п. додаються ще завади промислові.

З. прицільні /п. прицельные/ [aimed i.] — завади радіоелектронні, що мають ширину спектра, сумірну (рівну або таку, що перевищує в 1,5–2 раза) з шириною спектра сигналу, і створює високий рівень спектральної густини потужності у смузі частот сигналу при невисокій середній потужності передавача завад.

З. промислові /п. промышленные/ [man-made i.] — завади, що виникають внаслідок діяльності промислових підприємств. За характером спектра випромінювання поділяються на флуктуаційні, гармонічні та імпульсні. Флуктуаційні завади мають розподілений за частотою спектр і створюються коронами високовольтних ліній передач, лампами денного світла, неоновою рекламою, електрозварюванням та іншими засобами з електричними розрядами. Спектр промислових гармонічних завад локалізований на частотах випромінювання, що виникає при нелінійних перетвореннях в промислових установках. Імпульсні завади, що виникають, насамперед, при замиканні і розмиканні електричних контактів вимикачів, характеризуються зосередженням енергії електромагнітного випромінювання в короткий проміжок часу.

З. радіоелектронні /п. радиоэлектронные/ [electronic i.] — вплив енергії випромінювання електромагнітного, який погіршує показники якості функціонування радіоелектронних засобів. Можуть бути ненавмисними і навмисними, активними і пасивними. Розрізняють також світлові і шумові з. р., радіозавади і т. ін.

З. радіолокаційні /п. радиолокационные/ [parasitic oscillation] — електромагнітні коливання, які ма-

скують, імітують чи спотворюють відбитий радіолокаційний сигнал. Найпростішою р. з. є гармонічне коливання на частоті РЛС, яке створюється генератором завад в місці знаходження об'єкта, що підлягає захисту. Така завада створює шумове засвічення екрана локатора. Більш складною за структурою є модульована р. з. з одним або декількома змінними параметрами. Вона буває безперервною і імпульсною та має спектр, близький до спектра випромінювання РЛС. За ефектом впливу р. з. класифікуються на маскуючі зображення об'єкта шляхом зашумлення екрана РЛС і імітуючі шляхом створення на екрані світлових плям. Змінюючи структуру і інтервал затримки імітаційної завади, можна змінювати форму, місце і характер руху фальшивого засвічення на екрані локатора.

З. штучні /п. искусственные/ [man-made n.] — радіозавади, створені різноманітними засобами генерування завад з метою порушення управління та зв'язку в ході боротьби радіоелектронної. За ефектом впливу на радіоелектронні засоби з. ш. поділяються на завади маскуючі та імітуючі. За співвідношенням спектрів завад і корисних сигналів з. ш. поділяються на завади загороджувальні і прицільні.

ЗАВАДОЗАХИЩЕНІСТЬ /помехозащищенность/ [interference immunity, noise immunity] — 1) В радіоелектроніці — здатність радіоелектронної апаратури зберігати на необхідному рівні показники якості роботи при впливі радіозавад заданого виду (видів) та рівня. З. забезпечується підвищенням потужності сигналів, що генеруються, використанням антен спрямованої дії (просторовою селекцією), застосуванням інших видів селекції, що базуються на використанні відмінностей між корисними сигналами та завадами (частотною, часовою, амплітудною, поляризаційною і т. ін.), вибором оптимальної структури сигналів та виду модуляції, кодуванням інформації, що передається, застосуванням статистичних методів приймання та оброблення сигналів і т.ін. Підвищення з. може бути досягнуто також шляхом підвищення обсягу сигналу, тобто за рахунок надмірності по тривалості і ширині спектра, або перевищення сигналу над завадою в місці приймання. Критеріями з. може бути величина, обернена до ймовірності спотворення інформації, або коефіцієнт придушення — відношення середньої потужності завади і сигналу на вході радіоприймача, при якому відбувається придушення радіоприймального пристрою. Розрізняють потенційну (тільки при наяв-

ності власного шуму радіоприймача) і реальну з. 2) В обчислювальній техніці — здатність ЕОМ зберігати якість функціонування під впливом зовнішніх завад та наявності додаткових засобів захисту від завад, що не відносяться до принципу її дії або побудови.

ЗАВАДОСТІЙКІСТЬ /помехоустойчивость/ [interference immunity, noise immunity, noise stability] — 1) В радіоелектроніці — здатність радіоелектронної апаратури зберігати якість функціонування на необхідному рівні під впливом радіозавад при відсутності засобів захисту від завад, що не відносяться до принципу її дії або побудови. 2) В обчислювальній техніці — здатність ЕОМ зберігати якість функціонування під впливом зовнішніх завад та відсутності додаткових засобів захисту від завад, що не відносяться до принципу її дії або побудови.

З. системи зв'язку /п. системы связи/ — здатність системи зв'язку розрізняти (відновлювати) сигнали із заданою достовірністю. Визначення завадостійкості всієї системи в цілому — завдання у більшості випадків дуже складне. Тому часто визначають завадостійкість окремих ланок системи: приймача при заданому способі передавання, системи кодування або системи модуляції при заданому способі прийому і т.ін. Розрізняють реальну і потенційну (за Котельниковим) або таку, яку можна гранично досягти. Їхнє порівняння для конкретного пристрою дозволяє оцінити його якість, наприклад, знання потенційної завадостійкості приймача при різноманітних способах передавання дозволяє вибрати з них найбільш досконалі.

ЗАВДАННЯ /задание/ [assignment, task, job, mission] — 1) Визначений, запланований для виконання обсяг роботи. 2) Одиниця роботи, яка визначається користувачем і виконується машиною обчислювальною; одиниця системи операційної, що являє собою послідовність управляючих операторів, які визначають виконувані програми і використовувані ними дані. 3) Доручення. 4) Мета, ціль.

З. вибору виду інтелектуальної протидії /з. выбора вида интеллектуального противодействия/ — завдання інтелектуальної протидії, яке полягає у попередньому виборі типу стратегії протидії на основі проведеної класифікації несанкціонованого доступу.

З. вибору зони інтелектуальної протидії /з. выбора зоны интеллектуального противодействия/

— завдання інтелектуальної протидії, що передбачає реалізацію перерозподілу навантаження на мережу інформаційно-обчислювальну (ІОМ), викликаного інформаційною війною, та оптимізацію розташування в ІОМ вузлів інтелектуальної протидії (центрів безпеки).

З. захисту /з. защиты/ — в "критеріях Загальних" декларуються наступні завдання: захист від загроз порушення конфіденційності (несанкціонованого одержання) інформації з усіх каналів її витоку, особливо за рахунок каналів ПЕМВН і прихованих каналів зв'язку; захист від загроз порушення цілісності (несанкціонованого змінювання інформації); захист від загроз порушення доступності інформації (несанкціонованого або випадкового обмеження інформації й ресурсів самої системи); захист від загроз аудита системи (наприклад, загрози несанкціонованих вторгнень в систему, маніпуляцій з протоколами обміну й аудита, із загальносистемним програмним забезпеченням).

З. здійснення інтелектуальної протидії /з. осуществления интеллектуального противодействия/ — завдання інтелектуальної протидії, що включає побудову програми інтелектуальної протидії, що здійснює імітацію функціонування об'єкта атаки (див. об'єкт атаки хибний) та власне реалізацію інтелектуальної протидії.

З. інтелектуальної протидії /з. интеллектуального противодействия/ — комплекс завдань інтелектуальної протидії в мережах обміну інформацією, вирішення яких спрямоване на досягнення мети інформаційної боротьби. Якщо інтелектуальна протидія, заснована на впровадженні об'єкта атаки хибного, то формулюються чотири основні з. і. п.: завдання класифікації несанкціонованого доступу; завдання вибору виду інформаційної протидії; завдання вибору зони інтелектуальної протидії; завдання здійснення інтелектуальної протидії за допомогою хибного об'єкта атаки.

З. інформаційне /з. информационная/ [information t.] — завдання, яке зв'язане із створенням, пошуком, вибіркою даних і внесенням в них змін.

З. класифікації несанкціонованого доступу /з. классификации несанкционированного доступа/ — завдання інтелектуальної протидії, виконання якого передбачає: класифікацію об'єкта несанкціонова-

ного доступу; класифікацію суб'єкта несанкціонованого доступу; класифікацію зброї інформаційної, що використовується.

З. розвідувальне /з. разведывательная/ — питання (проблема) — загальне або конкретне — з якого необхідно одержати відомості розвідувальні.

З. технічне (ТЗ) /з. техническое (ТЗ)/ [requirements specifications]— сукупність вимог до виробу, що визначаються його призначенням, галуззю застосування, умовами експлуатації, типом виробництва. ТЗ складають на основі документації нормативно-технічної, вимог замовника, а також за результатами вивчення ринку й аналізу кращих зразків конкурентної техніки (аналогів), наукового прогнозування. Відповідно до стандарту, ТЗ має такі розділи: назва і галузь застосування; джерело розробки; мета та призначення; технічні вимоги; економічні показники; етапи розроблення; порядок контролю і приймання; додатки.

ЗАВІРЕННЯ /заверение/ [notarization] — реєстрація даних у довіреної третьої особи (див. третя сторона) з метою забезпечення надалі впевненості в правильності таких характеристик як зміст, джерело даних, час відправлення чи одержання тощо.

ЗАГЛУШЕННЯ /подавление/ [suppression] — див. придушення.

ЗАГРОЗА /угроза/ [threat] — 1) Можлива небезпека. 2) Будь-які обставини або події, що виникають у зовнішньому середовищі, які можуть бути причиною порушення політики безпеки інформації і (або) нанесення збитків автоматизованій системі.

З. активна /у. активная/ [active t.] — загроза навмисна несанкціонованої зміни стану системи.

З. безпеці /у. безопасности/ [security t.] — сукупність умов і факторів, що створюють небезпеку інтересам життєво важливим особистості, суспільства і держави.

З. безпеці інформації /у. безопасности информации/ [security t.] — загрози викрадення, зміни або знищення інформації. Бувають випадковими або навмисними. В найбільш загальному випадку загрози проявляються наступними шляхами: унаслідок дій зловмисників; спостереження за джерелами інформації; підслухування конфіденційних розмов людей і сигналів акустичних працюючих механізмів; перехоплення

електричних, магнітних і електромагнітних полів, сигналів електричних і радіоактивного випромінювання; несанкціонованого розповсюдження матеріально-речовинних носіїв за межі контрольованої зони; розголошення інформації людьми, що володіють інформацією секретною або конфіденційною; утрати носіїв з інформацією (документів, носіїв машинних, зразків матеріалів і т. ін.); несанкціонованого розповсюдження інформації через поля і електричні сигнали, що випадково виникають в електричних і радіоелектронних приладах в результаті їхнього старіння, неякісного конструювання (виготовлення) та порушень правил експлуатації; впливу стихійних сил, насамперед, вогню під час пожежі і води в ході гасіння пожежі та витоку води в аварійних трубах водопостачання; збоїв в роботі апаратури збирання, оброблення, зберігання і передавання інформації, викликаних її несправністю, а також ненавмисних помилок користувачів або обслуговуючого персоналу; впливу потужних електромагнітних і електричних промислових і природних завад.

З. безпеці мережі обміну інформацією /у. безопасности сети обмена информацией/ — потенційно можлива подія, яка може вчинити небажаний вплив на мережу обміну інформацією (МОІ), а також на інформацію, що зберігається, обробляється й передається в ній. Виділяють три основних види загроз безпеці МОІ: загрози розкриття конфіденційної інформації; загрози цілісності інформації, що полягають у зловмисному змінюванні даних; загрози відмови в обслуговуванні, що полягають в блокуванні доступу до деякого ресурсу системи обчислювальної або МОІ.

З. безпеці обчислювальної системи /у. безопасности вычислительной системы/ —- впливи на систему обчислювальну, які прямо або побічно можуть нанести шкоду її безпеці. Розробники вимог безпеки і засобів захисту виділяють три види загроз: загрози порушення конфіденційності інформації, що обробляється; загрози порушення цілісності інформації, що обробляється; загрози порушення працездатності системи (відмови в обслуговуванні).

З. випадкова (ненавмисна) /у. случайная (неумышленная, непреднамеренная)/ [accidental, unintentional t.] — загроза, що спричинюється випадковими впливами на інформацію в процесі її введення, зберіга-

ння, оброблення, виведення і передавання. В результаті таких впливів на апаратному рівні відбуваються фізичні зміни сигналів в цифрових кодах, що несуть інформацію, а на програмному рівні може відбутися зміна алгоритму оброблення інформації на непередбачений, характер якої може бути різноманітним: у кращому випадку — зупинка обчислювального процесу, а в гіршому — його модифікація. Якщо засоби функціонального контролю змін не виявили, то наслідки модифікації алгоритму або даних можуть пройти непоміченими або привести до руйнування інформації, а при переплутуванні адреси пристрою — до витоку інформації. Причинами випадкових впливів при експлуатації інформаційних (обчислювальних) систем можуть бути: відмова і збої апаратури; завади на лініях зв'язку від впливів зовнішнього середовища; помилки людини як ланки системи; схемні і схемотехнічні помилки розробників; структурні, алгоритмічні і програмні помилки; аварійні ситуації та інші впливи.

З. для інформації /у. для информации/ [t. for information] — витік, порушення цілісності інформації або відмова в авторизованому доступі до неї.

З. інформаційна /у. информационная/ [information t.] — 1) Вплив з боку дестабілізуючих факторів на стан інформованості, що піддає небезпеці інтереси життєво важливі особистості, суспільства і держави. В результаті впливу і. з. знижується інформованість особистості, у неї з'являється спотворене уявлення про навколишні явища і процеси. Це у свою чергу відбивається на її поведінці, розвитку, освіченості, вихованні, психіці, здоров'ї, тобто порушує основи існування особистості. Вплив з. і. на інформаційне поле суспільної свідомості приводить до пониження загальної культури населення, розвитку бездуховності, розпусти, розповсюдженню антигуманних ідей, аморального способу життя і т. ін. В матеріальній сфері з. і. створюють підстави для шантажу, розкрадання, корупції, монополізму і т.ін. У внутріполітичному житті за їхньою допомогою нескладно інспірувати заворушення, страйки, міжнаціональну ворожнечу і т.ін. В різноманітних сферах державної діяльності вплив з. і. може проявлятися по-своєму. Проте очевидно, що неадекватне сприйняття дійсності особами, що приймають рішення на державному рівні, може призвести до найсерйозніших наслідків. 2) Вхідні дані, призначені для активізації в системі інформаційній алгоритмів,

відповідальних за порушення звичного режиму функціонування. З. і. можуть бути явними і прихованими.

З. інформаційній безпеці /у. информационной безопасности/ [information security t.] — сукупність умов і факторів, що створюють небезпеку інтересам життєво важливим особистості, суспільства і держави в інформаційній сфері. Основні з. і. б. можна розділити на три групи: загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу; загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання); загрози інформаційним правам і свободам особистості (праву на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації; праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на особисту таємницю; праву на захист честі і достоїнства і т. ін.).

З. інформаційно-психологічній безпеці /у. информационно-психологической безопасности/ — загрози, що викликають деструктивний вплив інформаційний на психіку людей. Основними з. і.-п. б. можуть бути: блокування на неусвідомлюваному рівні свободи волевиявлення людини, прищеплювання їй синдрому залежності; розроблення, створення і застосування спеціальних технічних і програмних засобів для деструктивного впливу на психіку людини; маніпуляція суспільною свідомістю з використанням спеціальних засобів впливу; деструктивний вплив на психіку людини зон геопатогенних і антропогенних; руйнування простору єдиного інформаційного і духовного держави, традиційних устоїв суспільства і суспільної моралі.

З. навмисна /у. умышленная/ [advertent t.] — загроза, пов'язана з діями людини (порушника, зловмисника, злочинця). При відсутності захисту порушник може скористатися як штатними (законними), так і іншими фізичними каналами, через які можна одержати доступ до апаратури, програмного забезпечення і здійснити викрадення, руйнування, модифікацію інформації і ознайомлення з нею. Для обчислювальних систем характерні наступні штатні канали доступу: термінали користувачів; термінал адміністратора системи; термінал оператора функціонального контролю; засоби відображення інформації; засоби документування інформації; засоби завантаження програмного забезпечення в обчислювальний комплекс; носії

інформації; зовнішні канали зв'язку, а також інші фізичні канали, такі як: технологічні пульти управління; внутрішній монтаж апаратури; лінії зв'язку між апаратними засобами даної обчислювальної системи; побічне електромагнітне випромінювання інформації з апаратури системи; побічні наведення інформації на допоміжних і сторонніх комунікаціях; відходи оброблення інформації у вигляді паперових і магнітних носіїв, викинутих на смітник.

З. порушення конфіденційності /у. нарушения конфиденциальности/ — загрози безпеці обчислювальної системи, спрямовані на розголошення інформації з обмеженим доступом.

З. порушення працездатності /у. нарушения работоспособности/ — загрози безпеці обчислювальної системи, спрямовані на створення ситуацій, коли в результаті навмисних дій понижується працездатність обчислювальної системи, або її ресурси стають недоступними (див. доступність).

З. порушення цілісності /у. нарушения целостности/ — загрози безпеці обчислювальної системи, що полягають у спотворенні або зміні неавторизованим користувачем інформації, що зберігається або передається. Цілісність інформації може бути порушена як зловмисником, так і в результаті об'єктивних впливів із сторони середовища експлуатації системи. Найбільш актуальна ця загроза для систем передавання інформації — комп'ютерних мереж і систем телекомунікацій.

З. потенційні безпеці інформації в локальній обчислювальній мережі /у. потенциальные безопасности информации в локальной вычислительной сети/ — загрози, пов'язані з наявністю навмисних і випадкових каналів несанкціонованого доступу до інформації в мережі обчислювальній локальні. Зі сторони "периметра" системи вони можуть бути наступними: доступ до ЛОМ із сторони штатної ПЕОМ (сервера) (див. З. потенційні безпеці інформації, що обробляється в ПЕОМ); доступ в ЛОМ із сторони кабельних ліній зв'язку. Несанкціонований доступ в ЛОМ із сторони кабельних ліній може здійснюватися наступними каналами: із сторони штатного користувача-порушника однієї ПЕОМ при зверненні до іншої інформації, в тому числі до файл-сервера; при приєднанні сторонньої ПЕОМ та іншої сторонньої апаратури; при побічних електромагнітних випромінюваннях і наведеннях інформації. Крім того, в результаті аварійних ситуацій,

відмов апаратури, помилок операторів і розробників програмного забезпечення ЛОМ, можливі переадресування інформації, відображення і видача її на робочих місцях, для неї не призначених, втрата інформації в результаті її випадкового стирання або пожежі.

З. потенційні безпеці інформації, що оброблюється в ПЕОМ /у. потенциальные информации, обрабатываемой в ПЭВМ/ — загрози, пов'язані з наявністю навмисних і випадкових несанкціонованих каналів доступу до інформації в ПЕОМ. До них відносяться: несанкціоноване спостереження інформації; несанкціонований доступ до інформації іншого користувача; несанкціонований вхід в ПЕОМ; знімання копій; уведення несанкціонованих програм; викрадення гнучких магнітних дисків; запис інформації на носій, що не стоїть на обліку; зміна схеми ПЕОМ і встановлення стороннього пристрою, прийом інформації на спеціальну апаратуру; читання залишків інформації.

З. прихована /у. скрытая/ [covert t.] — неусвідомлювані системою інформаційною в режимі реального часу вхідні дані, що загрожують її безпеці.

З. явна /у. явная/ [clear t.] — вхідні дані, що усвідомлюються системою інформаційною як загроза.

ЗАДАЧА /задача/ [task, problem, sum] — 1) Питання, яке розв'язується шляхом обчислень за визначеною умовою. 2) Основна одиниця роботи обчислювальної системи, яка потребує виділення ресурсів.

З. інформаційно-логічна /з. информационно-логическая/ [information-logical t.] — задача, яка об'єднує в собі ознаки завдання інформаційного і задачі логічної.

З. інформаційно-розрахункова /з. информационно-расчетная/ [information-computing t.] — задача, яка поєднує інформаційне завдання і розрахункову задачу.

З. логічна /з. логическая/ [logical t.] — задача обчислювальна, яка вирішується шляхом виконання логічних операцій.

З. обчислення дискретного логарифма /з. вычисления дискретного логарифма/ — див. проблема дискретного логарифма.

З. обчислювальна (розрахункова) /з. вычислительная (расчетная)/ [computing t.] — задача, яка

потребує виконання обчислювальних — арифметичних і логічних операцій.

З. прикладна /з. прикладная/ [application t.] — задача, яка ставиться у певній галузі практичної діяльності людини у інформаційному середовищі (полі). Див. також забезпечення математичне прикладне і забезпечення програмне прикладне.

ЗАЗЕМЛЕННЯ /заземление/ [ground] — з'єднання електричного апарата, пристрою із землею для захисту від небезпечної дії струму.

ЗАКЛАДКА /закладка/ [bug] — потай установлений технічний засіб або властивість деяких програм, які спрямовані на здійснення загрози для інформації (див. також пристрої закладні).

З. алгоритмічна /з. алгоритмическая/ — навмисне завуальоване спотворення будь-якої частини алгоритму вирішення задачі, або побудова його таким чином, що в результаті його кінцевої програмної реалізації у складі програмних компонент або комплексу програм останні будуть мати обмеження на виконання необхідних функцій, які задані специфікацією (технічним завданням) на програмні засоби, або взагалі їх не виконувати, при певних умовах протікання обчислювального процесу, що задаються семантикою даних, що перероблюються програмою, або появою у програмних компонент функцій, які не передбачені прямо або непрямо специфікацією, і які можуть бути виконаними при строго визначених умовах протікання обчислювального процесу.

З. апаратна /з. аппаратная/ [hardware b.] — див. зброя інформаційна апаратна.

З. до алгоритму шифрування /з. к алгоритму шифрования/ [black door] — випадково або навмисно зроблена особливість алгоритму шифрування, яка дозволяє проводити злом алгоритму шифрування. На відміну від лазівки її наявність, звичайно, є невідомою.

З. програмна /з. программная/ [program b.] — 1) Потай впроваджена програма або незадокументовані властивості забезпечення програмного, використання яких може призвести до обходу комплексу засобів захисту і (або) порушення політики безпеки. 2) Клас програм з потенційно небезпечними наслідками, для яких обов'язковим є виконання наступних функцій: руйнування (спотворення довільним чином) кодів програм в

оперативній пам'яті; збереження фрагментів інформації з оперативної пам'яті в деякій ділянці зовнішньої пам'яті прямого доступу (локальної або віддаленої); спотворення довільним чином, блокування і (або) підміни масивів інформації, що виводиться у зовнішню пам'ять або в канал зв'язку, утворених в результаті роботи прикладних програм, або масивів даних, що уже знаходяться у зовнішній пам'яті. Відмітною ознакою (відносно засобів несанкціонованого доступу) є відсутність функцій подолання захисту. Виділяють декілька видів з. п.: троянські програми; бомби логічні; люки логічні; пастки програмні; черв'яки програмні. Усі з. п. можна також класифікувати у відповідності до мети створення та за способом доставки в систему. За метою створення: з. п. класу "дослідник"; з. п. класу "перехоплювач"; з. п. класу "руйнівник"; з. п. класу "активна завада". За способом доставки в систему: закладки, асоційовані з програмно-апаратним середовищем (BIOS) (див. асоціювання з іншою програмою); закладки, асоційовані з програмами первинного завантаження (знаходяться в MasterBoot або Record BOOT — секторах активних розділів); закладки, асоційовані із завантаженням драйверів, командного інтерпретатора, мережних драйверів (завантаженням операційної системи); закладки, асоційовані з прикладним програмним забезпеченням загального призначення (вбудовані в клавіатурні й екранні драйвери, програми тестування ПЕОМ, утиліти й оболонки типу NORTON); модулі, що виконуються, які містять тільки код закладки (як правило, впроваджуються в пакетні файли типу .BAT); модулі-імітатори, що співпадають з деякими програмами, що потребують введення конфіденційної інформації, за зовнішнім виглядом; закладки, що маскуються під програмні засоби оптимізаційного призначення (архіватори, прискорювачі і т. ін.); закладки, що маскуються під програмні засоби ігрового й розважального призначення (як правило використовуються для первинного впровадження закладок типу "дослідник"). Як засоби зброї інформаційної п. з. мають достатньо специфічну форму реалізації процедури нападу, виконання функцій розвідки і дослідження систем захисту (наприклад, паролів доступу) елементів обчислювального середовища. 3) Сукупність операторів і (або) операндів (програмна конструкція), яка навмисне в завуальованій формі включається до складу виконуваного коду програмної компоненти на будь-якому етапі її розробки та реалізує певний несанкціонований алгоритм з метою обмеження або блокування

виконання програмною компонентою необхідних функцій при певних умовах протікання обчислювального процесу, що задаються семантикою даних, що перероблюються програмою, або появою у програмних компонент функцій, які не передбачені, але які можуть бути виконаними при строго визначених умовах протікання обчислювального процесу.

З. проектна /з. проектная/ — навмисне завуальоване спотворення вихідної формальної моделі керуючих даних або вибір заздалегідь некондиційної формальної моделі керуючих даних, такої, що в результаті її кінцевої програмної реалізації у складі програмних компонент або комплексу програм останні будуть мати обмеження на виконання необхідних функцій або взагалі їх не будуть виконувати, при певних умовах умовах протікання обчислювального процесу, що задаються семантикою даних, що перероблюються програмою, або з метою постачання програмної компоненти функціями , які не передбачені специфікацією (технічним завдання), і які можуть бути виконаними при строго визначених умовах протікання обчислювального процесу.

ЗАКЛИК /призыв/ — відозва, гасло; звертання до певної групи людей, в якому в стислій формі висловлена провідна ідея, вимога, завдання. З. є складовою частиною впливу змістом інформації. У практиці психологічної війни використовуються наступні види з.: прямі заклики; непрямі заклики; заклики на основі конкретних прикладів; невиразні заклики.

З. на основі конкретних прикладів /п. на основе конкретних примеров/ — заклики, призначені для популяризації (пропаганди) конкретних дій противника, які уже реалізували вимоги закликів. В цьому випадку сам заклик є прихованим показом переваг, які одержали особи, що здійснили ті чи інші дії.

З. невиразні /п. неопределенные/ — заклики, що спонукають об'єкт самостійно прийти до висновків, які логічно витікають з пред'явленої йому аргументації, хоча в тексті повідомлення відсутні конкретні пропозиції.

З. непрямі /п. косвенные/ — заклики, призначені для переконування (див. метод переконування)

шляхом натяків і обіцянок.

З. прямі /п. прямые/ — заклики, що припускають переконування (див. метод переконування), засноване на поданні сильних прямих аргументів. Об'єктові впливу в цьому випадку у відкритій формі пропонують, що йому слід зробити.

ЗАКОН /закон/ [law] — 1) Незалежна ні від чиєї волі, незаперечність, заданість, що склалася в процесі існування даного явища, його зв'язків і відношення з навколишнім світом. 2) Постанова державної влади, нормативний акт, прийнятий державною владою; установлені державною владою загальнообов'язкові правила.

З. інформаційної боротьби /з. информационной борьбы/ [information warfare l.] — закони, що характеризують впорядкованість будови і функціонування, тенденції зміни і розвитку тих чи інших явищ боротьби інформаційної. З. і. б. являють собою більш менш точне відображення у свідомості людей тих об'єктивних зв'язків і відносин, які існують і діють у інформаційному просторі. Якщо вони пізнані, відображені, описані, то стають основою для практичної діяльності з підготовки і ведення інформаційної боротьби. Так як сфера інформаційна є частиною соціальної діяльності суспільства, то в ній проявляють себе: загальні закони діалектики; загальні і специфічні закономірності соціального розвитку; власні закони, закономірності війни, інформаційної боротьби (наприклад, закон визначальної ролі політичних цілей війни; закони залежності ходу і кінця війни (інформаційної боротьби) від економічних, соціально-політичних, науково-технічних і воєнних можливостей протиборчих сторін). Особливістю законів (закономірностей) війни, а також інформаційної боротьби є те, що на відміну від законів і закономірностей природи вони проявляються тільки через діяльність людей.

ЗАКОНОДАВСТВО /законодательство/ [legislation] — 1) Встановлення, видання законів. 2) Сукупність усіх законів, що діють у будь-якій державі; юриспруденція.

З. воєнне /з. военное/ [military l.] — сукупність законів та інших нормативно-правових актів, що

регулюють відносини у сфері будівництва, життя і діяльності збройних сил.

З. інформаційне /з. информационное/ [information l.] — сукупність правових актів нормативних і окремих норм права, спрямованих на регулювання суспільних відносин у сфері інформаційній. З. і. є нормативною базою права інформаційного і являє собою комплексну галузь, що включає як деякі галузі законодавства і спеціальні нормативні акти, повністю присвячені проблемам інформації, так і окремі норми інформаційно-правові в актах інших галузей законодавства.

З. про захист інформації (даних) /з. о защите информации (данных)/ [data protection l.] — сукупність законів (норм), що регламентують законодавчі заходи, прийняті у державі для захисту інформації (даних), що оброблюються системами автоматизованими (комп'ютерами).

З. про інтелектуальну власність /з. о интеллектуальной собственности/ [copyright l.] — галузь законодавства інформаційного, основою якого є норми інформаційно-правові про захист законом власності інтелектуальної, а також про право кожного вільно шукати, одержувати, передавати, створювати і розповсюджувати інформацію будь-яким законним способом, гарантії для кожного свободи літературного, художнього, наукового, технічного та інших видів творчості, викладання. Результати творчої діяльності охороняються правом авторським, законодавством про промислову власність і про ноу-хау. Право про інтелектуальну власність закріплюється: фактом створення твору; шляхом реєстрації формули (змісту) винаходу; шляхом фіксації і зберігання в таємниці результату творчості. В перших двох випадках інформація, що створюється в процесі творчості і супроводжує цей процес, не потребує додаткового захисту, оскільки вона або сама є таким результатом або містить опис результату творчості. Додаткового захисту потребує інформація, що відображає секрети виробництва або секрети науки. З. п. і. в. можна поділити, в свою чергу, на: законодавство про авторське право і суміжні права, патентне законодавство і законодавство про ноу-хау.

З. про інформаційну безпеку /з. о информационной безопасности/ [information security l.] — сукупність законів (норм інформаційно-правових), що регламентують відносини з приводу прав, обов'язків і

відповідальності суб'єктів у зв'язку із створенням і застосуванням засобів і механізмів інформаційної безпеки у державі. Складовою частиною законодавства є сукупність актів нормативних, а також законів у галузі захисту державної таємниці. У зв'язку з введенням у практику мереж інформаційних транскордонних виникає необхідність правового регулювання відносин у галузі усіх видів і способів захисту інформації в цих мережах, насамперед засобами підпису цифрового електронного, засобами криптографічними.

ЗАКОНОМІРНІСТЬ /закономерность/ — 1) Властивість відбуватися відповідно до законів природи або суспільства, зумовленість цими законами. 2) Об'єктивно існуючий, постійний і необхідний взаємозв'язок між предметами, явищами, процесами, що випливає з їхньої внутрішньої природи, сутності.

З. психологічного впливу /з. психологического влияния/ — закономірності впливу на психіку людини: якщо вплив психологічний спрямований на споживчо-мотиваційну сферу психіки людини, то його результати виявляються в першу чергу на спрямованості й силі спонукання (потягу й бажань) людей; коли під прицілом емоційна сфера людей, то це відбивається на внутрішніх переживаннях, а також на відносинах між особистостями; сполучення впливів на споживчо-мотиваційну й емоційну сфери дозволяє впливати на вольову активність людей і таким чином керувати їхньою поведінкою; вплив на комунікативно-поведінкову сферу (специфіку взаємовідносин і спілкування) дозволяє створювати соціально-психологічний комфорт і дискомфорт, заставляти людей співробітничати або конфліктувати з оточуючими; в результаті впливу на інтелектуально-пізнавальну сферу психіки людини в потрібну сторону змінюються її уявлення, характер сприйняття нової інформації і, в результаті, "картина світу" людини.

ЗАКРИТТЯ /закрытие/ [close] — дія, спрямована на те, щоб будь-що стало недоступним для сторонніх, призначеним не для всіх.

З. інформації /закрытие информации/ [information-hiding] — див. захист інформації.

З. мовної інформації технічне /техническое з. речевой информации/ — спосіб приховування інформаційного мовної інформації, що забезпечується скремблюванням аналоговим мовної інформації, яка передається кабелями або радіоканалами.

ЗАЛУЧЕННЯ /привлечение/ [attraction] — спонукання до участі в будь-чому.

З. до співробітництва /п. к сотрудничеству/ — метод доступу до інформації, що ґрунтується на залученні до роботи співробітників державних і комерційних структур, які мають доступ до інформації, що цікавить органи розвідки або зловмисників. Основними способами залучення таких співробітників є наступні: співробітництво ініціативне; співробітництво через підкуп; співробітництво під загрозою. З. д. с. використовується для забезпечення регулярного добування інформації.

ЗАМОК /замок/ [lock] — 1) Пристрій для замикання дверей або воріт. Сучасні з. класифікуються наступним чином: механічні, що відкриваються (закриваються) механічним ключем; механічні кодові; електромеханічні; електронні кодові. Основною характеристикою з. є його стійкість до несанкціонованого відкривання. 2) В обчислювальній техніці — код, структура даних або програма, що використовуються для керування доступом до інформації; операція, що дозволяє тільки одному процесу мати доступ до певного ресурсу.

З. безсувальдні /з. бессувальдные/ — механічні замки, у яких ригелі переміщуються борідками ключа. Ригель в кожному замку стопорить підпружинена собачка. Секретність з. б. реалізують пристрої, що перешкоджають введенню в ключовину "чужого" ключа.

З. електронні /з. електронные/ [electronic l.] — замки кодові з електронними ідентифікаторами у вигляді мікросхем, розташованих в герметичному корпусі з нержавіючої сталі. Кожна мікросхема має незмінюваний 64-розрядний номер (ключ), для визначення якого необхідно перебрати біля 10^{20} комбінацій. Механічна стійкість з. е. забезпечується за рахунок подовжених горизонтальних і вертикальних ригелів. Ключ може вводитися зі спеціальної клавіатури, або з ідентифікаційної картки.

З. захисту (секретності) /з. защиты (секретности)/ [protection (privacy) l.] — програмний механізм перевірки паролів при зверненні до бази даних або до її фрагментів (файлів, областей), що забезпечує обмеження доступу до записів.

З. кодовий /з. кодовий/ [code l., combination l.] — замок, ключем до якого служить певний код. З. к.

бувають механічними, електромеханічними, електронними.

З. механічні /з. механические/ [key-operated l., mechanical l.] — замки, для яких характерна наявність ригеля (засува), сувальд, ключа, корпусу і запірної планки. З. м. поділяються на врізані, накладні і навісні. За механізмом секретності розрізняють безсувальдні, сувальдні, циліндрові і сейфові замки.

З. пам'яті /з. памяти/ [memory l.] — код у дескрипторі сегмента або сторінки віртуальної пам'яті, що використовується для обмеження доступу. При цьому до сегмента можуть звертатися тільки процеси, що мають у своєму дескрипторі відповідний ключ.

З. сейфові /з. сейфовые/ [safe l.] — замки, призначені для закривання (відкривання) сейфів. Бувають сувальдного типу з кількістю сувальд не менше 8 і складним профілем борідок ключа, кодовими механічними, часовими і електронними. Найпоширенішими з. с. є дискові кодові замки з секретністю $10^6 - 10^7$ комбінацій.

З. сувальдні /з. сувальдные/ [level l.] — замки механічні, що мають ригель, зблокований з пакетом з 3–6 і більше підпружинених сувальд, змонтованих на одній осі. Сувальди виготовлені у вигляді пластин, що мають з боку сполучення з борідками ключа різні контури. Різноманітні секрети утворюють сувальди, складені разом пакетом. Їм відповідають в замку профілі борідки ключа.

З. циліндрові /з. цилиндровые/ [cylinder l.] — замки механічні, що діють за принципом сувальдних, але в іншому конструктивному виконанні. Циліндричний механізм в зібраному вигляді являє собою однорядний або дворядний сувальдний пристрій. Сердечник обертається, коли верхні торці вставлених в нього штифтів розташовані урівень з поверхнею цього сердечника, що можливо тільки при наявності в ключовому пазові "свого" ключа. Подібні замки мають малу замкову щілину і легкий плоский ключ.

ЗАПАМ'ЯТОВУВАННЯ /запоминание/ — узагальнена назва процесів, які забезпечують збереження матеріалу в пам'яті людини. Успішність з. визначається в першу чергу можливістю введення нового матеріалу в систему осмислених зв'язків. Важливу роль серед його механізмів має повторення. Разом з тим можна обійтися і без повторення, якщо людині необхідно запам'ятати життєво важливий матеріал, або

відомості, які несуть велику смислове навантаження.

ЗАПИС /запись/ [record, writing] — 1) Матеріалізація будь-якої інформації шляхом зміни параметрів носія інформації. 2) Фіксація звуків і (або) зображень за допомогою технічних засобів в будь-якій матеріальній формі, що дозволяє здійснювати їхнє неодноразове сприйняття, відтворення або повідомлення. 3) Одиниця обміну даними між програмою і зовнішньою пам'яттю. 4) В мовах програмування — агрегат, складові якого (поля) можуть мати ім'я та різні атрибути.

З. дублюючий /з. дублирующая/ [duplicate r.] — запис, що має однаковий ключ з іншим записом у цьому ж файлі або у базі даних.

З. з ключем /з. с ключом/ [r. with key] — запис, що містить вбудований або невбудований ключ.

З. контрольний /з. контрольная/ [control r.] — запис, що містить контрольні суми, обчислені шляхом підсумовування значень з інших записів файла. Контрольні суми можуть також нести додаткову інформацію або використовуватися тільки для перевірки правильності даних.

ЗАПИТ /запрос/ [query, request, interrogation] — 1) Посилання сигналу, що ініціює відповідь. 2) Вхідне повідомлення, яке містить вимогу до системи на виділення ресурсу.

З. на доступ /з. на доступ/ [access r.] — звернення одного об'єкта комп'ютерної системи до іншого з метою отримання певного типу доступу.

ЗАПОБІГАННЯ /предотвращение/ [prevention] — недопущення чогось заздалегідь, відвертання.

З. витоку інформації матеріально-речовими каналами /п. утечки информации по материально-вещественному каналу/ – спосіб протидії зняттю інформації з матеріально-речовинних носіїв інформації, що включає захист інформації, що міститься у відходах і захист демаскуючих речовин.

З. витоку інформації через закладні підслуховуючі пристрої /п. утечки информации по закладных подслушивающих устройствах/ — спосіб протидії підслухуванню, що включає виявлення, локалізацію і вилучення або придушення закладних пристроїв. Відповідно до цього засоби запобігання витоку поділяються на засоби радіоконтролю приміщень, засоби пошуку невипромінюючих закладних пристроїв і засоби

придушення закладних пристроїв.

З. витоку інформації через побічні випромінювання і наведення /п. утечки информации побочными излучениями и наводками/ [an. TEMPEST] — спосіб протидії витоку інформації за допомогою небезпечних сигналів, що створюються випромінюваннями і наведеннями електромагнітними побічними. Способи і засоби захисту інформації через ПЕМВН повинні задовольняти наступним вимогам: небезпечні сигнали, які можуть нести конфіденційну інформацію, повинні бути ослаблені до рівня, що виключає зняття з них інформації на межі контрольованої зони; засоби захисту не повинні вносити помітних спотворень в роботу функціональних пристроїв, що використовуються в організації, і не ускладнювати процес користування ними. Запобігання витоку інформації небезпечними сигналами здійснюється шляхом придушення небезпечних електричних сигналів акустоелектричних перетворювачів і екранування побічних полів. Див. також захист від ПЕМВН.

З. несанкціонованому запису мовної інформації на диктофон /п. несанкционированной записи речевой информации на диктофон/ — виявлення працюючого диктофону, прихованого в кишені, портфелі, сумці або інших речах, що носяться, та порушення роботи диктофону таким чином, щоб якість записаної інформації була нижчою за допустимий рівень. Вирішення навіть першого завдання дозволяє прийняти заходи захисту інформації, в тому числі: припинити переговори або нараду; знижувати рівень конфіденційності розмови, не допускаючи висловлювань, які можуть після їхнього документування на диктофон заподіяти шкоду організації або учасникам переговорів.

ЗАРАЖЕННЯ /заражение/ [contamination] — процес передавання зарази комусь, чомусь.

З. психічне /з. психическое/ — процес передавання емоційного стану від одного індивіда до іншого на психофізіологічному рівні контакту — окрім смислового впливу або додатково до нього. Наприклад, через з. п. передається такий психічний стан як паніка, в результаті якого організована група перетворюється в некерований натовп. В процесі зараження на кожного члена групи діє не тільки навіюючий об'єкт, але й інші члени групи, що помітно збільшує загальний ефект навіювання.

ЗАСВОЄННЯ /усвоение/ — основний шлях набування суспільного досвіду.

З. психологічного впливу /у. психологического влияния/ — засвоєння інформації об'єктом впливу психологічного. Ефективність з. п. в. в першу чергу залежить від особливостей пізнавальних процесів людини: пам'яті, мислення і уяви.

ЗАСЕКРЕЧУВАННЯ /засекречивание/ [classification, scrambling, security classifying, cryptment] — дія, спрямована на встановлення будь-чого секретним, недоступним для сторонніх осіб.

З. відомостей і їхніх носіїв /з. ведомостей и их носителей/ — уведення в передбаченому законом порядку для відомостей, що складають державну таємницю, обмежень на їхнє розповсюдження і доступ до їхніх носіїв. Обґрунтованість засекречування полягає у встановленні шляхом експертної оцінки доцільності засекречування конкретних відомостей, ймовірних економічних і інших наслідків цього акту, виходячи з балансу інтересів життєво важливих держави, суспільства і громадян.

ЗАСІБ /средство/ — 1) Спосіб, прийом, захід, якась спеціальна дія, що дає можливість здійснити щось. 2) Те, що служить знаряддям у якійсь дії, справі.

З. авторизації програм /с. авторизации программ/ [program authorized f.] — засоби, що дозволяють ідентифікувати програму, що має обмеження на доступ до даних. Звичайно, для цього використовуються засоби ідентифікації, паролі та обмеження на доступ.

З. апаратні /с. аппаратные/ [hardware] — технічні засоби, що використовуються для оброблення даних, на відміну від програм, процедур, правил і документації; усе механічне, електричне і електронне обладнання, яке використовується в техніці обчислювальній.

З. високочастотного нав'язування /с. высокочастотного навязывания/ — засоби добування мовної інформації шляхом підслухування на основі дистанційного впливу високочастотним випромінюванням електромагнітним або сигналами електричними на елементи, що здатні модулювати їхні інформаційні параметри первинними електричними або акустичними сигналами з мовною інформацією. Такими елементами можуть бути різноманітні порожнини з електропровідною поверхнею, які являють собою високочастотні

контури з розподіленими параметрами і об'єм яких може змінюватися під дією акустичної хвилі. Якщо частота такого контуру співпадає з частотою високочастотного нав'язування, а поверхня порожнини знаходиться під впливом акустичної інформації, то еквівалентний контур перевипромінює і модулює зовнішнє випромінювання. Більш часто модулюючим елементом служить будь-який нелінійний елемент, в тому числі в схемі телефонного апарата. В цьому випадку високочастотне нав'язування забезпечується підведенням до телефонного апарата високочастотного гармонічного сигналу шляхом приєднання до телефонного кабелю високочастотного генератора. В результаті взаємодії високочастотного коливання з мовними сигналами на нелінійних елементах телефонного апарата здійснюється модуляція високочастотного коливання низькочастотним сигналом. Модульовані високочастотні сигнали можуть бути перехоплені приймачем зловмисника.

З. виявлення елементів закладок /с. обнаружения элементов закладок/ — засоби виявлення невипромінюючих закладних пристроїв за фізичними властивостями елементів електричної схеми або конструкції. Такими елементами є: напівпровідникові прилади, які застосовуються в будь-яких закладних пристроях, металеві деталі конструкцій, елементи, що поглинають рентгенівські промені. До з. в. е. з. відносяться локатори нелінійні, металодетектори, установки рентгенівські.

З. відновлення даних /с. восстановления данных/ [data restore f.] — програми і процедури, призначені для відновлення даних у разі їхнього спотворення або стирання.

З. гасіння пожежі /с. тушения пожара/ — сукупність засобів, призначених для ліквідації пожежі. Традиційні з. г. п. (піноутворюючі вогнегасники, механічні засоби (багри, сокири) для руйнування осередку пожежі, бочки з піском, пожежні рукави і т. ін.) розташовуються в легкодоступних місцях організації. Поряд з піноутворюючими вогнегасниками все частіше використовуються малогабаритні самоспрацьовуючі порошкові вогнегасники. Гасіння пожежі за їхньою допомогою здійснюється без участі людини шляхом імпульсного викиду порошку в зону загоряння. Запуск здійснюється автоматично при дії на вогнегасник відкритого полум'я або при підвищені температури в об'ємі, що захищається. Перспективними засобами

пожежної охорони є автоматичні системи гасіння пожежі.

З. глушення акустичних сигналів /с. глушения акустических сигналов/ — засоби приховування акустичних сигналів енергетичного, призначені для інтенсивного поглинання енергії акустичної хвилі при розповсюдженні її в спеціальній конструкції, що називається глушником. В залежності від способу глушення звуку глушники поділяються на абсорбційні, реактивні і комбіновані. В абсорбційних глушниках здійснюється звукопоглинання в матеріалах і конструкціях, в реактивних — в результаті відбиття звуку назад до джерела. Комбіновані глушники об'єднують обидва способи. Найбільш ефективним заходом попередження витоку інформації через повітропроводи будівлі (приміщень) є встановлення в них абсорбційних глушників.

З. добування інформації /с. добывания информации/ — технічні пристрої, призначені для дистанційного добування інформації. В залежності від способу дистанційного добування інформації розподіляються на засоби спостереження, засоби перехоплення, засоби підслухування, засоби добування інформації про радіоактивні речовини. В залежності від місця розташування з. д. і. — на засоби добування інформації наземні, засоби добування інформації космічні, засоби добування інформації повітряні, засоби добування інформації корабельні і т. ін.

З. добування інформації корабельні /с. добывания информации корабельные / — засоби добування інформації, призначені для добування інформації без порушення державного кордону, розташовані на кораблях, що в мирний час плавають в нейтральній зоні біля морських кордонів. До к. з. д. і. відносяться засоби радіо- і радіотехнічної розвідки, засоби спостереження берегів та їхнього підводного рельєфу.

З. добування інформації космічні /с. добывания информации космические/ — засоби добування інформації зверху, розташовані на космічних апаратах або штучних супутниках Землі, призначені для добування інформації без порушення державного кордону. Входять до складу різноманітних космічних розвідувальних систем: спеціалізованих (фото, оптико-електронних, радіо і радіотехнічних, радіолокаційних)

і комплексної розвідки, наприклад, фотографування і перехоплення радіотехнічних сигналів.

З. добування інформації наземні /с. добывания информации наземные/ — засоби добування інформації наземного розташування, призначені для добування інформації без фізичного проникнення в контрольовану зону. За способом застосування з. д. і. н. розподіляються на стаціонарні та мобільні. Мобільні засоби можуть розташовуватися та функціонувати в нерухомих і рухомих наземних транспортних засобах (найчастіше автомобілях) або носитися та функціонувати в одежі людини, сумках, портфелях тощо.

З. добування інформації повітряні /с. добывания информации воздушные/ — засоби добування інформації, призначені для добування інформації без порушення державного кордону, розташовані на літальних апаратах (розвідувальних літаках, апаратах літальних безпілотних), що здійснюють у мирний час польоти вздовж повітряного кордону. До з. д. і. п. відносяться: авіаційна фотоапаратура; бортові засоби радіо- і радіотехнічної розвідки; радіолокаційні станції бічного огляду; засоби спостереження в інфрачервоному діапазоні; апаратура телевізійного спостереження.

З. добування інформації про радіоактивні речовини /с. добывания информации о радиоактивных веществах/ — засоби виявлення і вимірювання демаскуючих ознак радіоактивних речовин, якими є α, β і γ-випромінювання. Заряд і кінетичну енергію α і β-часток визначають за їхнім відхиленням в електричному і магнітному полях відомої напруженості. Енергію і довжину хвилі γ-випромінювання розраховують за енергією електронів, що вивільнюються з різноманітних речовин під дією цього випромінювання. Типовий прилад радіаційної розвідки складається з детектора, підсилювача та індикатора. Детектор перетворює енергію радіоактивного випромінювання в електричні сигнали, які після підсилення подаються на стрілочний або цифровий індикатор. Детекторами можуть служити іонізаційні камери, газорозрядні та сцинтиляційні лічильники, кристали напівпровідника, фотоплівка. В залежності від призначення прилади для виявлення і вимірювання радіоактивного випромінювання поділяються на індикатори радіоактивності, радіометри і дозиметри.

З. доступу до даних /с. доступа к данным/ [access f.] — оператори (макрокоманди) прикладної

програми і керуючі модулі операційної системи, що забезпечують доступ до даних в пам'яті ЕОМ.

З. доступу до мережі /с. доступа к сети/ [network access f.] — пристрої, що забезпечують взаємодію між місцевою та магістральною мережами: концентратори, мультиплексори, комутатори і т. ін.

З. забезпечення автоматизованих інформаційних систем і їхніх технологій /с. обеспечивания автоматизированных информационных систем и их технологий/ — засоби програмні, технічні, лінгвістичні, організаційно-правові засоби, засоби технологічного забезпечення, які використовуються або створюються при проектуванні систем інформаційних та забезпечують їхню експлуатацію.

З. забезпечення автоматизованих інформаційних систем лінгвістичні /с. обеспечения автоматизированных информационных систем лингвистические/ — словники, тезауруси, класифікатори, інші лінгвістичні засоби.

З. забезпечення автоматизованих інформаційних систем програмні /с. обеспечения автоматизированных информационных систем программные/ — системи операційні, програми прикладні, інші програмні засоби.

З. забезпечення автоматизованих інформаційних систем технічні /с. обеспечения автоматизированных информационных систем технические/ — засоби обчислювальної техніки; копіювально-розмножувальна техніка, оргтехніка, засоби зв'язку, засоби телекомунікацій, інші технічні засоби.

З. захисту /с. защиты/ [protection f.] — програмні, програмно-апаратні та апаратні засоби, що реалізують механізми захисту.

З. захисту автоматизованої інформаційної системи організаційно-правові /с. защиты автоматизированной информационной системы организационно-правовые/ [administrative security f., security regulations (інструкції із заходів забезпечення безпеки)] — положення і статут, порядок реалізації функцій і завдань, посадові інструкції, порядок застосування і користування системою захисту системи інформаційної автоматизованої, нормативно-технічні документи.

З. захисту апаратні /с. защиты аппаратные/ — засоби апаратні, призначені для захисту інформації

від несанкціонованого доступу, копіювання, крадіжки, модифікації або руйнування.

З. захисту від несанкціонованого доступу /с. защиты от несанкционированного доступа/ [acess control facility] — програмні, технічні або програмно-технічні засоби, що призначені для запобігання або суттєвого утруднення доступу несанкціонованого.

З. захисту інформації /с. защиты информации/ [security f., protection f,] — апаратні, програмні, криптографічні та інші засоби, що запобігають доступу несанкціонованому до інформації, засоби, в яких вони реалізовані, а також засоби контролю ефективності захисту інформації.

З. захисту інформації в локальній обчислювальній мережі від випадкових впливів /с. защиты информации в локальной вычислительной сети от случайных влияний/ — сукупність засобів системи захисту інформації в локальній обчислювальній мережі, призначених для захисту від випадкових впливів на апаратуру та програмне забезпечення мережі локальної обчислювальної. До таких засобів відносяться засоби підвищення вірогідності інформації, резервування інформації, спеціальні схемотехнічні рішення та система функціонального контролю та діагностики відмов.

З. захисту інформації в локальній обчислювальній мережі від умисних несанкціонованих доступів /с. защиты информации в локальной вычислительной сети от умышленных несанкционированных доступов/ — сукупність засобів системи захисту інформації в локальній обчислювальній мережі, призначених для контролю доступу на територію об'єкта, захисту інформації в ПЕОМ, упізнавання і розмежування доступу до інформації мережі локальної обчислювальної, захисту інформації в лініях зв'язку, захисту інформації від випромінювань і наведень електромагнітних побічних, контролю цілісності мережі.

З. захисту інформації в трактах передавання даних /с. защиты информации в трактах передачи данных/ — набір засобів, що забезпечують захист інформації в елементах (сукупностях елементів) тракту передавання даних: ланцюжок "станція робоча — сервер комунікаційний — апаратура передавання даних" закривається системою захисту інформації в комплексі засобів автоматизації; канал зв'язку — засобами шифрування лінійного; вузол комутації повідомлень — власною системою захисту, аналогічною захисту в

КЗА. Передавання документів з певними юридичними гарантіями потребує введення спеціальних засобів захисту, до функцій яких входять: шифрування з гарантованою стійкістю інформації її відправником і дешифрування одержувачем; забезпечення відповідних повноважень користувачів шляхом розповсюдження ключів шифрування; забезпечення юридичної значущості документам, що передаються по мережі передавання даних. Перші дві функції виконують засоби шифрування абонентського, а третю — засоби підпису цифрового.

З. захисту інформації сертифіковані /с. защиты информации сертифицированные/ [certificate safeguards] — засоби захисту інформації, які відповідають вимогам захисту відомостей відповідного ступеня секретності.

З. захисту програмного забезпечення /с. защиты программного обеспечения/ [software protection facility] — засоби, що забезпечують захист програмних засобів від несанкціонованого доступу.

З. зашумлення /с. зашумления/ — засоби енергетичного приховування акустичного сигналу, призначені для маскування акустичних сигналів. Зашумлення здійснюється за допомогою шумових генераторів — акустичних і вібраційних. Акустичне зашумлення приміщень забезпечує ефективний захист інформації в ньому, коли акустичний генератор розташований до приймача акустичного зловмисника ближче, ніж джерело інформації. Більш ефективним і активним способом захисту інформації, що передається структурним звуком, є вібраційне зашумлення. Шум в звуковому діапазоні у твердих тілах створюють п'єзокерамічні вібратори акустичного генератора, що прикріплюються до поверхні зашумлюваної огорожі (вікна, стіни, стелі і т. ін.) або твердотільного звукопровода (батареї опалення, труби і т. ін.). Один вібровипромінювач (вібратор) вібраційного акустичного генератора забезпечує ефективне зашумлення в радіусі 1,5–5 м.

З. зв'язку /с. связи/ [communication(s) f.] — технічний пристрій, що здійснює передавання, оброблення та (або) приймання, а також доставку повідомлень у системі зв'язку.

З. звукоізоляції акустичного сигналу /с. звукоизоляции акустического сигнала/ — засоби приховування акустичного сигналу енергетичного, призначені для локалізації джерел акустичних сигналів у

замкнутому просторі усередині контрольованих зон. Основна вимога до з. з. а. с. — забезпечення за межами контрольованої зони співвідношення сигнал-завада, яке не повинно перевищувати максимально-допустимі значення, що виключають добування інформації зловмисниками. Враховуючи, що середня гучність звуку людини, що розмовляє, в приміщенні складає біля 50–60 дБ, то в залежності від категорії приміщення (3, 2, 1) показник звукоізоляції засобів звукоізоляції приміщення для різних частот (500, 1000, 2000, 4000 Гц) повинен складати від 43 до 55 дБ. Звукоізоляція забезпечується за допомогою архітектурних і інженерних конструкцій: звукоізолюючих огорож, акустичних екранів, звукоізолюючих кабін (для людей) і кожухів (для випромінюючих звуки механізмів і машин).

З. звукопоглинання акустичної хвилі /с. звукопоглощения акустической волны/ — засоби приховування акустичного сигналу енергетичного, що забезпечують перетворення в матеріалі звукопоглинальному кінетичної енергії акустичної хвилі в теплову енергію. Для поглинання звуку в приміщеннях застосовуються звукопоглинальні облицювання у вигляді акустичних плит дрібнозернистої або стільникової структури та звукопоглинальні облицювання із шару пористо-волокнистого матеріалу (скляного або базальтового волокна, мінеральної вати) у захисній оболонці з тканини або плівки з перфорованим покриттям (металевим, гіпсовим та ін.). Плоский шар звукопоглинального матеріалу облицювань встановлюється на жорсткій основі, яка прикріплюється безпосередньо або з повітряним проміжком до поверхні огорожі, до стелі або стін. Для додаткового звукопоглинання і зменшення кількості перевідбиттів від огорож із метою зменшення часу реверберацій використовуються штучні звукопоглиначі, що являють собою одно або багатошарові об'ємні звукопоглинальні конструкції (у вигляді куба, паралелепіпеда, конуса), які підвішуються до стелі приміщення. Розміри граней штучних звукопоглиначів складають 40–400 см.

З. ідентифікації людей /с. идентификации людей/ [person identification f.] — засіб керування доступом людей на територію, що охороняється. З. і. л. поділяються на атрибутивні і біометричні.

З. інженерного захисту і технічної охорони об'єктів /с. инженерной защиты и технической охраны объектов/ — сукупність засобів, основу яких складають механічні засоби та інженерні споруди, що пере-

шкоджають фізичному пересуванню зловмисників до місця знаходження об'єкта захисту, технічні засоби, що інформують співробітників служби безпеки (охорону) про проникнення зловмисників у контрольовану зону і дозволяють спостерігати обстановку в них, а також люди і засоби, що знешкоджують загрози. Проникнення зловмисників може бути потайним, з механічним руйнуванням інженерних конструкцій і засобів охорони з допомогою спеціальних інструментів або вибуху і в деяких випадках у вигляді збройного нападу з нейтралізацією охоронців. У відповідності з принципами багатозональності і багаторубіжності захисту інформації рубежі захисту створюються, насамперед, на межах зон контрольованих. Люди і засоби інженерного захисту і технічної охорони об'єкта утворюють систему охорони об'єкта.

З. інформаційно-психологічного ураження людей /с. информационно-психологического поражения людей/ — засоби зброї інформаційної, призначені для використання в війні психологічній (інформаційно-психологічній війні) для впливу на людей з метою зміни і керування їхньою індивідуальною і колективною поведінкою. Поряд із використанням традиційних засобів (друковані і електронні засоби масової інформації) іде активна розробка спеціальних психофізичних засобів впливу на людину як через ЗМІ, так і через комп'ютерні мережі і т. ін.

З. інформаційної безпеки /с. информационной безопасности/ [infosecurity f.] — засоби, за допомогою яких здійснюються заходи захисту систем керування, зв'язку, комп'ютерних мереж, недопущення підслуховування, маскування, запобігання викрадення.

З. керування доступом людей і транспорту /с. управления доступом людей и транспорта/ — сукупність засобів пунктів контрольно-пропускних призначених для реалізації санкціонованого доступу на територію, що охороняється, людей і транспорту. До таких засобів відносяться механічні засоби (турнікети, розсувні або обертальні двері, ворота, шлагбауми для авто- і залізничного транспорту і т. ін.) і засоби (пристрої) ідентифікації людей.

З. керування системою охорони /с. управления системой охраны/ — сукупність засобів, що забезпечує функціонування системи охорони об'єктів і управління її елементами в різноманітних ситуаціях.

Збільшення кількості засобів в автономній системі охорони і об'єктів у централізованій системі охорони ускладнює управління ними. Для підвищення ефективності управління в автономній системі створюються автоматизовані інтегровані системи охорони. Підвищення ефективності управління централізованими системами охорони забезпечується автоматизацією процесів контролю й охорони (узяття під охорону і зняття з неї), оброблення сигналів сигналізаторів, реєстрації стану об'єктів охорони і прийнятих заходів.

З. комп'ютерні когнітивні /с. компьютерные когнитивные/ [cognitive computer tools] — комплекс віртуальних пристроїв, програм і систем, що реалізують спільне оброблення зорової інформації у вигляді образів, процесів і структур, а також інтерактивну взаємодію з ними.

З. контролю і керування доступом /с. контроля управления доступом/ [access control f.] — сукупність засобів для реалізації системи розпізнавання і розмежування доступу. До них найчастіше відносяться: спеціальне програмне забезпечення управління доступом, термінал служби безпеки інформації, з якого здійснюється централізоване управління доступом, комплект фізичних носіїв кодів паролів — магнітних карт, перепусток, кредитних карток і т. д., а також апаратура запису кодів паролів на ці носії і засоби захисту кодів паролів.

З. контролю і керування захистом інформації в локальній обчислювальній мережі /с. контроля и управления защитой информации в локальной вычислительной сети/ [security management f.] — сукупність засобів системи захисту інформації в локальній обчислювальній мережі, призначених для централізованого контролю і управління безпекою інформації. До таких засобів відносяться: забезпечення безпеки інформації в локальній обчислювальній мережі програмне спеціальне, персональне робоче місце служби безпеки інформації мережі, інформаційно-лінгвістичне забезпечення та організаційні заходи.

З. контролю проводових ліній /с. контроля проводных линий/ — засоби, призначені для виявлення в проводових лініях небезпечних сигналів і їхніх джерел, в тому числі пристроїв закладних. До з. к. п. л. відносяться прилади контролю телефонних ліній і ліній електроживлення. Засобами і програмним забезпеченням для виявлення і аналізу сигналів закладних пристроїв в проводових лініях можуть оснащуватися

також комплекси радіомоніторингу приміщень автоматизовані.

З. криптографічного захисту інформації /с. криптографической защиты информации/ [cryptographic information protection f., cryptographic f.] — програмний, апаратно-програмний, апаратний або інший засіб,призначений для захисту інформації криптографічного.

З. лазерного підслухування /с. лазерного подслушивания/ — засоби, призначені для зняття акустичної інформації з плоских поверхонь, що вібрують під впливом акустичних хвиль (насамперед з шибок закритих вікон). З. л. п. складається з лазера в інфрачервоному діапазоні і приймача оптичного. Лазерний промінь за допомогою оптичного прицілу направляється на вікно приміщення, в якому ведуться розмови, що цікавлять зловмисника. При відбиванні лазерного променя від вібруючої поверхні здійснюється модуляція акустичним сигналом кута відбиття променя або його фази. В залежності від способу демодуляції лазерного променя з. л. п. поділяються на засоби з демодуляцією кута відбиття променя і демодуляцією фази відбитого променя.

З. масової інформації (ЗМІ) /с. массовой информации (СМИ)/ [mass media] — періодичне друковане видання, радіопрограма, теле-, відеопрограма, кінохронікальна програма, інша форма розповсюдження інформації масової. Див. також мас-медіа.

З. нейтралізації загроз об'єктові охорони /с. нейтрализации угроз объекту охраны/ — сукупність засобів для фізичного і психологічного впливу на зловмисників, що проникли на територію, що охороняється, а також засобів гасіння пожежі, функціонально об'єднаних в підсистему нейтралізації загроз системи охорони об'єктів, яка може включати: підрозділ охорони; тривожну звукову і світлову сигналізацію; штатного або нештатного пожежника; засоби гасіння пожежі; джерела резервного (аварійного) електроживлення.

З. несанкціонованого доступу /с. несанкционированного доступа/ — клас програм з потенційно небезпечними наслідками, для яких обов'язковим є виконання наступних функцій: руйнування (спотворення довільним чином) кодів програм в оперативній пам'яті; збереження фрагментів інформації з оперативної пам'яті в деякій ділянці зовнішньої пам'яті прямого доступу (локальної або віддаленої); спотворення до-

вільним чином, блокування і (або) підміни масивів інформації, що виводиться у зовнішню пам'ять або в канал зв'язку, утворених в результаті роботи прикладних програм, або масивів даних, що уже знаходяться у зовнішній пам'яті; нейтралізування роботи тестових програм і систем захисту інформаційних ресурсів. До з. н. д. відноситься всіляке позаштатне програмне забезпечення мереж обміну інформацією, яке противник може використати для порушення цілісності операційної системи або обчислювального середовища. Часто цей тип програмного забезпечення використовується для аналізу систем захисту, з метою їхнього подолання й реалізації несанкціонованого доступу до інформаційних ресурсів мереж обміну інформацією. Відмітною ознакою (відносно закладок програмних) з. н. д. є наявність функцій подолання захисту.

З. обмеження доступу /с. ограничения доступа/ [access limit f.] — сукупність засобів, призначених для виключення випадкового або навмисного доступу сторонніх осіб на територію розташування комплексів технічних засобів оброблення інформації і безпосередньо до апаратури. За допомогою з. о. д. може бути створений захисний контур з двома видами перепон: фізичної і контрольно-пропускної. Такі перепони часто називають системою охоронної сигналізації і системою контролю доступу.

З. обчислювальної техніки захищені /с. вычислительной техники защищенные/ [trusted computer systems] — засоби обчислювальної техніки (автоматизовані системи), в яких реалізований комплекс засобів захисту.

З. охорони технічні (ТЗО) /с. технические охраны (ТСО)/ — складова частина підсистеми сповіщення системи охорони об'єктів, призначена для виявлення спроб подолання зловмисником бар'єрів і механічних перепон, а також пожежі. Сукупність ТЗО, призначених для вирішення певної групи завдань, утворюють систему або комплекс технічних засобів охорони.

З. перехоплення /с. перехвата/ — див. перехоплення, комплекс засобів радіоперехоплення.

З. підслухування /с. подслушивания/ [wiretapping f.] — технічні засоби і пристрої, призначені для реалізації різноманітних способів підслухування: приймачі акустичні, в тому числі з спрямованими мікрофонами; приймачі небезпечних сигналів; пристрої закладні; засоби лазерного підслухування; засобів

високочастотного нав'язування і т. ін.

З. порушення роботи закладки /с. нарушения работы закладки/ — засоби придушення закладних пристроїв, що генерують сигнали-завади з частотою, вищою за 20 кГц, які змінюють режими роботи приєднаних до телефонної лінії закладних пристроїв, в результаті чого змінюється частота і розширюється спектр їхнього випромінювання. Внаслідок цього погіршується розбірливість мови, що приймається зловмисником, зменшується в декілька разів дальність підслухування, а також порушується робота пристроїв автоматичного регулювання рівня запису і автоматичного включення диктофона голосом.

З. пошуку невипромінюючих закладних пристроїв /с. поиска неизлучающих закладных устройств/ — засоби, призначені для виявлення *х пристроїв закладних проводових* і радіозакладок, що управляються дистанційно. До засобів пошуку таких закладок відносяться засоби контролю проводових ліній, виявники пустот та засоби виявлення елементів закладок.

З. придушення закладних пристроїв /с. подавления закладных устройств/ — засоби, призначені для енергетичного приховування сигналів пристроїв закладних, порушення працездатності закладок або їхнього фізичного руйнування. До з. п. з. п. відносяться генератори завад з лінійним або просторовим зашумленням, засоби порушення роботи закладки та засоби руйнування закладних пристроїв. Для придушення радіовипромінюючих закладних пристроїв найбільш доцільно застосовувати загороджувальні завади, що мають ширину спектра випромінювання в 1,5–2 рази більшу за ширину спектра сигналу. В цьому випадку малопотужний генератор завад (до 1 Вт) може гарантовано забезпечити безпеку інформації від витоку через закладки, але при умові збігу частот генератора і закладки. Знання частоти радіозакладки передбачає її виявлення, а виявлення — локалізацію з наступним вилученням. Тому зашумлення сигналів закладок доцільно здійснювати при безперервному радіомоніторингу приміщень шляхом автоматичного вмикання на частотах випромінювання радіозакладок передавача загороджувальної завади.

З. психологічної війни технічні /с. психологической войны технические/ — технічні засоби призначені для практичного вирішення завдань психологічного впливу на війська і цивільне населення. До з. п. в.

т. відносяться: засоби звукового мовлення; засоби радіомовлення і телебачення; поліграфічні засоби; засоби доставки інформаційно-пропагандистських матеріалів.

З. психотропні /с. психотропные/ — лікувальні речовини, що здійснюють вибірковий вплив на психічні функції людини: антидепресанти, нейролептичні, психостимулюючі засоби, транквілізатори.

З. радіоелектронні (РЕЗ) /с. радиоэлектронные (РЭС)/ — технічні пристрої, дія яких базується на принципах радіотехніки та електроніки і, які призначені для генерування, випромінювання, приймання, перетворення та підсилення електромагнітних коливань. Конструктивно РЕЗ складаються з передавальних, приймальних та антенних пристроїв, апаратури оброблення, реєстрації та відображення інформації (сигналів). РЕЗ є важливою складовою частиною бойових засобів, систем та комплексів розвідки і спостереження, управління військами (силами) та бойовими засобами.

/с. радиоконтроля помещений/ — засоби, призначені для виявлення пристроїв закладних, що випромінюють радіохвилі під час їхнього пошуку. До з. р. п. відносяться виявники поля, побутові радіоприймачі, приймачі спеціальні та комплекси радіомоніторингу приміщень автоматизовані.

З. радіолокаційного спостереження /с. радиолокационного наблюдения/ — засоби радіотехнічні, призначені для спостереження повітряного простору і земної поверхні методами радіолокації. Можливості з. р. с. з добування інформації визначаються в основному характеристиками радіолокаційних сигналів і розподілом їхньої енергії у просторі (діаграмою спрямованості). Див. також радіолокаційна станція та радіолокатор.

З. радіонавігації /с. радионавигации/ — засоби радіотехнічні, призначені для визначення місцезнаходження об'єкта на суші, воді, в повітрі і в космосі.

З. радіопротидії (радіоелектронної боротьби) /с. радиопротиводействия (радиоэлектронной борьбы/ — радіотехнічні засоби, призначені для порушення систем управління військами і зброєю противника у воєнний час.

З. радіотелекерування /с. радиотелеуправления/ — засоби радіотехнічні, що забезпечують керува-

ння віддаленими об'єктами.

З. радіотелеметрії /с. радиотелеметрии/ — засоби радіотехнічні, що забезпечують вимірювання і передавання різноманітних фізичних величин віддалених об'єктів.

З. радіотеплолокаційного спостереження /с. радиотеплолокационного наблюдения/ — спеціальні радіоприймальні пристрої — радіометри, в яких здійснюється підсумовування потужностей теплового радіовипромінювання з поверхні об'єкта спостереження, детектування сигналу, підсилення відеосигналу і формування радіотеплолокаційного зображення на індикаторі (екрані). Див. також радіотеплолокація.

З. радіотехнічні /с. радиотехнические/ — технічні пристрої, дія яких базується на використанні електромагнітної енергії радіохвиль для передавання інформації, розвідки, навігації і т.ін. Поділяються: за призначенням — на розвідувальні, розпізнавання, зв'язку, навігації, керування об'єктами і зброєю і т. ін.; за видом засобів — на засоби радіолокації, радіонавігації, радіотелеметрії, радіотелекерування, радіозв'язку, телевізійні, радіопротидії (радіоелектронної боротьби) і т. ін.; за місцем розташування і умовах експлуатації — на стаціонарні і рухомі (бортові, переносні).

З. розвідки /с. разведки/ — технічні пристрої, призначені для добування, оброблення та доведення інформації розвідувальної.

З. руйнування закладних пристроїв /с. разрушения закладных устройств/ — засоби придушення закладних пристроїв, призначені для фізичного руйнування закладок, приєднаних до телефонних ліній і ліній електроживлення. Принцип дії таких засобів ґрунтується на генеруванні і подачі в лінію коротких імпульсів великої амплітуди (1,5–5 кВ), які пробивають низьковольтні деталі (транзистори, конденсатори) закладок і виводять їх з ладу. Це так звані руйнівники "жучків" і випалювачі телефонних закладних пристроїв. Фізичне зруйнування закладних пристроїв здійснюється при від'єднанні від телефонної лінії радіоелектронних засобів (сучасних телефонних апаратів, модемів ПЕОМ, факсів і т. ін.).

З. спостереження /с. наблюдения/ — технічні пристрої для добування інформації дистанційного на основі одержання і аналізу зображення об'єкта спостереження. Поділяються на засоби спостереження в

оптичному діапазоні і засоби спостереження в діапазоні радіочастот.

З. спостереження в діапазоні радіочастот /с. наблюдения в диапазоне радиочастот/ — пристрої (станції, комплекси, системи), призначені для добування інформації про ознаки об'єкта видові спостереження в діапазоні радіочастот електромагнітного випромінювання. Поділяються на засоби радіолокаційного спостереження і засоби радіотеплолокаційного спостереження.

З. спостереження в оптичному діапазоні /с. наблюдения в оптическом диапазоне/ — пристрої (прилади, апарати, станції, комплекси), призначені для добування інформації про видові ознаки об'єкта спостереження в оптичному діапазоні електромагнітного випромінювання (видимого та інфрачервоного). Основу більшості засобів спостереження складають приймачі оптичні, що перетворюють електромагнітне випромінювання оптичного діапазону у видиме зображення об'єкта. Характеристики засобів спостереження в оптичному діапазоні визначаються, насамперед, параметрами оптичної системи і світлоелектричного перетворювача оптичного приймача, а також залежать від способів оброблення електричних сигналів і формування зображення при індикації. До засобів спостереження в оптичному діапазоні відносяться прилади візуально-оптичні, фото — і кіноапарати, комплекси телевізійного спостереження, прилади нічного бачення, тепловізори.

З. спостереження телевізійні /с. наблюдения телевизионные/ — сукупність засобів телевізійної техніки, що створюють так звану систему замкнутого телебачення або відеоконтролю, в якій передача відеосигналів від телевізійних камер до моніторів здійснюється у межах контрольованої зони, як правило, кабелями. Т. з. с. забезпечують: візуальний контроль за зонами і рубежами захисту; спостереження за порушниками рубежів охорони, визначення їхньої кількості, озброєності, дій і намірів; контроль за діями осіб охорони і персоналу організації; запис відеозображення для наступного виявлення і упізнавання зловмисників, контролю і аналізу дій співробітників охорони. В сучасних т. з. с. указані функції доповнюються процедурою автоматичного виявлення рухомого порушника.

З. ураження інформаційних комп'ютерних систем /с. поражения информационных компьютер-

ных систем/ — засоби зброї інформаційної, небезпечні для систем інформаційних комп'ютерних органів державної влади, управління військами і зброєю, фінансами і банками, економікою держави і т.ін. До таких засобів відносять: віруси комп'ютерні; пристрої закладні програмні; засоби придушення інформаційного обміну в телекомунікаційних мережах, його фальсифікації, передавання каналами державного і воєнного управління противника необхідної для себе інформації; засоби, що дозволяють впроваджувати програмні закладні пристрої в державні і корпоративні інформаційні системи і керувати ними на відстані. З. у. і. к. с. можна класифікувати за наступними критеріями: керованість (можливість або неможливість дистанційного або безпосереднього керування); походження (самостійні, спеціально створені або модифіковані програмні засоби); об'єкт впливу (уражають системні або прикладні програми, дезорганізують роботу засобів керування і т. ін.); термін дії (разової або довготривалої дії); спосіб приведення в дію (негайної або відкладеної дії); здатність до самовідтворення; цільове призначення (для ураження об'єктів інформаційного впливу або для перерозподілу даних).

ЗАСТОСУВАННЯ /применение/ [application] — використання будь-чого.

З. інформаційної зброї /п. информационного оружия/ — підбір вхідних даних для системи інформаційної, щоб активізувати в ній певні алгоритми, а у випадку відсутності цих алгоритмів — активізувати алгоритми генерації цих алгоритмів.

ЗАХИСТ /защита/ [protection, security, lock out] — 1) Прагнення запобігти, убезпечити від несприятливих впливів, втручання. 2) Засіб для обмеження доступу чи використання всієї або частини обчислювальної системи; юридичні, організаційні та технічні (в тому числі — криптографічні) заходи запобігання несанкціонованому доступові до апаратури, програм і даних.

З. апаратний /з. аппаратная/ [hardware s., hardware-based s.] — використання апаратних засобів (наприклад, регістрів границь, замків і ключів або апаратури шифрування) для захисту даних в ЕОМ.

З. багаторівневий /з. многоуровневая/ [multilevel s.] — режим захисту при обробленні даних, коли користувачі з різним статусом в частині забезпечення секретності мають обмежені можливості звернення

до бази даних, яка містить інформацію з різними грифами секретності.

З. безпосередній /з. непосредственная/ [physical s.] — заходи, що передбачають фізичний захист ресурсів від навмисних або випадкових загроз.

З. від аварійних ситуацій /з. от аварийных ситуаций/ — створення засобів попередження, контролю і організаційних заходів для виключення несанкціонованого доступу на комплексі засобів автоматизації в умовах відмов його функціонування, відмов системи захисту інформації, систем життєзабезпечення людей на об'єкті розташування і при виникненні стихійного лиха.

З. від вірусів /з. от вирусов/ [virus p.] — сукупність програмних засобів та організаційних заходів, спрямованих на виключення зараження файлів вірусом комп'ютерним. Див. антивірус.

З. від записування /з. от записи/ [write p.] — спосіб захисту інформації на диску та (або) в оперативній пам'яті, який полягає в забороні звернення до файла для виконання операції записування даних. Дозволяється тільки читання даних. Це дає змогу запобігти записуванню нових даних і зберегти наявні дані від руйнування. Реалізується шляхом встановлення ключів захисту або за допомогою мітки зчитування на диску.

З. від копіювання /з. от копирования/ [copy p.] — в комерційному програмному забезпеченні програмно-апаратний засіб для запобігання використання одного екземпляра програми на декількох ЕОМ одночасно. Диск із захищеною програмою містить закодовану інформацію (ключ), що втрачається при копіюванні стандартними засобами. При запуску захищена програма виконується тільки у випадку наявності ключа.

З. від несанкціонованого доступу /з. от несанкционированного доступа/ [p. from unauthorized access] — 1) Попередження або суттєве утруднення доступу несанкціонованого до інформації (програм та даних) шляхом використання апаратних, програмних і методів криптографічних та засобів захисту, а також проведення організаційних заходів. Найбільш розповсюдженим програмним методом захисту є система паролів. 2) Діяльність, спрямована на забезпечення додержання правил розмежування доступу шляхом

створення і підтримки в дієздатному стані системи заходів захисту інформації.

З. від побічного електромагнітного випромінювання і наведень /з. от побочного электромагнитного излучения и наводок/ [p. against compromising emanation] — захист, що здійснюється, якщо рівень сигналу на межі встановленої зони перевищує допустимі для перехоплення випромінювання або наведення значення. Захисні заходи можуть носити різноманітний характер в залежності від складності, вартості і часу, витраченого на їхню реалізацію. Такими заходами можуть бути: доопрацювання апаратури з метою зменшення рівня сигналів, встановлення спеціальних фільтрів, паралельно працюючих апаратних генераторів шуму, спеціальних екранів та інші заходи. Суттєвим заходом є використання в каналах і лініях зв'язку волоконно-оптичних систем передавання, в яких відсутнє електромагнітне випромінювання.

З. від читання /з. от чтения/ [read p.] — заборона звернення до файла для виконання операції читання даних.

З. границь /з. границ/ [boundary p.] — використання обмежувальних регістрів (регістрів захисту пам'яті) для захисту ресурсів комп'ютера.

З. даних (файла) /з. данных (файла)/ [data (file) p.(security)]— 1) Оберігання даних від несанкціонованого, навмисного чи випадкового їхнього розкриття (порушення їхньої конфіденційності), модифікації або знищення. З. д. передбачає проведення організаційних заходів, застосування програмних та технічних методів і засобів, спрямованих на задоволення обмежень, які встановлені для типів і екземплярів даних в системі оброблення даних. 2) Здатність системи керування базою даних контролювати правомочність доступу користувачів до певних порцій даних, що зберігаються, і способи використання цих даних. Механізм з. д. усувають також можливість одночасного оновлення однієї і тієї ж порції даних декількома користувачами, що паралельно звернулися до бази даних. Для перевірки прав програм користувачів на доступ до даних і (або) їхнє оброблення вводяться так звані замки захисту.

З. демаскуючих речовин /з. демаскирующих веществ/ — сукупність заходів, які забезпечують зменшення концентрації речовин демаскуючих до значень, які виключають виявлення зловмисниками їхньої

структури і властивостей шляхом фізичного і хімічного аналізу. Основні напрямки зменшення концентрації демаскуючих речовин — впровадження безвідходних або маловідходних технологій, а також глибоке очищення відходів і викидів. Відходи, очищення від ознак демаскуючих яких неможливе або економічно недоцільне, належать захороненню.

З. державної таємниці /з. государственной тайны/ — сукупність заходів, спрямованих на забезпечення захисту відомостей, що складають державну таємницю, і їхніх носіїв у відповідності до чинного законодавства. З. д. т. потребує створення потужних механізмів, насамперед організаційних структур (див. система захисту державної таємниці.

З. запобіжний /з. предотвращающая/ [disincentive p.] — організаційно-правові заходи захисту від копіювання, що передбачають суворий штраф або загрозу штрафу особі, яка намагається несанкціонованим чином копіювати програму або файл.

З. інтелектуальної власності /з. интеллектуальной собственности/ [p. of intellectual property] — проблема, що постає перед авторами текстів, які без дозволу піддаються мультимедійним перетворенням і розповсюдженню по супермагістралям інформаційним або у формі піратських дискозаписів, коли множина операторських маніпуляцій стирає видимі межі власності інтелектуальної і встановлення на неї юридичних прав ускладнюється.

З. інформації /з. информации/ [infosecurity] — організаційні, програмні та технічні методи і засоби для обмеження доступу до інформації, що обробляється або зберігається. Види інформації, які належить захистити, як правило встановлюються законодавством держави. Це можуть бути: відомості, що відносяться до державної таємниці (інформація в галузі воєнної, зовнішньополітичної, економічної, розвідувальної, контррозвідувальної і оперативно-розшукової діяльності), розповсюдження яких може нанести шкоду безпеці держави; відомості, що відносяться до службової і комерційної таємниці (інформація, що має сьогочасну або потенційну цінність в силу того, що вона невідома третім особам, якщо до неї нема законного доступу на законній (санкціонованій) основі і власник такої інформації вживає заходи до охорони її конфіденцій-

ності); відомості, що мають статус персональних даних (інформація про громадян, що входить до складу державних інформаційних ресурсів, інформаційних ресурсів органів місцевого самоуправління, а також та, що одержується і збирається недержавними організаціями і т. ін.).

З. інформації в автоматизованій системі /з. в автоматизированной системе/ [information p., information s., computer system s.] — діяльність, яка спрямована на забезпечення безпеки інформації, що оброблюється в системі автоматизованій, та автоматизованої системи в цілому, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків унаслідок реалізації загроз.

З. інформації інженерно-технічний /з. информации инженерно-техническая/ — те ж, що захист інформації технічний.

З. інформації технічний /з. информации техническая/ [technical p. of information] — одна з основних компонент комплексу заходів захисту інформації, що складає державну, службову, комерційну або особисту таємницю. З. і. т. включає комплекс нормативно-правових, організаційних і технічних заходів забезпечення безпеки інформації технічними засобами. Він виконує наступні завдання: попередження проникнення зловмисника до джерел інформації з метою її знищення, викрадення або зміни (модифікації); захист носіїв інформації від знищення в результаті впливу стихійних сил і насамперед пожежі і води (піни) при її гасінні; попередження витоку інформації різноманітними технічними каналами.

З. інформації, що міститься у відходах /з. информации, содержащейся в отходах/ — сукупність заходів, що включають способи захисту інформації на паперових (машинних) носіях і інформації, яка міститься у відходах і бракові наукової і виробничої діяльності організації. Для реалізації захисту пропонуються наступні заходи: облік окремих аркушів, використаного копіювального паперу, макетів, бракованих вузлів і деталей; збирання чернеток документів і різноманітних записів на окремих не врахованих аркушах в спеціальні опечатані ящики; знищення паперових і стирання (знищення) машинних носіїв; розбирання макетів

і блоків, руйнування механічних деталей.

З. інформаційний /з. информационная/ [infosecurity] — 1) Захист інтересів життєво важливих фізичних та юридичних осіб від загроз інформаційних. Він досягається шляхом внесення в порядку законодавчої ініціативи законопроектів, здійснення судового захисту, проведення оперативних заходів силами і засобами інформаційної безпеки. 2) Сукупність заходів захисту від протидії інформаційної противника, які включають дії з деблокування інформації, необхідної для вирішення завдань управління, і блокування дезінформації, що розповсюджується і впроваджується в систему управління. З. і. досягається проведенням контрольної розвідки, перевіркою інформації, захистом від вогневого ураження (захоплення) елементів систем інформаційних, а також захистом радіоелектронним. З. і. підвищує ефективність забезпечення інформаційного в умовах інформаційної протидії противника.

З. кодів паролів /з. кодов паролей/ [password p.] — сукупність застережних заходів, спрямованих на те, щоб дійсні коди паролів були недоступні стороннім особам. Рекомендуються наступні основні заходи обережності для захисту кодів паролів: паролі ніколи не слід зберігати в обчислювальній системі в явному вигляді, вони завжди повинні бути зашифровані; паролі не слід друкувати (відображати) в явному вигляді на терміналі користувача (за виключенням термінала оператора служби безпеки інформації, який повинен знаходитися в ізольованому приміщенні); пароль необхідно міняти як можна частіше і по випадковому закону (чим більший період часу використовується один і той же пароль, тим більша ймовірність його розкривання); система ніколи не повинна виробляти новий пароль в кінці сеансу зв'язку навіть у зашифрованому вигляді, так як це може дозволити порушникові легко ним скористатися. Для закриття кодів паролів можна використати метод шифрування необоротного і більш складний метод "необоротного безладного складення", коли паролі за допомогою спеціального полінома перетворюються в зашифрований пароль. Найбільш ефективним захистом пароля від несанкціонованого доступу вважається розділення його на дві частини: одну — для запам'ятовування користувачем, іншу — для зберігання на спеціальному носії. На випадок утрати або викрадення носія пароля у користувача буде час заявити про це у службу безпеки

інформації, а ця служба може встигнути змінити пароль.

З. комерційної таємниці /з. коммерческой тайны/ — запобігання витоку, викраденню, втрати, викривлення, підробки інформації, що складає таємницю комерційну.

З. комп'ютерних систем фізичний /з. компьютерных систем физическая/ — захист, що здійснюється шляхом застосування пристроїв, які би виключали доступ до інформації в системі комп'ютерній без порушення фізичної цілісності комп'ютерів. В ряді випадків принциповим є застосування заходів, що виключають негласний (в тому числі і регулярний) доступ до комп'ютера з метою копіювання або модифікації інформації. Засобами з. к. с. ф. можуть бути: опечатування системного блока та інших елементів комп'ютерних систем спеціальними пломбами або печаткою керівника служби безпеки; використання спеціальних уставок в "кишеню" дисковода, обладнаних замком з фіксацією на ключ; застосування спеціальних замків, що блокують клавіатуру комп'ютера; організація зберігання магнітних і оптичних носіїв в сейфах або у спеціальних дискетницях, що закриваються на замок.

З. криптографічний /з. криптографическая/ [cryptographical s.] — вид захисту, що реалізується за допомогою перетворень (перетворень криптографічних) інформації з використанням спеціальних параметрів (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

З. мовної інформації /з. речевой информации/ [voice s.] — комплекс заходів, спрямованих на протидію зловмисним спробам несанкціонованого доступу до мовної інформації. Див. приховування мовної інформації інформаційне.

З. об'єктів /з. объектов/ [object p.] — засоби захисту об'єктів типу сейфів, файлів і т. ін.

З. обчислювальної мережі /з. вычислительной сети/ [network s.] — виключення або суттєве утруднення несанкціонованого доступу користувачів до елементів та ресурсів обчислювальної мережі шляхом використання апаратних, програмних і методів криптографічних та засобів захисту, а також проведення

організаційних заходів.

З. пам'яті /з. памяти/ [memory p.] — механізм контролю доступу до якої-небудь області пам'яті з урахуванням розроблених звернень. Дозволений режим звернення може бути різним для різних процесів. При розмітці області оперативної пам'яті можуть використовуватися граничні регістри; конкретні зафіксовані ділянки пам'яті можуть контролюватися за допомогою замків; доступ до конкретних слів може контролюватися за допомогою тегів (ознак даних). З. п. є одним із багатьох способів управління доступом або використання пам'яті і дозволяє запобігти некоректному втручанню користувача, забезпечити захист системи або виконує відразу обидві функції.

З. паролем (за допомогою пароля) /з. паролем (с помощью пароля)/ [password p.] — спосіб захисту даних, що полягає у перевірці відповідності наданого суб'єктом доступу пароля еталонному паролю для надання доступу до об'єкта доступу. Являє собою один з видів простої автентифікації.

З. по умовчанню /з. по умолчанию/ — призначення повноважень доступу користувачів за принципом: "усе, що не дозволено, те заборонено". Тобто всі ресурси, доступ до яких явно не дозволений користувачу, вважаються недоступними.

З. прав користувачів /з. прав пользователей/ [p. of consumers] — сукупність правил, методів і засобів, спрямованих на забезпечення безперешкодного та своєчасного доступу користувачів до програм і даних та захист їхньої інформації від використання іншими особами.

З. програми /з. программы/ [software lock] — сукупність умов, що запобігають запуску програми на виконання.

З. радіоелектронний /защита радиоэлектронная/ [radio electronic p.] — сукупність заходів забезпечення стійкої роботи засобів управління і розвідки в умовах ведення противником боротьби радіоелектронної, застосування розвідувально-ударних комплексів, самонавідної зброї та усунення взаємного впливу радіоелектронних засобів.

З. резервуванням /з. резервированием/ — метод відновлення даних, які зберігаються в зовнішній

пам'яті, що полягає у копіюванні на додатковий носій тільки тих файлів, котрі були створені пізніше визначеного строку.

З. системи /з. системы/ [system s.] — сукупність заходів, що вживаються для виключення несанкціонованого доступу до програм і даних системи або випадкового втручання в її роботу.

ЗАХИЩЕНІСТЬ /защищенность/ [protectability, immunity, proofness] — здатність до оборони, охорони когось, чогось від нападу, замаху, удару, ворожих дій і т. ін.

З. автоматизованої системи /з. автоматизированной системы/ — здатність системи автоматизованої протистояти доступу несанкціонованому до інформації, а також її випадковому спотворенню або руйнуванню. З. а. с. є змінною величиною, залежить вид багатьох факторів і повинна підтримуватися на усіх етапах життєвого циклу системи. Для забезпечення захищеності використовується велика кількість методів, які умовно поділяють на три основні групи: керування доступом до інформації; резервування інформації та інших ресурсів; приховування (в тому числі криптографічними та стеганографічними методами).

З. інформації /з. информации/ — забезпечення цілісності, конфіденційності і доступності інформації. З. і. досягається забезпеченням захисту інформації від несанкціонованої змінювання, від несанкціонованого одержання, від несанкціонованого утримування.

ЗАХОДИ /мероприятия/ [measure] — сукупність дій, засобів для досягнення, здійснення чогось.

З. забезпечення безпеки /м. обеспечения безопасности/ [safeguards] — послуги, функції, механізми, правила і процедури, призначені для забезпечення захисту інформації.

З. захисту інформації законодавчі /м. защиты информации законодательные/ [legal] — сукупність заходів, спрямованих на виконання існуючих в державі або введення нових законів, положень, постанов і інструкцій, що регулюють юридичну відповідальність посадових осіб-користувачів і обслуговуючого персоналу за витік, втрату або модифікацію довіреної їм інформації, що належить захисту, в тому числі і за спроби виконати аналогічні дії за межами своїх повноважень, а також відповідальності сторонніх осіб за спробу навмисного доступу несанкціонованого до апаратури і інформації. Мета законодавчих заходів —

попередження і стримування потенційних порушників. У Кримінальних кодексах багатьох країн існують розділи, присвячені злочинам комп'ютерним.

З. захисту інформації організаційні /м. защиты информации организационные/ [administrative security] — 1) Сукупність адміністративних і організаційно-технічних заходів захисту інформації при створенні і експлуатації систем оброблення інформації. При плануванні заходів автоматизованих чітко вказується мета заходу, розподіл відповідальності і перелік заходів захисту. Здійснюються на всіх етапах існування системи: проектування, розробки, виготовлення і експлуатації. Розрізняють заходи захисту інформації організаційні в процесі створення системи, в процесі підготовки системи до експлуатації, у процесі експлуатації системи, по закінченню експлуатації системи. 2) Рекомендації Головного конструктора системи з організації захисту інформації, які включаються в інструкцію з експлуатації, а також адміністративні заходи, які включаються в посадові інструкції і виконуються на місці споживачем системи.

З. захисту інформації організаційні в процесі експлуатації системи /м. защиты информации организационные в процессе эксплуатации системы/ — система заходів захисту інформації організаційних, здійснюваних в процесі експлуатації системи. У процесі експлуатації системи служба безпеки інформації здійснює централізований контроль доступу до інформації за допомогою термінала і організаційними засобами; виконуються функції, що забезпечують функціонування засобів захисту в цілому і розмежування доступу до інформації: введення списку імен користувачів, терміналів, процесів, допущених до інформації в комплексі засобів автоматизації; вибір і введення носіїв кодів паролів; уведення призначених повноважень користувачів, терміналів, процесів; збирання сигналів незбігу кодів паролів і порушення повноважень; ведення журналу доступу до інформації; збір сигналів розкривання апаратури; взаємодія з службою функціонального контролю КЗА; контроль функціонування систем упізнавання і розмежування доступу до інформації та контролю розкривання апаратури; контроль доступу в приміщення з апаратурою КЗА; контроль і забезпечення можливості шифрування інформації; контроль реєстрації і обліку носіїв інформації і документів; контроль стирання і знищення залишків секретної інформації; ведення статистики і

прогнозування спроб несанкціонованого доступу. Для виконання перелічених функцій використовуються спеціальні апаратні і програмні засоби, що входять в склад технічних засобів КЗА, а організаційні заходи включаються в окрему інструкцію по експлуатації засобів захисту КЗА.

З. захисту інформації організаційні в процесі підготовки системи до експлуатації /м. защиты информации организационные в процессе подготовки системы к эксплуатации/ — сукупність заходів захисту інформації організаційних, що здійснюються при підготовці системи до експлуатації. Можна виділити організаційні заходи до розгортання засобів системи, організаційно-кадрові заходи і організаційні заходи, що здійснюються після розгортання апаратури.

З. захисту інформації організаційні в процесі створення системи /организационные м. защиты информации в процессе создания системы/ — сукупність заходів захисту інформації організаційних, що здійснюються на етапах проектування, розробки, виготовлення і випробування системи. Розроблюються і впроваджуються у відповідності з вимогами технічного завдання організацією, що здійснює проектування. До організаційних заходів в процесі створення системи відносяться: введення на необхідних ділянках проведення робіт з режимом секретності; розробка посадових інструкцій по забезпеченню режиму секретності у відповідності до діючих в державі інструкцій і положень; при необхідності виділення окремих приміщень з охоронною сигналізацією і системою перепусток; розмежування завдань по виконавцях і випуску документації; присвоєння грифа секретності матеріалам, документації, апаратурі і зберігання їх під охороною в окремих приміщеннях з обліком і контролем доступу виконавців; постійний контроль за дотримуванням виконавцями режиму і відповідних інструкцій; визначення і розподіл відповідальних осіб за витік інформації; інші заходи, що встановлюються головним конструктором при створення конкретного пристрою (системи).

З. захисту інформації організаційні до розгортання апаратури /м. защиты информации организационные до разворачивания аппаратуры/ — сукупність заходів по захисту інформації в процесі підготовки системи до експлуатації. Для їхньої реалізації необхідно: при виділенні території, будівель і приміщень позначити контрольовану зону навкруг розташування комплексу засобів автоматизації (КЗА); установити і

обладнати охоронну сигналізацію по межах охоронної зони; перевірити схему розташування і місця установки апаратури КЗА; перевірити стан системи життєзабезпечення людей, умови функціонування апаратури і зберігання документації.

З. захисту інформації організаційні після закінчення експлуатації системи /м. защиты информации организационные после окончания эксплуатации системы/ — сукупність заходів, здійснюваних після заміни системи оброблення інформації на більш сучасну. Вони обумовлюють проведення ревізії залишків інформації, що зберігалася в КЗА. Цінна інформація переписується на більш сучасні носії при забезпеченні відповідного режиму обмеженого доступу, а рештки інформації знищуються.

З. захисту інформації організаційно-кадрові в процесі підготовки системи до експлуатації /м. защиты информации организационно-кадровые в процессе подготовки системы к эксплуатации/ — заходи, спрямовані на підбір, навчання і розстановку кадрів для експлуатації системи. Проводяться паралельно з заходами захисту інформації організаційними до розгортання апаратури. Для їхньої реалізації необхідно провести: перебудову структури організації-споживача у відповідності до потреб системи, що впроваджується; підібрати кадри для технічного і оперативного обслуговування КЗА; при необхідності підібрати спеціальні кадри для роботи по захисту інформації в системі і створити централізовану службу безпеки інформації при керівництві організації; провести навчання кадрів; організувати розподіл функціональних обов'язків і відповідальності посадових осіб; встановити повноваження посадових осіб відносно доступу до технічних засобів і інформації; розробити посадові інструкції по виконанню функціональних обов'язків технічного, оперативного складу посадових осіб, включаючи службу безпеки інформації.

З. контролю захисту інформації технічні /м. контроля защиты информации технические/ — заходи контролю технічного захисту інформації, що здійснюються з використанням технічних засобів радіо- і електровимірювань, фізичного і хімічного аналізу і забезпечують перевірку: напруженості полів з інформацією на межах контрольованих зон; рівні небезпечних сигналів і завад в проводах і екранах кабелів, що виходять за межі контрольованої зони; ступені зашумлення генераторами завад структурних звуків в

огорожах; концентрації демаскуючих речовин у відходах виробництва.

З. контролю технічного захисту інформації організаційні /м. контроля технической защиты информации организационные/ — заходи контролю технічного захисту інформації, що включають: перевірку виконання співробітниками вимог керівних документів по захисту інформації; перевірку працездатності засобів охорони і захисту інформації від спостереження, підслухування, перехоплення і витоку інформації по матеріально-речовому каналові (наявності занавісок, штор, жалюзі на вікнах, чохлів на виробах, що розроблюються, стан звукоізоляції, екранів, засобів придушення небезпечних сигналів і зашумлення, ємностей для збирання відходів з демаскуючими речовинами і т. ін.); контроль за виконанням інструкцій по захисту інформації про продукцію, що розроблюється; оцінка ефективності способів і засобів захисту інформації.

З. психологічної війни /м. психологической войны/ — короткочасні цілеспрямовані дії окремих підрозділів або окремих фахівців, які відрізняються обмеженим характером і здійснюються в обмежених (локальних) масштабах. З. п. в. (як складова або самостійна частина операцій психологічних) проводять для впровадження у свідомість населення й військ противника конкретних поглядів, переконань або лозунгів, мотивів недовіри або невдоволення діями свого політичного й воєнного керівництва, усвідомлення свого незавидного положення, загрози життю й благополуччю родичів, і для введення їх в оману, обманювання, схилення до співробітництва. З. п. в. поділяють на заходи зниження морального духу населення і військовослужбовців противника, заходи підривання боєздатності підрозділів і частин противника, заходи схилення противника до переходу на іншу сторону.

З. технічного захисту інформації /м. технической защиты информации/ [technical m. facilities] — заходи, спрямовані на забезпечення безпеки інформації за допомогою технічних засобів. Включають два етапи: побудова або модернізація системи захисту; підтримування захисту інформації на необхідному рівні. З. т. з. і. поділяються на заходи технічного захисту інформації організаційні та заходи захисту інформації технічні.

З. технічного захисту інформації організаційні /м. технической защиты информации органи-

зационные/ — заходи, спрямовані на ефективне використання технічних засобів регламентації доступу і керування доступом до інформації, що потребує захисту, а також на встановлення порядку і режимів роботи технічних засобів захисту.

ЗАШИФРОВУВАННЯ /зашифровывание/ [encipherement, encryption] — процес перетворення тексту відкритого до виду, незрозумілого несанкціонованому користувачеві (в шифртекст).

ЗБЕРІГАННЯ /хранение/ [storage] — процес тримання чогось в певних умовах, запобігання псуванню, руйнуванню.

З. інформації /х. информации/ [information s.] — один з основних видів роботи інформаційної. Має велике значення для багатократного використання інформації, передавання накопичуваного знання іншим людям (поколінням). Інформатика вносить в проблеми з. і. способи перенесення інформації на носії машинні, методи забезпечення як її збереження, так і доступності до неї.

ЗБИРАННЯ /сбор/ [collection, acquisition] — 1) Вибирання чогось з різних місць, від різних осіб і т. ін. 2) Поступове приєднання, складання чогось одного до одного, частину до частини. 3) Складання чогось докупи, в одне місце.

З. даних /с. данных/ [data c.] — процес ідентифікації і одержання даних від різних джерел, групування одержаних даних і подання їх у формі, необхідній для введення в ЕОМ.

З. знань /с. знаний/ [knowledge a.] — одержання інформації про частину предметну від фахівців-експертів і подання її в формі, необхідній для введення в ЕОМ.

З. сміття /с. мусора/ — загроза, що полягає в захопленні й аналізі користувачем або процесом спільно використовуваних об'єктів, звільнених іншим користувачем чи процесом, з метою одержання інформації, що в них знаходиться.

ЗБІЙ /сбой/ [fault] — самоусувна відмова або одноразова відмова, яку незначним втручанням усуває оператор.

ЗБРОЯ /оружие/ [arm, weapon] — пристрої і засоби, призначені для ураження противника в боротьбі

збройній. Складається із засобів ураження і засобів їхньої доставки до цілі; більш складна з. включає також прилади і пристрої керування і наведення.

З. інформаційна /о. информационное/ — 1) Широкий клас засобів і способів впливу інформаційного на противника від дезінформації і пропаганди до засобів боротьби радіоелектронної. 2) Сукупність спеціально організованої інформації та технологій інформаційних, яка дозволяє цілеспрямовано змінювати (знищувати, спотворювати), копіювати, блокувати інформацію, долати системи захисту, обмежувати допуск законних користувачів, здійснювати дезінформацію, порушувати функціонування носіїв інформації, дезорганізовувати роботу технічних засобів, систем комп'ютерних та мереж інформаційно-обчислювальних, що застосовується в ході боротьби інформаційної (війни) для досягнення поставлених цілей. За метою використання з. і. поділяється на зброю інформаційну атаки та зброю інформаційну забезпечення. Успішне застосування інформаційної зброї забезпечення дозволяє здійснювати впливи деструктивні на інформацію, що зберігається, обробляється й передається в мережах обміну інформацією, з використанням інформаційної зброї атаки. За способом реалізації і. з. поділяють на три великих класи: зброя інформаційна алгоритмічна (математична); зброя інформаційна програмна; зброя інформаційна апаратна. З. і., що відноситься до різних класів, може застосовуватися спільно, а також деякі види і. з. можуть мати риси декількох класів. 3) Алгоритм, що реалізує процес керування системою через дані, що поступають в систему і оброблюються нею та та дозволяють здійснювати цілеспрямоване керування одною системою інформаційною в інтересах іншої.

З. інформаційна алгоритмічна (математична) /о. информационное алгоритмическое (математическое)/ — вид зброї інформаційної до якого, звичайно, відносять: алгоритми, що використовують сполучення санкціонованих дій для здійснення доступу несанкціонованого до ресурсів інформаційних; алгоритми застосування санкціонованого (легального) програмного забезпечення і програмні засоби несанкціонованого доступу для здійснення незаконного доступу до інформаційних ресурсів.

З. інформаційна апаратна /апаратное информационное о./ — засоби апаратні, призначені для вико-

нання функцій зброї інформаційної. Прикладом з. і .а. можуть бути закладки апаратні, які впроваджуються в ПЕОМ, що готуються на експорт та їхнє периферійне обладнання. Апаратні закладки маскуються під звичайні пристрої мікроелектроніки і застосовуються для збирання, оброблення й передавання конфіденційної інформації. Див. також троянський кінь в електронних колах.

З. інформаційна атаки /о. информационное атаки/ — зброя інформаційна, за допомогою якої здійснюється вплив на інформацію, що зберігається, оброблюється і передається в мережах інформаційно-обчислювальних і (або) порушуються технології інформаційні, що застосовуються в ІОМ. У складі з. і. а. виділяють чотири основних види засобів впливів інформаційних: засоби порушення конфіденційності інформації; засоби порушення цілісності інформації; засоби порушення доступності інформації; засоби впливу психологічного на абонентів ІОМ. Застосування з. і. а. спрямоване на зрив виконання ІОМ цільових завдань.

З. інформаційна забезпечення /о. информационное обеспечения/ — зброя інформаційна, за допомогою якої здійснюється вплив на засоби захисту інформації об'єкта атаки, наприклад, систему інформаційно-обчислювальну. До складу з. і. з. входять засоби розвідки комп'ютерної та засоби подолання системи захисту (інформаційно-обчислювальної системи).

З. інформаційна програмна /программное информационное о./ — програми з потенційно небезпечними наслідками своєї роботи для ресурсів інформаційних мережі обміну інформацією.

З. інформаційна стратегічна /о. информационное стратегическое/ — засоби і способи впливу інформаційного на інформаційно-технологічні системи, обслуговуючі інфраструктури — транспорт, зв'язок управління державними органами, військами і т. ін.

З. інформаційної атаки /о. информационной атаки/ — віруси комп'ютерні, здатні розмножуватися, упровадитися в програми, передаватися лініями зв'язку, мережами передавання даних, виводити з ладу системи управління і т. ін.; бомби логічні — програмні закладні пристрої, які заздалегідь упроваджують в інформаційно-керуючі центри, щоб за сигналом або у встановлений час привести їх у дію; засоби придушення інформаційного обміну в телекомунікаційних мережах, фальсифікації інформації в каналах управління;

засоби нейтралізації тестових програм; різного роду помилки, які свідомо вводяться вивідачами в забезпечення програмне об'єкта (люки). об'єкта (люки).

З. психотронна /о. психотронное/ — засоби впливу психотронного, створені на основі можливостей і знань психотроніки при вирішенні ПСІ-проблеми. Відомі факти робіт з створення генераторів високочастотного і низькочастотного кодування мозку, біологічних установок, з використання хімічних і біологічних засобів для стимулювання певних психологічних реакцій.

ЗВ'ЯЗКОВИЙ /связник/ [messenger] — посередник (третя людина), діяльність якої спрямована на приховування контактів між двома іншими людьми, як правило, між агентом розвідки і його куратором, яким не слід зустрічатися, так як хтось один з них може знаходитися під спостереженням.

ЗВ'ЯЗОК /связь/ [binding, communication, link] — 1) Передавання й приймання інформації за допомогою різноманітних технічних засобів. Див. також комунікація. 2) Установа, установи, що забезпечують технічні засоби спілкування на відстані.

З. гідроакустичний /с. гидроакустическая/ [hydroacoustic c.] — зв'язок, який здійснюється у водному середовищі передаванням модульованих хвиль звукових чи ультразвукових. Застосовується для двостороннього зв'язку між кораблями (суднами) або пливучими і береговими об'єктами, між надводними суднами і глибоководними апаратами, водолазами, аквалангістами і т.ін. Дальність з. г. залежить від випромінюваної потужності передавача, чутливості приймальних пристроїв, швидкості корабля (судна) і гідрологічних умов в районі зв'язку.

З. комунікативний /с. коммуникативная/ [communications l.] — зв'язок між комп'ютерами для передавання даних.

З. космічний /с. космическая/ [space radiocommunication] — радіозв'язок, у якого як середовище розповсюдження радіохвиль використовується космічний простір і який здійснюється: між віддаленими наземними об'єктами за допомогою космічних активних і пасивних ретрансляторів; між наземними пунктами

і космічними літальними апаратами; між космічними літальними апаратами.

З. оптоелектронний /с. оптоэлектронная/ [optical c.] — електрозв'язок, який здійснюється передаванням хвиль електромагнітних оптичного діапазону волоконно-оптичним кабелем.

З. паразитний /с. паразитная/ [spurious c., stray c.] — передавання сигналу з одного елемента радіопристрою на інший, не передбачена його схемою та конструкцією і викликана впливом певних фізичних факторів. розрізняють три види з. п.: гальванічний, індуктивний і ємнісний.

З. паразитний гальванічний /с. паразитная гальваническая/ [stray galvanic c.] — зв'язок паразитний через опір. Виникає, коли одними і тими ж колами протікають струми від різних джерел. В цьому випадку відбувається проникнення сигналів в непризначені для них елементи схеми. Сигнали, що несуть конфіденційну інформації, за рахунок з. п. г. можуть проникати в кола, що мають вихід за межі контрольованої зони. Це створює умови для витоку інформації. До таких ланцюгів відносяться, насамперед, кола живлення і заземлення.

З. паразитний ємнісний /с. паразитная емкостная/ [stray capacitive c.] — (зв'язок паразитний з одного елемента радіопристрою на інший, не передбачений його схемою та конструкцією і викликаний впливом змінного електричного поля даного елемента (ланцюга) на інший. Створює загрозу безпеці інформації у випадку, коли елемент (коло), з яким здійснюється паразитний зв'язок, має вихід сигналів за межі контрольованої зони (див. наведення паразитне).

З. паразитний індуктивний /с. паразитная индуктивная/ [stray inductive c.] — зв'язок паразитний з одного елемента радіопристрою на інший, не передбачений його схемою та конструкцією і викликаний впливом електромагнітного поля. Створює загрозу безпеці інформації у випадку, коли елемент (коло), з яким здійснюється паразитний зв'язок, має вихід сигналів за межі контрольованої зони (див. паразитне наведення).

З. пейджинговий /с. пейджинговая/ [paging c.] — система служби радіозв'язку рухомої для персонального радіовиклику і передавання текстових або голосових повідомлень мобільним абонентам. У біль-

шості стандартів п. з. реалізований принцип одностороннього зв'язку — від центральної станції до пейджера абонента. В деяких системах передбачена послуга двостороннього зв'язку. Виклик абонента і передавання повідомлень може здійснюватися або через оператора п. з., або за допомогою телефонного апарата з тоновим набором номера, або через мережу Інтернет. Послуги з. п. можуть надаватися в деяких системах зв'язку стільникового і супутникового.

З. проводовий /с. проводная/ [wire/line c.] — електрозв'язок, який здійснюється передаванням електричних сигналів металевими проводами.

З. радіорелейний /с. радиорелейная/ — радіозв'язок, що ґрунтується на ретрансляції радіосигналів на хвилях дециметрових і більш коротких.

З. стільниковий /с. сотовая/ [cellular c.] — система рухомої служби дуплексного телефонного радіозв'язку загального користування. Зв'язок з рухомими абонентами організується з використанням декількох базових радіостанцій, розподілених по зоні обслуговування і сполучених між собою лініями зв'язку. Зона обслуговування поділяється на ділянки (стільники), в центрі яких установлюється антена і обладнання ретранслятора-комутатора.

З. супутниковий /с. спутниковая/ [satellite c.] — космічний радіозв'язок між наземними станціями, що здійснюється завдяки ретрансляції радіосигналів через один або декілька супутників Землі.

З. телеграфний /с. телеграфная/ [telegraphy] — вид електрозв'язку документального, який забезпечує передавання літеро-цифрового тексту.

З. телефонний /с. телефонная/ [telephony, voice telephony] — вид електрозв'язку, який забезпечує передавання сигналів, що відображають природну мову, на відстань у встановленій смузі частот між абонентами та (або) операторами.

З. факсимільний /с. факсимильная/ [document facsimile telegraphy, facsimile telegraphy] — вид електрозв'язку документального, який забезпечує передавання на відстань усіх форм графічних, рукописних чи друкованих матеріалів.

ЗВУКОМАСКУВАННЯ /звукомаскировка/ [acoustic camouflage] — комплекс заходів, спрямованих на зниження рівня демаскуючих шумів, а також створення шумів, що утруднюють противникові ведення розвідки. Проводиться для приховування від противника звукової перегрупування, заміни та маневру військ (сил), їхньої підготовки до бойових дій.

ЗДАТНІСТЬ /способность/ [capability] — властивість робити щось, поводити себе певним чином.

З. відбивна цілі /с. цели отражающая/ — властивість цілі (об'єкта) відбивати (розсіювати) енергію хвиль електромагнітних. Кількісно характеризується ефективною поверхнею розсіювання. Для понижения в. з. ц. на поверхню наносяться спеціальні покриття, що поглинають енергію хвиль (див. матеріали радіопоглинаючі).

З. пропускна каналу зв'язку /с. канала связи пропускная/ — кількість інформації, що передається каналом зв'язку за одиницю часу з певною якістю. В теорії зв'язку з. к. з. п. в бодах (бітах за секунду) оцінюється за формулою:

$$C = \triangle F \log_2(1 + P_c/P_n),$$

де $\triangle F$ — ширина смуги пропускання каналу зв'язку; P_c і P_n — відповідно потужність сигналу і завади (у вигляді білого шуму) в смузі пропускання каналу. Тобто, з. к. п. з. є інтегральною характеристикою, що враховує як ширину смуг частот сигналу, яку пропускає канал, так і його енергетику. Із зменшенням відношення потужностей сигналу і завади збільшується кількість помилок в прийнятому повідомленні і зменшується кількість переданої інформації.

З. роздільна об'єктива /с. разрешающая объектива/ — здатність об'єктива передавати дрібні деталі зображення. Виражається максимальною кількістю штрихів і проміжків між ними на 1 мм поля зображення в його центрі і по краях. Найбільш високу роздільну здатність мають об'єктиви для мікрофотографування в мікроелектроніці. Вона сягає 280–440 ліній на мм в центрі і 260–400 ліній на мм по краях поля зображення.

З. роздільна фотографічного матеріалу /с. разрешающая фотографического материала/ — здатність матеріалу фотографічного передавати дрібні деталі зображення. Оцінюється таким само чином, як

роздільна здатність об'єктива. Визначається структурними властивостями матеріалу. Зерниста структура фотографічної емульсії викликає розсіювання світла в шарі при експонуванні і обмежує можливості відображення дрібних деталей і різкість зображення. Чим вища чутливість фотографічного матеріалу, тим більша зернистість емульсії. Роздільна здатність фотоплівок для аерофотозйомки сягає 500 і більше лін/мм, плівки широкого застосування мають розділення 100 лін/мм і менше.

ЗЕРНО /зерно/ [seed] — те ж, що паросток.

ЗЙОМКА /съемка/ [shooting] — фіксація фото-, кіно-, теле- або будь-якого іншого зображення.

З. в інфрачервоних променях /с. в инфракрасных лучах/ — фотографування з використанням випромінювання в інфрачервоній частині спектра. Найбільш просто здійснюється за допомогою звичайного апарата фотографічного на матеріал фотографічний, чутливий до інфрачервоного випромінювання. Внаслідок меншого розсіювання інфрачервоних променів в атмосфері порівняно з видимими променями, така зйомка дозволяє одержувати чіткі зображення віддалених об'єктів, а також зображення об'єктів, які неможливо одержати при фотографуванні з використанням променів в інших частинах спектра.

З. космічна /с. космическая/ — зйомка Землі, небесних тіл, туманностей і т. ін., що виконується приладами, що знаходяться поза межами земної атмосфери (на відміну від аерофотозйомки). Використовується кінофотоапаратура, телевізійна апаратура, апаратура спектрометрії та інші методи.

З. радіолокаційна /с. радиолокационная/ — одержання зображень місцевості за допомогою радіолокаційної апаратури, встановленої на літальних апаратах. Може проводитися у складних метеорологічних умовах і в будь-який час доби, а також для вивчення об'єктів, закритих снігом, рослинністю, рихлими відкладеннями і т.ін. Дає додаткову інформацію, яка відсутня на фотографіях.

ЗЛОВМИСНИК /злоумышленник/ [abuser, Bad-Guy, badguy, intruder] — 1) Особа або організація, що займаються добуванням інформації в інтересах розвідки державної і комерційної, кримінальних елементів, непорядних співробітників або просто психічно хворих людей. 2) Стосовно обчислювальних мереж — особа або організація, що зацікавлена в одержанні несанкціонованого доступу до програм або даних, які

здійснюють спробу такого доступу або здійснили її.

ЗЛОЧИН /преступление/ [crime] — 1) Суспільно небезпечна дія, що чинить зло людям; злочинство, злодіяння. 2) Неприпустимий, ганебний вчинок.

З. комп'ютерний /п. компьютерное/ [computer c.] — передбачені кримінальним законом суспільно небезпечні дії, що здійснюються з використанням засобів електронно-обчислювальної (комп'ютерної) техніки. До суспільно небезпечних дій відносять: неправомірний доступ до комп'ютерної інформації, що охороняється законом (інформації на машинному носії, в ЕОМ, в системі ЕОМ або їхньої мережі), якщо ці дії спричинили знищення, блокування, модифікацію або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ або їхньої мережі; створення програм для ЕОМ або внесення змін в існуючі програми, якщо це явно привело до несанкціонованого знищення, блокування, модифікації або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ або їхні мережі, а також використання або розповсюдження таких програм або машинних носіїв з такими програмами; порушення правил експлуатації ЕОМ, системи ЕОМ або їхньої мережі особою, що має доступ до ЕОМ, системи ЕОМ або їхньої мережі, що викликало знищення, блокування або модифікацію інформації ЕОМ, що охороняється. Способи здійснення к. з. можна розділити на п'ять основних груп: вилучення засобів комп'ютерної техніки (ЗКТ); перехоплення інформації; доступ несанкціонований до ЗКТ; маніпулювання даними і управляючими командами; комплексні методи.

ЗЛОЧИНЕЦЬ /преступник/ [criminal] — особа, що здійснила злочин; правопорушник, беззаконник.

З. комп'ютерний /п. компьютерный/ [computer intruder] — особа, що здійснила злочин комп'ютерний.

ЗМІННА /переменная/ [variable] — змінна величина.

З. Буля /п. Буля/ [boolean v.] — змінна, яка приймає значення $0(FALSE)$ або $1(TRUE)$. Для кодування булевої змінної достатньо одного біта інформації.

ЗНАК /знак/ [mark] — матеріальний предмет (явище, подія), що виступає як представник деякого іншого предмета, властивості або відносин та використовується для придбання, зберігання, перероблення та

передавання повідомлень (інформації, знань).

З. цифровий водяний /з. цифровой водяной/ [digital watermark] — спеціальна позначка, яка за допомогою методів стеганографії комп'ютерної непомітно додається до інформації (зображення, музичного твору і т.ін.) з метою контролю авторських прав цієї інформації.

ЗНАННЯ /знание/ [knowledge] — 1) Продукт діяльності людей, що являє собою ідеальне відтворення в мовній формі подій і закономірних зв'язків об'єктивного світу. З. є прямою силою, що дозволяє людині фактично володарювати над світом. Межі цієї влади визначаються рівнем знань. Людина, у свою чергу, обумовлює точність і межі інформації, що міститься в знаннях. Мірою сили з. є кількість інформації, що міститься в знаннях. З цього погляду з. може розглядатися як зброя інформаційна у відносинах суперництва. 2) Вид інформації (подібно до програм і даних), що зберігається в базах знань і відображає знання людини — фахівця (експерта) в певній предметній частині; множина всіх поточних ситуацій в об'єктах даного типу і способи переходу від одного опису об'єкта до іншого. Для з. характерні внутрішня інтерпретованість, структурованість, зв'язність і активність. Говорячи образно: "знання = факти + переконання + правила".

ЗНІМОК /снимок/ [picture] — 1) Фотографія; зображення когось, чогось, одержане способом фотографування. 2) Копія; точне відтворення чогось.

ЗОБРАЖЕННЯ /изображение/ [image] — відображення інформації, візуальне подання даних.

З. радіолокаційне /и. радиолокационное/ — образ об'єкта, який одержують на різних пристроях індикації при добуванні інформації активними радіолокаційними засобами. З. р. місцевості одержують за допомогою панорамних радіолокаційних станцій та радіолокаційних станцій бічного огляду.

ЗОНА /зона/ [zone] (від грец. $\zeta\acute{\omega}\nu\eta$ — пояс) — певний простір, район, територія, що характеризується спільними ознаками.

З. антропогенна /з. антропогенная/ (від антропо..., що з грец. $\tilde{\alpha}\nu\vartheta\rho\omega\pi\varnothing\varsigma$ — людина і ... ген, що з грец. $\gamma\varepsilon\nu\nu\acute{\alpha}\omega$ — породжую, створюю) — зона, де раніше проводилися масові знищення і (або) захоронення

людей, скотобійні і т. ін., що здійснює вплив деструктивний на людину.

З. безпеки інформації /з. безопасности информации/ [security z.] — простір, в межах якого забезпечується безпека інформації.

З. геопатогенна /з. геопатогенная/ (від гео..., що з грец. $\gamma\tilde{\eta}$ — земля і ...патогенез, що з грец. $\pi\alpha\vartheta\varnothing\varsigma$ — біль і $\gamma\acute{\varepsilon}\nu\varepsilon\sigma\iota\varsigma$ — походження, породження) — зона, якій властивий природний вплив деструктивний на психіку людей.

З. демілітаризована /з. демилитаризованная/ [DeMilitarized Z. (DMZ)] — сегмент мережі, який розташований між мережею організації та загальнодоступною мережею, звичайно Інтернет. Такі служби загальнодоступних мереж як DNS и Web-сервери звичайно установлюються в DMZ.

З. заборонена /з. запретная/ [prohibited area] — район або місцевість, куди нелегко проникнути і де важко організувати збирання відомостей розвідувальних. З. з. — частина країни, куди закритий доступ іноземним дипломатам, а отже, і представникам іноземних спеціальних служб, що діють під дипломатичним прикриттям. Відомості із з. з. поступають в іноземні спеціальні служби від нелегалів, накопичуються в результаті непрямого спостереження (допити біженців, перебіжчиків і т. ін.), а також в ході ведення розвідки космічної і радіоелектронної.

З. контрольована /з. контролируемая/ [controlled z.] — фізично огороджена або умовно (в документах) позначена територія, в межах якої забезпечується захист інформації або проводяться заходи захисту інформації. Зовнішньою межею з. к. є межа території підприємства, організації державних або комерційних структур. Межами з. к. держави є державний кордон.

ЗОНДУВАННЯ /зондирование/ [probe, reconnaissance, sounding] (франц. sonder — досліджувати, вивідувати) — попереднє обережне вияснення чого-небудь і кого-небудь; розвідування.

ЗЧИТУВАЧ /считыватель/ [reader] — пристрій для фіксування або переміщення інформаційного носія і сприйняття закодованих на ньому даних.

З. жетонів /с. жетонов/ [badge r.] — пристрій, призначений для зчитування інформації, записаної на

невеликих пластмасових платах (жетонах). З. ж. часто входить до складу систем збирання даних, в яких кожний користувач сповіщає відомості про себе машині, пред'являючи ідентифікаційний жетон. З. ж. може також використовуватися для контролю за доступом у приміщеннях, обладнаних електричними кодовими замками, або вбудовуватися в клавіатуру та інші пристрої, що входять до складу систем інформаційних, для забезпечення контролю за доступом до інформації.

З. карток /с. карточек/ [card r.] — пристрій, призначений для зчитування даних, записаних на картці, і їхнього перетворення в двійковий код, придатний для передавання з метою подальшого оброблення. У пристроях зчитування з магнітних карток є транспортувальний механізм, що затягує картку в машину і переміщує її відносно зчитувальної головки. В деяких пристроях перед зчитувальною головкою встановлені спеціальні щітки для очищення картки. Після зчитування картки напрямок руху транспортувального механізму змінюється на протилежний, і картка повертається оператору. У пристроях, що використовуються в автоматах для видачі готівки по кредитних картках, картка не повертається, якщо вона і (або) вказаний на ній ідентифікаційний номер є фальшивими.

І

ІДЕНТИФІКАТОР /идентификатор/ [identification (identifier) word] — лексична одиниця, що використовується як ім'я для елементів мови; ім'я, що присвоюється даним і являє собою послідовність латинських літер і цифр, яка починається з літери.

І. атрибутний /и. атрибутный/ [attribute i.] (від лат. attributum — додане) — засіб ідентифікації людей, допущених у зону контрольовану або до носіїв інформації, у вигляді певного атрибута: перепустка, жетон, будь-який інший документ на право допуску, картка ідентифікаційна. Основний недолік і. а. — можливість попадання до сторонніх осіб, які можуть скористатися ними для протиправних дій.

І. біометричний /и. биометрический/ [biometric i.] (від грец. $\beta\iota\varnothing\varsigma$ — життя і $\mu\varepsilon\tau\rho\varnothing\nu$ — вимірюю) — засіб ідентифікації людей, допущених у зону контрольовану або до носіїв інформації, що використовує інфор-

мативні пізнавальні ознаки конкретної людини. У пристроях біометричної ідентифікації використовуються: рисунок капілярних ліній пальців; узори сітківки очей; геометрія руки; динаміка підпису; особливості мови; ритм роботи з клавіатурою. У зв'язку з цим можна виділити наступні і. б.: пристрій ідентифікації особистості за рисунком капілярних ліній пальця; пристрій ідентифікації особистості за узорами сітківки очей; пристрій ідентифікації особистості за геометрією руки; пристрій ідентифікації особистості за динамікою підпису; пристрій ідентифікації особистості за голосом і т.ін. І. б., забезпечуючи низьку ймовірність помилкової ідентифікації, мають гірші, порівняно з ідентифікаційними картками, показники правильної ідентифікації (упізнавання "своїх"), низьку надійність роботи, високу вартість. При покращенні експлуатаційних характеристик б. і. слід очікувати на їхнє широке застосування в різноманітних системах (комплексах) керування доступом.

І. доступу /и. доступа/ [access i.] — унікальна ознака суб'єкта або об'єкта доступу.

І. користувача /и. пользователя/ [personal-identification code, userid] — число або літеро-рядкове дане, що ідентифікує користувача в системі обчислювальній.

І. об'єкта комп'ютерної системи /и. объекта компьютерной системы/ [object i.] — унікальний атрибут об'єкта комп'ютерної системи, що дозволяє однозначно виділити даний об'єкт серед подібних.

ІДЕНТИФІКАЦІЯ /идентификация/ [identification] (від лат. identicus — тотожний і лат. ...ficatio, від facio — роблю) — 1) Ототожнення, прирівнювання, уподібнення. 2) Надання суб'єктам і об'єктам доступу ідентифікатора і (або) порівняння пред'явленого ідентифікатора з переліком наданих ідентифікаторів. 3) Операція розпізнавання обчислювальною системою суб'єктів та об'єктів доступу за унікальною ознакою — ідентифікатором, яка необхідна для управління доступом; після і., як правило, проводиться перевірка повноважень (див. автентифікація). 4) Процедура присвоєння ідентифікатора об'єктові комп'ютерної системи або встановлення відповідності між об'єктом і його ідентифікатором.

І. і встановлення автентичності документів /и. и установление подлинности документов/ [document i. and authentication] — сукупність спеціальних заходів (протоколів) для забезпечення захисту

інформації кожною стороною, що приймає участь в обміні документами. Для цього широке застосування знаходять криптографічні методи. При неавтоматизованому обміні інформацією автентичність документа засвідчується позитивним результатом перевірки особистого підпису людини, автора документа. При автоматизованому передаванні документів каналами зв'язку застосовується підпис цифровий.

І. і встановлення автентичності інформації на засобах її відображення й друку /и. и установление подлинности информации на средствах ее отображения и печати/ — сукупність заходів контролю позитивних результатів забезпечення достовірності інформації і результатів дешифрування одержаної інформації до відображення її на екрані.

І. і встановлення автентичності об'єкта (суб'єкта) /и. и установление подлинности объекта (субъекта)/ [entity i. and authentication] — сукупність заходів ідентифікації та автентифікації, кінцевою метою яких є допуск об'єкта (суб'єкта) до інформації обмеженого використання у випадку позитивного закінчення перевірки або відмова допуску у випадку негативного закінчення перевірки. Об'єктами ідентифікації і встановлення автентичності в системі обчислювальній можуть бути: людина (оператор, користувач, посадова особа); технічний засіб (термінал, дисплей, ЕОМ, КЗА); документи; носії інформації; інформація на дисплеї, табло і т.ін. Установлення автентичності об'єкта може здійснюватися людиною, апаратним пристроєм, програмою, обчислювальною системою і т.ін. В системах автоматизованих застосування вказаних методів з метою захисту інформації при її обміні передбачає конфіденційність образів і імен об'єктів.

І. і встановлення автентичності особистості /и. и установление подлинности личности/ [user i. and authentication] — процедура допуску (відмови допуску) користувача до інформації обмеженого використання на основі збігу образу (системи ідентифікаторів), який знімається з особистості користувача, з образом, що зберігається (з урахуванням вимог щодо безпеки інформації) у захищеній пам'яті системи обчислювальної.

І. і встановлення автентичності технічних засобів /и. и установление подлинности технических средств/ — процедура допуску (відмови допуску) до входу в систему користувача з певного термінала.

Може здійснюватися за допомогою паролів. Пароль можна використати не тільки для автентифікації користувача і термінала по відношенню до системи, але й для зворотного встановлення автентичності ЕОМ по відношенню до користувача. Це важливо, наприклад, в обчислювальних мережах, коли зв'язок здійснюється з територіально віддаленими об'єктами. В цьому випадку застосовують одноразові паролі або більш складні системи шифрування інформації.

І. користувача /и. пользователя/ [user i.] — упізнання користувача (за прізвищем та паролем) для визначення його повноважень.

ІДЕЯ /идея/ [idea] (від грец. *ιδέα* — початок, основа, первообраз) — 1) Найвища форма пізнання і мислення, яка не тільки відображає об'єкт, а й спрямована на його перетворення. 2) Думка, загальне поняття про предмет чи явище.

ІЛЮСТРАЦІЯ /иллюстрация/ [illustration] (лат. illustratio, від illustro — освітлюю, пояснюю) — 1) Зображення, яке наочно пояснює або доповнює будь-який друкований текст (наприклад, малюнок, фотографія, репродукція, карта, схема). 2) Наочне пояснення чого-небудь; наведення прикладів у статті, промові тощо.

ІМІДЖ /имидж/ [image] (англ. image — зображення, відображення, копія, подоба, образ) — в комунікативістиці — образ реального факту, події, явища, особи, що формується під впливом засобів масової інформації, які здатні спотворювати дійсність на угоду тим чи іншим орієнтаціям і втілювати це у псевдореалістичній манері. Особливу роль у створення і., які піднімають престижну репутацію організацій, фірм, а також політичних діячів, зірок естради або спорту, відіграє реклама, що розповсюджується каналами мас медіа і має для цього своїх фахівців — іміджмейкерів.

ІМІДЖМЕЙКЕР /имиджмейкер/ [imagemaker] — творець іміджів, спеціаліст з організації пропагандистських компаній і реклами осіб, організацій, партій, які потребують створення авторитету й популярності серед масової аудиторії.

ІМІТОВСТАВКА /имитовставка/ [key hash function] — 1) Послідовність даних, одержана за певним правилом з відкритих даних та ключа і яка служить для забезпечення імітозахисту даних. 2) Блок інфор-

мації фіксованої довжини, що одержується з тексту відкритого і ключа, однозначно відповідний відкритому текстові.

ІМІТОЗАХИСТ /имитозащита/ — захист від несанкціонованого модифікування і нав'язування інформації фальшивої.

ІМПЕРІАЛІЗМ /империализм/ [imperialism] (франц. imperialisme від лат. imperium — влада, панування) — в широкому розумінні слова — державна політика, спрямована на завоювання територій, встановлення політичного або економічного контролю над іншими державами.

І. інформаційний /и. информационный/ [information i.] — термін, який використовується прихильниками точки зору країн, що розвиваються, на противагу точці зору прихильників "західної концепції", що передбачає дотримання доктрини вільного потоку інформації і її купівлі-продажу усім країнам на ринкових умовах. Вважається, що у таких умовах можливий колоніалізм культурний.

ІМПОРТ /импорт/ [import] (англ. import, від лат. importo — ввожу) — ввіз товарів або капіталів будь-якою країною з-за кордону.

І. інформації /э. информации/ [information i.] — уведення інформації ззовні під керування комплексу засобів захисту.

ІНДИВІД /индивид/ [individual] (від лат. individuum — неподільне) — окрема людина, особа.

ІНДИКАТОР /индикатор/ [indicator] (лат. indicator, від indico — вказую, визначаю) — прилад, за допомогою якого здійснюють вимірювання, записування різних показників, об'єктів.

І. поля /и. поля/ [field i.] — виявник поля, що являє собою широкосмуговий приймач прямого підсилення (у найпростішому випадку — детекторний) з телескопічною штировою антеною. Наведений радіозакладкою в антені сигнал детектується і підсилюється до значень, що перевищують поріг спрацьовування звукової і світлової сигналізації. Нові варіанти і. п. доповнюються пристроєм акустичного зворотного зв'язку (акустичної "зав'язки" між гучномовцем і. п. і мікрофоном закладки), який дозволяє виділити випромінювання закладки на фоні інших радіосигналів. Подальшим удосконалення і. п. є інтерсептори.

ІНДУСТРІЯ /индустрия/ [industry] (від лат. industria — діяльність, старанність) — 1) Промисловість. 2) Виробництво.

І. змісту /и. содержания/ — галузь індустрії інформаційної, до якої відносяться організації, що створюють інтелектуальну власність. Інформацію створюють вчені, інженери, письменники, композитори, художники, фотографи. В цьому їм допомагають видавці, продюсери і організації, які надають первинному змістові "товарний вигляд". Сюди ж входять організації, які самі не створюють нової інформації, але компілюють її, вироблюючи довідники, бази даних, статистичні збірники і т.ін. На частку цих постачальників інформації припадає значна частка прибутків, що одержують в і. з.

І. інформаційна /и. информационная/ [information i.] — галузь економіки, зв'язана з виробництвом, обробленням, передаванням, збереженням всіх видів інформації, створенням необхідних для цього технологічних пристроїв. До неї входять приватні й державні організації, які створюють інформацію різноманітних видів, власність інтелектуальну, забезпечують функціонування пристроїв для розповсюдження інформації споживачам, виробляють обладнання і програмне забезпечення, призначене для оброблення інформації. І. і. можна представити у вигляді трьох її галузей, які створюють зміст (індустрія змісту), його розповсюджують (індустрія розповсюдження інформації) і оброблюють (індустрія оброблення інформації). Вона є найбільш динамічним сектором світової економіки, породжує продукти й послуги, які суттєво змінюють характер ведення бізнесу в традиційних галузях, безпосередньо не зв'язаних із створенням і розповсюдженням інформації Використання інформаційно-телекомунікаційних технологій у багатьох сферах послуг і промисловості стало цілком необхідним елементом конкурентної боротьби і стратегічного розвитку.

І. оброблення змісту /и. обработки содержания/ — галузь індустрії інформаційної, яка охоплює виробників комп'ютерів, телекомунікаційного обладнання і електроніки для споживачів.

І. розповсюдження інформації /и. распространения информации/ — галузь індустрії інформаційної, пов'язана із створенням і керуванням телекомунікаціями й мережами розповсюдження інформації. Вона включає телекомунікаційні компанії, мережі кабельного телебачення, системи супутникового мовлення,

радіо- і телевізійні станції, компанії стільникового зв'язку і т. ін.

ІНІЦІАЛІЗАЦІЯ /инициализация/ [initialization] — встановлення системи або об'єкта у відомий чи визначений стан.

ІНКАПСУЛЯЦІЯ /инкапсуляция/ [encapsulation] — процес розташування дейтаграми усередині пакета даних іншого мережного пакета даних. Може використовуватися з тим же самим або іншим протоколом.

ІНСТАЛЯЦІЯ /инсталляция/ [installation] — встановлення програмного виробу на ЕОМ.

І. ключа /и. ключа/ [key i.] — процес уведення ключа до криптосистеми.

ІНСТРУКЦІЯ /инструкция/ [instruction] — 1) Документ, що регламентує яку-небудь сторону діяльності організації або містить вказівки щодо використання будь-яких засобів. 2) Документ, який визначає порядок роботи фахівця при виконанні своїх функціональних обов'язків або в процесі вирішення конкретних завдань.

І. із захисту інформації в організації /и. по защите информации в организации/ [security regulation] — документ системи захисту інформації керівний, що визначає порядок захисту інформації в організації. Вона може містити наступні розділи: загальні положення; перелік відомостей, що охороняються; ознаки демаскуючі об'єктів організації; речовини демаскуючі, що створюються в організації; оцінка можливостей органів і засобів добування інформації; заходи захисту інформації організаційні і технічні; порядок планування роботи служби безпеки; порядок взаємодії з державними органами, що вирішують проблеми матеріальної і інтелектуальної власності, державної і комерційної таємниці.

І. із захисту інформації про конкретний виріб /и. по защите информации о конкретном изделии/ — документ системи захисту інформації керівний, що містить відомості, необхідні для забезпечення безпеки інформації про конкретний виріб на кожному етапі його створення, в тому числі: загальні відомості про найменування зразка, відомості, що належать захисту, і демаскуючі ознаки, потенційні загрози безпеці інформації, задум і заходи захисту, порядок контролю (завдання, органи контролю, що мають право на перевірку, засоби контролю, допустимі значення параметрів, що контролюються, умови і методики,

періодичність і види контролю), прізвища осіб, відповідальних за безпеку інформації.

ІНСЦЕДЕНТ /инсцедент/ [incident] — група атак, які згруповані за ознакою типу, техніки проведення, часом та типом елементів операційних систем.

ІНТЕЛЕКТ /интеллект/ [intellect, intelligence](від лат. intellectus — розуміння, розсудок, пізнання) — здатність до мислення, особливо до його вищих теоретичних рівнів. Окремі інтелектуальні здібності людини можуть бути автоматизовані при створені систем штучного інтелекту.

І. машинний /и. машинный/ — сукупність апаратних і програмних засобів ЕОМ, за допомогою яких забезпечується таке спілкування людини з машиною (інтерфейс), яке за своїм рівнем наближається до спілкування між собою фахівців, що вирішують спільну задачу.

І. штучний /и. искусственный/ [artificial i.] — наука, що виникла на базі міжгалузевих досліджень в галузі техніки обчислювальної, математичної логіки, програмування, психології, лінгвістики, нейрофізіології та інших галузей знань. Об'єктом вивчення ш. і. є метапроцедури, що використовуються людиною при вирішенні задач, що традиційно називаються інтелектуальними або творчими. Мета досліджень в галузі і. ш. — створення арсеналу метапроцедур, достатнього для того, щоб ЕОМ (або інші технічні системи) могли знаходити по постановках задач їхнє рішення. Основними методами, що використовуються в і. ш., є різного роду програмні моделі і засоби, експеримент на ЕОМ і теоретичні моделі. Основні досліджувані проблеми: подання знань; моделювання міркувань, діалогові процедури на природній мові; планування доцільної діяльності; навчання інтелектуальних систем в процесі їхньої діяльності.

ІНТЕРВ'Ю /интервью/ [interview] (англ. interview, букв. зустріч, бесіда) — 1) Жанр публіцистики, розмова журналіста з політичним, громадським або іншим діячем з актуальних питань. 2) Вид програми радіомовлення у вигляді розмови, що включає в себе два основних елементи: питання, які ставить журналіст компетентній особі, і відповіді останньої на поставлені питання. Питання повинні бути такими, які хотів би поставити слухач і на які він хотів би отримати чіткі відповіді, якщо би опинився на місці журналіста. Тривалість і., звичайно, не перевищує 5 хвилин.

ІНТЕРЕСИ /интересы/ [interest] — потреби, зацікавленість.

І. життєво важливі /и. жизненно важные/ — сукупність потреб, задовольняння яких надійно забезпечує існування і можливості прогресивного розвитку особистості, суспільства і держави. До і. ж. в. особистості відносяться, насамперед, права і свободи людини і громадянина, в тому числі інформаційні. І. ж. в. суспільства зв'язані із створенням і розвитком вільного, гуманного, високоосвіченого, гармонійного суспільства, заснованого на принципах демократії, бережливого відношення до своїх традицій і національного надбання, суспільства, що підтримує і всіляко охороняє основний свій осередок — сім'ю. І. ж. в. держави базуються на принципах сильної держави, її територіальної цілісності, незалежності і суверенітету.

ІНТЕРМЕРЕЖА /интерсеть/ [internetwork] — декілька територіально віддалених мереж обчислювальних локальних, з'єднаних між собою через міст або маршрутизатор.

ІНТЕРНЕТ /Интернет/ [Internet] — глобальна загальнодоступна комерційна мережа (всесвітнє об'єднання мереж), що об'єднує мільйони комп'ютерів по усьому світі. Життєдіяльність і розвиток І. координує Товариство Інтернету. І. в основному складається з пристроїв семи видів: повторювачів, мостів, маршрутизаторів, комутаторів, шлюзів, хостів і вузлів. Більшість з них працює на рівнях фізичному, канальному і мережному моделі ISO/OSI.

ІНТЕРСЕПТОРИ /интерсепторы/ [interceptor] (англ. interceptor — перехоплювач) — індикатори поля, створені на основі широкосмугових радіоприймачів з автоматичним настроюванням їхніх селективних елементів на радіосигнал з найбільшим рівнем.

ІНТЕРФЕЙС /интерфейс/ [interface] (від лат. inter... і англ. face — лице) — 1) Сукупність засобів і правил, що забезпечують взаємодію пристроїв обчислювальної системи і (або) програм. 2) Сукупність уніфікованих технічних і програмних засобів, що використовуються для сполучення пристроїв в обчислювальній системі або сполучення між системами. Межа між двома функціональними пристроями, що визначається їхніми характеристиками, характеристиками з'єднання, сигналів обміну і т. ін.

ІНТРАМЕРЕЖА /интрасеть/ [intranet, intranetwork] — 1) Внутрішня корпоративна IP-мережа підпри-

ємства, зв'язана з Інтернетом через маршрутизатор. 2) Об'єднання декількох мереж обчислювальних локальних в межах одного або декількох сусідніх будівель.

ІНФІЛЬТРАЦІЯ /инфильтрация/ [infiltration, seepage] (від лат. in... — префікса, що означає заперечення, відсутність чогось, проникнення в щось і filtratio — проціджування) — 1) Просочування, проникнення. 2) Процес проникнення агента на територію ворожої держави або у ворожу організацію. В першому випадку впровадження може бути як відкритим (коли агент має легальне прикриття і на законних засадах приїжджає в країну), так і таємним (коли він нелегально перетинає кордон сушею, повітрям або водою).

ІНФОКРАТІЯ /инфократия/ (від інформація і грец. *κράτøς*– сила, влада) — влада інформації. Базується на можливості одержання точної інформації про кожного і маніпулювання масами людей, відбираючи і дозуючи інформацію.

ІНФОРМАТИВНІСТЬ /информативность/ [information density, self-descriptiveness] — якісний показник кількості інформації в джерелі інформації.

І. ознаки /и. признака/ — показник ознаки, що відповідає значенню ймовірності виявлення об'єкта за цією ознакою. Чим меншій кількості об'єктів належить ознака, тим більш вона інформативна. Найбільш інформативна ознака іменна, що притаманна тільки одному конкретному об'єктові. Інформативність ознак непрямих в загальному випадкові нижча ніж інформативність ознак прямих. Проте є виключення, наприклад, інформативність чітких відбитків пальців відповідає інформативності іменних ознак.

ІНФОРМАТИЗАЦІЯ /информатизация/ [informatization] — організаційний, соціально-економічний і науково-технічний процес створення оптимальних умов для задоволення інформаційних потреб та реалізації прав громадян, органів державної влади, органів місцевого самоврядування, організацій, громадських об'єднань на основі формування та використання інформаційних ресурсів.

ІНФОРМАТИКА /информатика/ [informatics, computer science] (від франц. informatidue) — наука, яка займається вивченням законів, методів і способів одержання, зберігання, перетворення, передавання і використання інформації. Об'єктом дослідження і. є інформація. Поділ і. на основні напрямки опирається

на внутрішню єдність завдань, що вирішуються в них, і підходів до розуміння суті інформації. Виділяють вісім основних напрямків інформатики: інформатика теоретична, кібернетика, програмування, інтелект штучний, системи інформаційні, техніка обчислювальна, і. у природі та суспільстві.

І. теоретична /и. теоретическая/ [scientific i., theoretical i.] — напрямок інформатики, що використовує методи математики для побудови і вивчення моделей обробки, передавання та використання інформації, створює той теоретичний фундамент, на якому будується вся інформатика.

ІНФОРМАТОР /информатор/ [informer, intelligencer] — 1) Фахівець в якій-небудь галузі знань або виробництва, який здійснює діяльність інформаційну. 2) Особа, що постачає інформацію в службу розвідувальну. 3) Система автоматичного інформування користувачів. 4) Компонент пакета програм прикладних, який призначений для видавання повідомлень про хід вирішення задач даним пакетом.

ІНФОРМАЦІЯ /информация/ [information, data, intelligence] (від лат. informatio — роз'яснення) — 1) Відомості про навколишній світ, процеси, які в ньому відбуваються, про події, ситуації, чиюсь діяльність, що їх сприймають людина і живі організми, керуючі машини та інші системи. За змістом будь-яка і. може бути віднесена до семантичної (цією, що містить смисл) або до інформації про ознаки матеріального об'єкта — ознакової. 2) Зміст повідомлення, сигналу, пам'яті, а також відомості, що містяться в повідомленні, сигналі або пам'яті. 3) Змістовно-суттєва частина знань (відомостей, даних) про склад, структури і алгоритми предметної частини, яка є потенційно доступною для кількісних оцінок. Неформально за кількісну міру і. можна вважати різницю між кількістю інформаційних невизначеностей апріорної і апостеріорної. Від'ємне значення цієї різниці часто називають дезінформацією. 4) В техніці обчислювальній — сукупність всіх даних і програм, які використовуються в системі автоматизованій незалежно від способу їхнього фізичного та логічного подання.

І. автентифікації /и. аутентификации/ [authentication i.] — інформація, що використовується для автентифікації.

І. авторитетна /и. авторитетная/ [authoritative i.] — інформація, яка одержана з надійних джерел, і

якість її не викликає ніяких сумнівів.

І. вихідна /и. выходная/ [output i.] — інформація, що створюється під впливом навколишнього середовища, а також на основі інформації похідної і відомостей з ресурсів інформаційних.

І. відкрита /и. открытая/ [public i.] — інформація, яка вільно розповсюджується в сфері (середовищі) інформаційній. До і. в. відносяться: інформація, що створюється в процесі творчості (твори науки і культури, відкриті патенти і авторські свідоцтва); обов'язкова документована інформація; офіційні документи; масова інформація, що розповсюджується засобами масової інформації; інша інформація необмеженого доступу.

І. дискретна /и. дискретная/ [discrete i.] — інформація, що виражається змінними, які змінюються переривчасто в просторових або часових координатах. І. д. зручна тим, що її можна виражати загальноприйнятими для записування і читання символами (набором знаків, літер або цифр) і задавати їх у вигляді скінченної послідовності. І. д. є універсальною і тому набуває особливого значення при використанні цифрових ЕОМ, а також при вивченні складних систем у тих випадках, коли досліджуються величини якісного характеру, які можуть бути виміряні і виражені числом.

І. для керівництва /и. для руководства/ [management i., i. for administration] — інформація, призначена для певного кола осіб, відповідальних за організацію і управління будь-якою діяльністю, та що сприяє прийняттю ними найбільш обґрунтованих рішень.

І. документована /и. документированная/ [documentary i.] — зафіксована на матеріальному носії інформація з реквізитами, що дозволяють її ідентифікувати (див. ідентифікація).

І. з відкритих джерел /и. с открытых источников/ [plain-language i.] — те ж, що інформація відкрита.

І. з обмеженим доступом /и. ограниченного доступа/ [limited access i.] — інформація, право доступу до якої обмежене встановленими правовими нормами та (або) правилами. Розповсюдження такої інформації можливе в умовах конфіденційності або секретності. До і. з о. д. відноситься: інформація документована про державну або службову таємницю (в порядку захисту інтересів держави); документована інформація,

що містить відомості про ноу-хау і ноу-ноу (в порядку захисту секретів виробництва і науки); персональні дані (в порядку захисту особистої таємниці).

І. закрита /и. закрытая/ [private i., confidential i.] — інформація, яка з тих чи інших міркувань є таємницею і розповсюдження якої можливе лише за згодою органів, уповноважених контролювати питання, пов'язані з цією інформацією.

І. комерційна /и. коммерческая/ [commercial i.] (від лат. commercium — торгівля) — інформація, що розповсюджується тільки за бажанням її власника і на його умовах; об'єкт купівлі-продажу.

І. конфіденційна /и. конфиденциальная/ [confidential (sensitive) i.] (від лат. confidentia — довір'я) — інформація з обмеженим доступом, що містить відомості, які перебувають у володінні, користуванні чи розпорядженні окремих фізичних чи юридичних осіб або держави і порядок доступу до якої встановлюється ними.

І. критична /и. критическая/ [sensitive i.] — інформація, що вимагає захисту; будь-яка інформація, втрата або неправильне використання якої (модифікація, ознайомлення) може нанести шкоду власникові інформації або системі автоматизованій, або будь-якій іншій фізичній (юридичній) особі чи групі осіб.

І. масова /и. массовая/ — призначені для необмеженого кола осіб друковані, аудіо, аудіовізуальні та інші повідомлення і матеріали.

І. машинна /и. машинная/ [machine i., computer c.] — інформація, що циркулює в обчислювальному середовищі, зафіксована на фізичному носії у формі, доступній для сприйняття ЕОМ, або та, що передається по телекомунікаційних каналах: сформована в обчислювальному середовищі і пересилається за допомогою електромагнітних сигналів з однієї ЕОМ в іншу, з ЕОМ на периферійний пристрій, або на керуючий датчик обладнання.

І. надважлива /и. сверхважная/ — інформація або відомості розвідки настільки високого ступеня важливості, що вони передаються безпосередньо голові держави та іншим членам керівництва, що відпо-

відають за прийняття державних рішень.

І. надлишкова /и. избыточная/ [redundant i., superfluous i.] — інформація, що перевищує повну інформацію і формально є зайвою у повідомленні, тобто такою, без якої можна точно та однозначно установити зміст або значення повідомлення.

І. наукова /и. научная/ [scientific i.] — відомості наукового характеру. Охоплює дані про природничі науки та охорону здоров'я, наукові кадри, здатність науки сприяти розвитку промисловості та організації дослідницької роботи. В роботі інформаційній стратегічної розвідки перевага надається і. н. з досліджень, які забезпечують воєнно-технічну перевагу наявного або ймовірного противника.

І. нерелевантна /и. нерелевантная/ [irrelevant i., false drops] — інформація, що видається інформаційно-пошуковою системою у відповідь на запит, але не стосується тематики запиту.

І. ознакова /и. признаковая/ — дані, що описують матеріальний об'єкт за допомогою його ознак. В залежності від виду опису об'єкта і. о. поділяється на інформацію про зовнішній вигляд (ознаки об'кта видові), про його поля (ознаки сигналів), про структуру і склад його речовин (ознаки речовин), тощо.

І. особиста /и. личная/ [private i.] — інформація про громадян країни або організації, що зачіпає їхні інтереси, розповсюдження якої можливе лише у випадку згоди на це відповідних осіб або організацій.

І. персональна /и. персональна/ [personal i.] (від лат. personalis — особистий, особовий) — те ж, що інформація про громадян (персональні дані).

І. політична /и. политическая/ [political i.] — інформація, що включає відомості про систему державного управління, політичні партії, зовнішню політику. Пріоритет надається інформації, що характеризує механізм формування та реалізації воєнної політики, основні напрямки розвитку збройних сил та їхнє бойове застосування в різних регіонах світу, вплив збройних сил на створення у світі певної воєнно-політичної обстановки.

І. похідна /и. производная/ [derivative i.] — інформація, що створюється як на основі інформації

вихідної, так і на основі відомостей з ресурсів інформаційних.

І. приватна /и. частная/ [private i.] (від лат. privatus — особистий, неофіційний, домашній, несуспільний) — інформація особиста, дані, що доступні тільки їхньому власникові.

І. про громадян (персональні дані) /и. о гражданах (персональные данные)/ [personal i.] (від лат. personalis — особистий, особовий) — відомості про факти, події і обставини життя громадянина, що дозволяють ідентифікувати його особистість.

І. розвідувальна /и. разведывательная/ [intelligence i.] — сукупність даних розвідувальних і відомостей розвідувальних, що ґрунтуються на зібраних, оцінених та витлумачених фактах, викладених таким чином, що ясне їх значення для вирішення конкретних завдань поточної політики. Р. і. стосується тільки іноземних держав, як дружніх, так і потенційно ворожих.

І. секретна /и. секретная/ [secret i.] — інформація з обмеженим доступом, що містить відомості, які становлять державну та іншу передбачену законом таємницю і розголошення яких завдає шкоди особі, суспільству та державі.

І. семантична /и. семантическая/ [semantic i.] (від грец. *σημαντικός* — означальний) — смислова сторона мови. І. с. є продуктом абстрактного мислення людини і відображає об'єкти, явища як матеріального світу, так і створювані ним образи і моделі за допомогою символів мовами спілкування людей, що включають як природні мови національного спілкування, так і штучні професійні мови.

І. фальшива /и. фальшивая/ [false i.] (польс. — falsz, від лат. falsus — неправдивий, хибний, помилковий) — свідомо сформована інформація, що неправильно, помилково відображає характеристики та ознаки об'єкта, або інформація про неіснуючий реально об'єкт.

ІНФОРМОВАНІСТЬ /информированность/ [awareness, information distribution] — задовольняння в будь-якій мірі потреб в інформації, що приводить до володіння відомостями про навколишній світ і процеси в ньому. Стан і. визначає ступінь адекватності сприйняття суб'єктами навколишньої дійсності і як наслідок

— обґрунтованість рішень та дій, що приймаються.

І. держав світового співтовариства адекватна /и. государств мирового содружества адекватная/ — право кожної держави на інформаційну безпеку, забезпечення інформаційної безпеки усіх членів співтовариства в рівній мірі, врахування інтересів усіх сторін без будь-якої дискримінації, виключення односторонніх переваг, відмова від дій, що наносять шкоду іншій державі.

І. об'єктів безпеки адекватна /и. объектов безопасности адекватная/ — право об'єктів безпеки володіти інформацією про явища і процеси, що їх цікавлять, обмежене тільки законодавчо з метою охорони особистої, сімейної, професійної, комерційної та державної таємниці, а також моралі.

ІНФОРМУВАННЯ /информирование/ [advice, inform] — акт передавання органу керування певної поточної інформації. В залежності від змісту інформації і. можна класифікувати наступним чином: інформування правильне; дезінформування правильне; трансінформування; трансдезінформування.

І. правильне /и. правильное/ — передавання органу керування неспотвореної інформації про істинну обстановку.

ІНФРАСТРУКТУРА /инфраструктура/ [infrastructure] (від лат. infra — нижче, під і структура) — сукупність галузей та видів діяльності, що використовують як виробничу, так і невиробничу сфери економіки (транспорт, зв'язок, комунальне господарство, загальна і професійна освіта, охорона здоров'я і т. ін.).

І. відкритих ключів /и. открытых ключей/ [Public Key I. (PKI)] — сукупність систем, які існують для генерації, розповсюдження, виведення з використання, а також інших видів керування сертифікатами відкритих ключів.

І. влади /и. власти/ [i. of power] — комплекс соціально-політичних і правових органів, закладів, норм, силових, інформаційних та інших структур, на яких базується влада і які сприяють її існуванню, функціонуванню і розвитку. В їхньому числі — суспільні рухи, політичні партії, системи відбору і підготовки лідерів, засоби масової інформації, органи політичного маркетингу.

І. інформаційна /и. информационная/ [information i.] — структура системи забезпечення інформацій-

ного держави, до складу якої входять центри інформаційно-обчислювальні, банки даних і знань та Єдина система зв'язку автоматизована. Забезпечує загальні умови доступу всіх користувачів до інформації, що зберігається та надає їм можливість використання технологій інформаційних.

І. інформаційна глобальна /и. информационная глобальная/ — інфраструктура інформаційна світового (міждержавного) масштабу. Може створюватися на основі трансформації інфраструктур інформаційних національних при створенні глобального суспільства інформаційного з дотриманням наступних принципів: забезпечення справедливої конкуренції; заохочення приватних інвестицій; визначення й адаптація регулюючих механізмів; забезпечення відкритого доступу до мереж; створення умов для забезпечення універсального доступу до інформаційних послуг; забезпечення рівних можливостей для громадян; забезпечення різноманітності змісту, включаючи культурний і мовний. Ці принципи застосовуються до і. і. г. за допомогою: забезпечення технічної можливості з'єднання й оперування різних комп'ютерних мереж; розвитку глобальних ринків для комп'ютерних мереж і телекомунікаційних та послуг інформаційних; забезпечення інформаційної безпеки особистості і даних; кооперації в галузі досліджень і розробок з створення нових інформаційних продуктів і послуг; моніторингу соціальних наслідків становлення інформаційного суспільства.

І. інформаційна національна /и. информационная национальная/ — інфраструктура інформаційна однієї держави. До її складу входить не тільки обладнання для передавання, зберігання, оброблення даних, голосу, образів, але й цілий широкий ряд пристроїв, включаючи камери, сканери, клавіатури, телефони, комп'ютери, компакт-диски, відео- і аудіострічки, кабелі, проводи, супутники, оптичні кабелі, лінії передач, мікрохвильові мережі, телевізори, монітори і т.ін. Цінність і. і. н. полягає визначається такими її компонентами, як: інформація, яка може приймати вигляд наукових або ділових баз даних, звукових записів, бібліотечних архівів і т. ін.; програмне забезпечення, яке дозволяє користувачам маніпулювати даними, одержувати доступ і переглядати великі масиви інформації; стандарти мереж і кодів передач, що полегшують встановлення взаємозв'язків між мережами і забезпечують захист інформації і надійність мереж;

люди, що створюють інформацію, програмні продукти, обладнання і т. ін.

І. мережі обміну інформацією /и. сети обмена информацией/ — система організації відносин між об'єктами мережі обміну інформацією і сервісними службами, що використовуються в мережі.

І. телекомунікаційна /и. телекоммуникационная/ — система об'єктів інфраструктури інформаційної, призначена для розповсюдження інформації.

ІОНОСФЕРА /ионосфера/ [ionosphere] (від іони і сфера) — верхні шари атмосфери іонізовані внаслідок дії ультрафіолетового випромінювання Сонця. В залежності від концентрації вільних електронів і, відповідно, позитивно заряджених іонів іоносферу умовно поділяють на шари — D, E, F_1 і F_2. Найменша концентрація в шарі D, найбільша — в шарі F_2. Склад і. безперервно змінюється, він залежить від години доби, пори року і сонячної активності, які мають 11-річний цикл змінювання. Шар D розташовується до висоти приблизно 60 км. В нічні години в шарі D переважає рекомбінація електронів, іонізація зменшується або зникає. Шар E розташований на висоті 100–120 км і менше залежить від години доби, а шари F_1 і F_2 займають місце на висоті приблизно 160–400 км, причому уночі шар F_1 зникає. В іоносфері здійснюється переломлення, відбиття і поглинання радіохвиль (див. іоносферні хвилі).

ІСТЕБЛІШМЕНТ /истэблишмент/ [establishment] (англ. the Establishment — правлячі кола, впливові кола) — домінантна система державних, економічних, ідеологічних відносин, організацій, закладів та інших структур, що мають владний вплив на суспільство, а також особи й групи, що займають в них ключові позиції, мають вплив і користуються своїм привілейованим станом. В сферу і. інкорпоруються і мас-медіа, за допомогою яких здійснюється маніпуляція свідомістю масової аудиторії і формування її життєвого стилю.

Й

ЙМОВІРНІСТЬ /вероятность/ [probability] — математична числова характеристика ступеня можливості появи якої-небудь випадкової події при тих чи інших визначених умовах, що можуть повторюватися

необмежену кількість разів.

К

КАБЕЛЬ /кабель/ [cable, conductor] (нім. Kabel, голл. kabel, від лат. capulum — аркан) — один або кілька ізольованих проводів, вміщених у захисну оболонку. Застосовують для передавання електроенергії, звукових, радіо та телевізійних сигналів на великі віддалі тощо.

К. волоконно-оптичний /к. волоконно-оптический/ [fiber optic c.] — сукупність волокон оптичних, покритих захисною оболонкою. За умовами експлуатації кабелі розподіляються на монтажні, станційні, зонові і магістральні. Кабелі перших двох типів використовуються всередині будівель і споруд. Зонові і магістральні кабелі прокладаються в колодязях кабельних комунікацій, у ґрунтах, на опорах, під водою.

К. коаксіальний /к. коаксиальный/ [coaxial c.] — кабель, у якого два провідники: центральний дріт та циліндричний заземлений екран. Екран ізолюється від центрального проводу за допомогою різноманітних матеріалів і конструкцій. Для ізоляції використовується поліетилен, фторлан (фторопласт), поліпропілен, гума, неорганічна ізоляція. Для забезпечення гнучкості к. к. екран виготовляється з мідної або залізної сітки, а для захисту від зовнішніх впливів покривається шаром ізолятора (поліхлорвінілу). К. к. мінімізує електричні та радіочастотні завади: сигнали у к. к. не впливають на сусідні компоненти, потенційні завади від цих компонентів не впливають на сигнал, що передається кабелем.

К. симетричний /к. симметрический/ [balanced c.] — кабель, у якого провідники (жили) виконані з проводу однакового діаметра, мають однакову ізоляцію і розташовані так, що між ними можна провести площину симетрії.

КАДАСТР /кадастр/ [cadastre] (франц. cadastre) — системне зведення відомостей про відповідний об'єкт.

К. інформаційний /к. информационный/ [information k.] — сукупність відомостей, необхідних для прийняття рішення органом керування. К. і. може мати вигляд двомірної матриці, стовпці якої відповідають тематичним розділам кадастру, а рядки — їхнім характеристикам.

КАМЕРА /камера/ [camera, chamber] (лат. camera від грец. *καμάρα* — склеписта кімната) — внутрішня порожниста частина якої-небудь споруди, машини або приладу.

К. телевізійна /к. телевизионная/ [television k.] — пристрій для перетворення зображення у сигнал телевізійний. До складу т. к. входить перетворювач світлоелектричний, формувач телевізійного сигналу, пристрій синхронізації і розгортки. К. т. поділяються на чорно-білі і кольорові. Чорно-білі камери мають більш високу роздільну здатність і чутливість. Проте кольорове зображення більш інформативне. За конструктивною ознакою к. т. поділяються на корпусні і безкорпусні. Останні являють собою друковану плату з радіоелементами і світлоелектричним перетворювачем, на мішень якого за допомогою об'єктива проектується зображення. Твердотільні перетворювачі на основі пристроїв із зарядовим зв'язком середньої роздільної здатності забезпечують розділення приблизно 400 телевізійних ліній, високої роздільної здатності — 600 ліній. Чутливість к. т. при цьому складає 0,01–1 лк. Для підтримування на постійному рівні яскравості зображення на мішені в умовах широкого діапазону яскравості зображення території к. т. можуть обладнуватися електронним затвором, а об'єктиви — автоматичною діафрагмою. В залежності від конфігурації простору спостереження (від декількох градусів до майже 180°) застосовуються об'єктиви з постійної і змінною фокусною відстанню. Для послідовного огляду території або приміщення к. т. встановлюють на поворотні платформи з кутом повороту в горизонтальній площині до 360° і до 180° у вертикальній площині.

К. телевізійна мініатюрна /к. телевизионная миниатюрная/ — камера телевізійна дуже малих розмірів, призначена для прихованого спостереження в системах відеоконтролю і комплексах телевізійного спостереження. Обладнується об'єктивом із "винесеною вхідною зіницею", у якого площина апертури співпадає з вхідною зіницею, або спеціальними насадками. При використанні об'єктивів із діаметром зіниці від 0,9 до 2 мм камеру можна приладнати у двері, стіни, під шпалери, настінний годинник, в корпус сигналізатора та інші предмети. Для прихованого спостереження через невеликі отвори використовується також насадка у вигляді оптико-волоконного кабелю діаметром біля 2 мм і довжиною 50 і більше см з об'єктивом

на кінці.

К. фотографічна /к. фотографическая/ [photographic c.] — частина апарата фотографічного.

КАНАЛ /канал/ [channel] (від лат. canalis — труба, жолоб) — частина комунікаційної системи, що зв'язує між собою джерело і приймач повідомлень.

К. витоку інформації /к. утечки информации/ [c. of information leakage] — фізичний шлях перенесення інформації від її джерела до несанкціонованого одержувача (зловмисника).

К. витоку інформації агентурний /к. утечки информации агентурный/ [human c. of information leakage] — канал витоку інформації, переносником інформації в якому є особа (агент, шпигун), що усвідомлює протиправність своїх дій.

К. витоку інформації акустичний /к. утечки информации акустический/ [acoustic c. of information leakage] — канал витоку інформації технічний, носієм якої є механічні пружні хвилі акустичні в інфразвуковому (менше 16 Гц), звуковому (16–20 кГц) і ультразвуковому (понад 20 кГц) діапазонах частот, що розповсюджуються в атмосфері, воді і твердому середовищі.

К. витоку інформації електричний /к. утечки информации электрический/ — канал витоку інформації радіоелектронний, носієм якої є електричний струм. Сигнали електричні у вигляді змін електричного струму як носії інформації можуть бути аналоговими і дискретними, їхній спектр може містити частоти від десятків Гц до десятків ГГц. Найбільш широко застосовуються сигнали, ширина спектра яких відповідає ширині спектра стандартного телефонного каналу. Такі сигнали розповсюджуються лініями зв'язку, що зв'язують абонентів як у межах однієї організації, так і земної кулі в цілому.

К. витоку інформації електромагнітний /к. утечки информации электромагнитный/ — канал витоку інформації радіоелектронний, носіями якої є поля: у ближній зоні джерела поля — електричне і магнітне, в дальній зоні — електромагнітне.

К. витоку інформації з волоконно-оптичного кабелю /к. утечки информации из волоконно-оптического кабеля/ — канал витоку інформації оптичний, у якому для зняття інформації руйнують захи-

сну оболонку кабелю волоконно-оптичного, притискують фотодетектор приймача до очищеної площадки волокна і згинають кабель на кут, при якому частина світлової енергії направляється на фотодетектор приймача.

К. витоку інформації матеріально-речовий /к. утечки информации материально-вещественный/ — канал витоку інформації технічний, в якому витік інформації здійснюється шляхом несанкціонованого розповсюдження за межі організації речовинних носіїв з інформацією, що підлягають захисту, насамперед, чернеток документів, забракованих деталей і вузлів, демаскуючих речовин.

К. витоку інформації навмисний /к. утечки информации умышленный/ [premeditated c. of information leakage] — канал витоку інформації, в якому носії інформації та (або) середовище їхнього поширення формується цілеспрямовано.

К. витоку інформації ненавмисний /к. утечки информации неумышленный/ [unpremeditated c. of information leakage] — канал витоку інформації, в якому носії інформації та (або) середовище їхнього поширення формується самочинно.

К. витоку інформації одноканальний /к. утечки информации одноканальный/ — канал витоку інформації технічний, що складається з передавача, середовища розповсюдження і приймача.

К. витоку інформації оптичний /к. утечки информации оптический/ [optical c. of information leakage] — канал витоку інформації технічний, носієм якої є електромагнітне випромінювання в діапазоні 0,46–0,76 мкм (видиме світло) і 0,76–13 мкм (інфрачервоне випромінювання). Об'єкт спостереження в к. в. і. о. є одночасно джерелом інформації і джерелом сигналу, тому що світлові промені, що несуть інформацію про видові ознаки об'єкта, є відбиті об'єктом промені зовнішнього джерела або його власне випромінювання. Відбите від об'єкта світло містить інформацію про його зовнішній вигляд (видові ознаки), а випромінюване об'єктом світло — про параметри випромінювання (ознаки сигналів). Середовище розповсюдження в к. в. і. о. можливе трьох видів: безповітряний (космічний) простір; атмосфера; хвилеводи оптичні. Приймачами

сигналу в к. в. і. о. є приймачі оптичні.

К. витоку інформації радіоелектронний /к. утечки информации радиоэлектронный/ [radioelectronical c. of information leakage] — канал витоку інформації технічний, носієм якої є випромінювання електромагнітне в радіодіапазоні, а також електричний струм, що розповсюджується металевими проводами з частотами коливань від звукового діапазону до десятків ГГц. К. в. і. р. відноситься до найбільш інформативних каналів витоку інформації. В цьому каналі здійснюється перехоплення радіо- і електричних сигналів, спостереження радіолокаційне і радіотеплове та добувається інформація семантична, ознаки демаскуючі видові і сигнальні. К. в. і. р. використовують радіорозвідка, розвідка радіотехнічна, радіолокаційна і радіотеплова. В найбільш загальному випадку к. в. і. р. включає джерело сигналу або передавач, середовище розповсюдження електричного струму або електромагнітної хвилі і приймач сигналу. В к. в. і. р. джерела сигналів можуть бути чотирьох видів: передавачі функціональних каналів зв'язку; джерела небезпечних сигналів; об'єкти, що відбивають електромагнітні хвилі в радіодіапазоні; об'єкти, що випромінюють власні (теплові) радіохвилі. Середовищем розповсюдження к. в. і. р. є атмосфера, безповітряний простір, а також електричні проводи різноманітних типів та хвилеводи. Носій у вигляді електричного струму розповсюджується проводами, а електромагнітне випромінювання (поля) — в атмосфері, в безповітряному просторі або хвилеводами. У приймачі здійснюється виділення носія з інформацією за частотою, підсилення виділеного сигналу і одержання з нього інформації (демодуляція, декодування). У відповідності до виду носіїв інформації к. в. і. р. поділяються на електромагнітні і електричні, а в залежності від способу перехоплення на канали витоку інформації з функціональних каналів зв'язку та канали з джерелами небезпечних сигналів і пристроями закладними.

К. витоку інформації складений /к. утечки информации составной/ — канал витоку інформації технічний, що складається з декількох послідовних або паралельних каналів. При цьому використовується властивість інформації переписуватися з одного носія на інший. Наприклад, якщо в кабінеті ведеться конфіденційна розмова, то витік можливий не тільки каналом акустичним через стіни, двері, вікна, але й каналом

оптичним — шляхом одержання інформації лазерним променем із скла вікна або каналом радіоелектронним із використанням установленої в кабінеті радіозакладки. У двох останніх варіантах використовується складений канал, створений з послідовно з'єднаних акустичного і оптичного (на лазерному промені) або акустичного і радіоелектронного (радіозакладка — середовище розповсюдження — радіоприймач) каналів. Для підвищення дальності може також використовуватися ретранслятор, який поєднує функції приймача одного каналу і передавача наступного каналу.

К. витоку інформації технічний /к. утечки информации технический/ [technical c. of information leakage] — канал витоку інформації, несанкціоноване перенесення інформації в якому від джерела до зловмисника здійснюється з використанням технічних засобів. Основною класифікаційною ознакою к. в. і. т. є фізична природа носія інформації. За цією ознакою вони поділяються на оптичні; радіоелектронні; акустичні; матеріально-речові. Крім того, к. в. і. т. можуть поділятися: за інформативністю — на інформативні і малоінформативні; за часом проявляння — на постійні, епізодичні і випадкові; за структурою — на одноканальні і складені. Як будь-який канал зв'язку (канал передавання інформації) к. в. і. т. характеризується пропускною здатністю і дальністю передавання інформації.

К. достовірний /к. достоверный/ [trusted path] — захищений шлях передавання інформації між користувачем і комплексом засобів захисту, що не може бути імітований, а інформація, що передається ним, не може бути отримана або модифікована стороннім користувачем або процесом.

К. доступу до ПЕОМ несанкціоновані /к. доступа к ПЭВМ несанкционированные/ — канали (пристрої), через які можливий несанкціонований витік інформації, що оброблюється в ПЕОМ. Такими каналами можуть бути: термінал користувача (клавіатура і засоби відображення інформації); засоби документування інформації; засоби завантаження програмного забезпечення; носії інформації (машинні і паперові); внутрішній монтаж ПЕОМ; побічне електромагнітне випромінювання; побічні наведення інформації по мережі електроживлення і заземлення апаратури; побічні наведення в ланцюгах сторонньої апаратури;

відходи, викинуті у корзину для сміття.

К. зв'язку /к. связи/ [communication c.] — середовище (лінія зв'язку) і сукупність технічних засобів між двома точками тракту зв'язку.

К. інформаційний /к. информационный/ — те ж, що канал передавання даних.

К. передавання даних /к. передачи данных/ [data c.] — канал електрозв'язку для передавання сигналів даних.

К. передавання інформації /к. передачи информации/ — фізичний шлях перенесення інформації від її джерела до одержувача. К. п. і. містить три основних елементи: джерело сигналу (інформації), середовище розповсюдження носія інформації і приймач.

К. прихований /к. скрытый/ [covert c.] — 1) Канал передавання інформації між двома процесами, які взаємодіють із метою порушення прийнятої в системі політики безпеки. 2) Спосіб одержання інформації за рахунок використання шляхів передавання інформації, існуючих в системах комп'ютерних, але не керованих комплексом засобів захисту, або спостереження за існуючими потоками інформації.

К. прихований з пам'яттю /к. скрытый с памятью/ [storage covert c.] — канал прихований, що реалізується шляхом прямого або непрямого запису інформації в певну область пам'яті одним процесом і прямим чи непрямим читанням даної області пам'яті іншим процесом.

К. прихований часовий /к. скрытый временный/ [timing covert c.] — прихований канал, що дозволяє передавати інформацію від одного процесу до іншого шляхом модулювання першим процесом часових характеристик системи (наприклад, часу зайнятості процесора центрального), що спостерігається іншим процесом.

К. стеганографічний (Стегоканал) /к. стеганографический (стегоканал)/ — канал передавання стеганограми.

КАРТКА /карточка/ [card] (від грец. $\chi\acute{\alpha}\tau\eta\varsigma$ — аркуш папірусу) — носій інформації (даних) у формі прямокутної пластини. Картка повинна відповідати специфікаціям Міжнародної організації по стандартизації

(ISO), які встановлюють фізичні розміри картки і те, як вона буде себе вести при різноманітних механічних, фізичних, хімічних та інших впливах. У відповідності із специфікацією ISO 7816/1 розміри картки повинні бути: довжина — 85,6 мм; ширина — 53,9 мм; товщина — 0,76 мм.

К. з магнітною смугою /к. с магнитной полосой/ [magnetic striped c.] — картка (картка пластикова), що має магнітну смугу на зворотній стороні картки. Магнітна смуга може зберігати біля 100 байт (символів) інформації, яка зчитується спеціальним зчитувачем.

К. ідентифікаційна /к. идентификационная/ [identifying c., identity c.] (від лат. identicus — тотожний) — картка (картка пластикова), яка поряд із набором традиційних реквізитів її власника (прізвища, імені, по батькові, фотографії) містить прихований персональний ідентифікаційний номер (код) та інші дані, необхідні для його достовірного впізнавання. Зворотна сторона картки може мати місце для підпису власника картки. В залежності від способу запису ідентифікаційної інформації к. і. поділяються на наступні види: картки ідентифікаційні магнітні; картки ідентифікаційні інфрачервоні; картки ідентифікаційні штрихові; картки ідентифікаційні Віганда; картки ідентифікаційні безконтактні (проксіміті). Найменше захищеними від фальсифікації вважаються магнітні картки, більш захищеними — інфрачервоні і картки Віганда, більш високий рівень захисту мають безконтактні картки. Перевагою останніх є безконтактний спосіб зчитування її атрибутів, що забезпечує високу пропускну здатність КПП з високою надійністю ідентифікації. Основні недоліки — відносно висока ціна і неможливість оперативного змінювання коду картки.

К. ідентифікаційна безконтактна (проксіміті) /к. идентификационная бесконтактная (проксимити)/ [proximity c.] — картка, ідентифікаційний номер якої зчитується без безпосереднього контакту із зчитувачем (на відстані 10–80 см). Основу картки складає мікросхема з енергонезалежною пам'яттю і рамкова антена, розташована всередині герметизованої пластикової картки. Вбудована в картку електронна схема радіочастотного ідентифікатора посилає зчитувачеві свій код, на основі якого приймається рішення про допуск. В залежності від джерела живлення застосовують два види к. і. б.: активні і пасивні. Активні картки (з джерелом енергоживлення) забезпечують роботу на значно більших відстанях, ніж пасивні,

проте вони дорожчі, мають збільшену товщину, менш надійні і потребують регулярної заміни джерела живлення. Як джерело живлення пасивних карт використовується радіоприймач картки, який акумулює електромагнітну енергію, що випромінюється високочастотним генератором зчитувача.

К. ідентифікаційна Віганда /к. идентификационная Виганда/ — картка, у пластикову основу якої впресовуються відрізки тонкого проводу з випадковою орієнтацією. Кожна картка в результаті такої технології виготовлення має свій неповторний рисунок просторово-орієнтованих відрізків проводу, які специфічним чином реагують на зовнішнє електромагнітне поле. Відгук картки на це поле запам'ятовується і служить еталоном при ідентифікації за допомогою спеціального зчитуючого пристрою.

К. ідентифікаційна інфрачервона /К. идентификационная инфракрасная/ — картка, виготовлена з прозорого для інфрачервоних променів пластику. На внутрішню поверхню шару пластику наноситься за допомогою речовини, що адсорбує інфрачервоні промені, ідентифікаційний номер власника. Атрибути власника зчитуються в інфрачервоних променях зовнішнього джерела.

К. ідентифікаційна магнітна /к. идентификационная магнитная/ [identity magnetically coded c.] — картка з магнітною смугою, на якій записана інформація про повноваження її власника.

К. ідентифікаційна штрихова /к. идентификационная штриховая/ — картка, в якій на один з внутрішніх шарів наноситься ідентифікаційний штриховий код власника, який зчитується зчитувачем штрихового коду.

К. оптичної пам'яті /к. оптической памяти/ [optical memory c.] — картка, призначена для одноразового запису і багаторазового зчитування інформації за допомогою лазерного променя. Звичайна к. о. п. може зберігати від 2 до 16 Мбайт інформації.

К. пам'яті /к. памяти/ [memory c.] — картка (картка пластикова), яка обладнана мікросхемою пам'яті. Можливості к. п. підтримуються спеціальним зчитувачем (пристроєм, який може читати і записувати в пам'ять картки). Обсяг пам'яті звичайної картки складає приблизно 256 байт, проте існують картки з більшим обсягом пам'яті. Ця пам'ять може бути реалізована або у вигляді програмованих пристроїв за-

пам'ятовуючих постійних (ППЗП), які можна зчитувати багато разів, але в кожну адресу такої пам'яті інформація може бути записана тільки один раз, або у вигляді ППЗП із стиранням, яким може записуватися і зчитуватися багаторазово.

К. пластикова /к. пластиковая/ [plastic c.] — найпростіший носій даних у вигляді прямокутної пластикової пластини (див. картка).

КАРТОТЕКА /картотека/ [card file, file] — 1) Система карток з довідковими, обліковими чи іншими даними. 2) Скринька або шафа для зберігання карток. 3) Інформаційний документ органів психологічної війни. Містить інформацію на певні теми (питання), або про політичних діячів, керівні кадри в алфавітному порядкові (у вигляді характеристик, формулярів, анкет). Інформація розташовується в певній послідовності. Наприклад, наступним чином: анкетні дані (рік і місце народження, національність, соціальне походження, освіта, сімейний стан, партійна належність; соціально-політичні і психологічні дані (службова кар'єра, соціальний і майновий стан, політичні погляди, авторитет серед підлеглих, характеристика службової діяльності, особливості характеру); дані, що мають особливий інтерес (погані поступки, негативні якості особистості, вади і т. ін.); висновки про найбільш придатні форми й способи впливу психологічного на даного індивіда.

КАСЕТА /кассета/ [cartridge, cassette] (від франц. cassette — скринька) — 1) Світлонепроникний футляр для зберігання світлочутливих фото- й кіноплівок. 2) Контейнер, призначений для розміщення та захисту різноманітних носіїв інформації — магнітних стрічок, магнітних і оптичних дисків.

КАТЕГОРИЗАЦІЯ /категоризация/ [categorization] — класифікація об'єктів за категоріями.

КАТЕГОРІЯ /категория/ [category] (від грец. *κατηγόρία* — ознака, обвинувачення) — 1) Загальне поняття, що відображає універсальні властивості і відношення об'єктивної дійсності, загальні закономірності розвитку всіх матеріальних, природних і духовних явищ. 2) Поняття, що означає розряд предметів. 3) Клас, рівень категоризації.

К. допуску /к. допуска/ [security clearance] — категорія, що пов'язана з суб'єктом доступу і визначає

категорію захисту інформації, до якої цьому суб'єктові надане право доступу.

К. доступу /к. доступа/ [access c., access level] — 1) Атрибут об'єкта доступу, що визначає рівень повноважень, який повинен мати суб'єкт доступу для одержання права доступу до даних об'єкта (наприклад, категорія секретності і службові повноваження). 2) Комбінація ієрархічних і неієрархічних атрибутів доступу, що відображає рівень критичності (наприклад, конфіденційності) інформації або повноважень користувача щодо доступу до такої інформації.

К. загрози /к. угрозы/ — категорія, що пов'язана з загрозою безпеці інформації (даних). Так в мережах обчислювальних виділяють п'ять категорій загроз: розкриття змісту повідомлень, що передаються; аналіз трафіка, що дозволяє визначити належність відправника і одержувача даних до однієї з груп користувачів мережі; зміна потоку повідомлень, що може привести до порушення режиму роботи будь-якого об'єкта, що керується з віддаленої ЕОМ; неправомірна відмова в наданні послуг; несанкціоноване встановлення з'єднання. Згідно до визначення терміну "безпека інформації" першу і другу загрозу можна віднести до витоку інформації, третю і п'яту — до її модифікації, а четверту загрозу до порушення процесу обміну інформацією, тобто до її втрати.

К. захисту /к. защиты/ [security classification] — див. гриф секретності.

К. інформаційної боротьби /к. информационной борьбы/ — категорії, що відображають найбільш загальні, суттєві предмети, процеси і властивості інформаційної боротьби. Розрізняють загальні і часткові категорії. Загальні мають відношення до всіх галузей теорії інформаційної боротьби. Головні з них "інформація" і "боротьба інформаційна". Часткові формують у складових частинах теорії. Так, теорія захисту інформації має свої категорії, наприклад, "захист інформації" і "безпека інформаційна", теорія ураження інформації — свої, наприклад, "ураження інформації".

К. керування доступом /к. управления доступом/ [access control c.] — мовні елементи, призначені для визначення правил, що запобігають виконанню несанкціонованих операцій.

К. користувача /к. пользователя/ [user c.] — класифікаційна група, до якої віднесений даний кори-

стувач або група користувачів. За обсягом знань у галузі програмного забезпечення та ступенем їхнього використання в виробничій діяльності користувачі поділяються на системних програмістів (найвища категорія), прикладних програмістів та кінцевих користувачів.

К. обслуговування /к. обслуживания/ [grade of service] — сукупність видів обслуговування, які можуть бути надані користувачу.

КВАДРАТОР /квадратор/ [squarer] (від італ. quadro, букв. квадратний) — пристрій, призначений для зменшення кількості моніторів у системі відеоконтролю за рахунок одночасного показу на екрані монітора декількох зображень (4 і більше). При цьому екран ділиться на частини за кількістю моніторів.

КВАЛІФІКУВАННЯ /квалифицирование/ [analysis] (від лат. qualis — який, якої якості) — оцінювання, визначення внутрішньої якості чогось.

К. рівня безпеки /к. уровня безопасности/ [evaluation] — кінцевий етап технологічного циклу створення систем оброблення інформації захищених, що безпосередньо передує процедурі сертифікації і закінчується присвоєнням обчислювальній системі того чи іншого класу чи рівня безпеки (див. також аналіз кваліфікаційний).

КВАРТИРА /квартира/ [flat, apartment] — частина житлового будинку з окремим входом, що складається, звичайно, з однієї або кількох кімнат, кухні, передпокою тощо.

К. конспіративна /к. конспиративная/ [secret address] — житловий будинок (або квартира), яка утримується на кошти служби розвідувальної (або організації) і використовується в оперативних цілях (наприклад, для таємних зустрічей, явок, допитів агентів і інформаторів або укриття перебіжчиків.

КВОТА /квота/ [quota] (від лат. quot — скільки) — 1) Частка, частина, певна норма. 2) Обмеження можливості використання певного ресурсу системи комп'ютерної користувачем або процесом.

КЕРУВАННЯ /управление/ [control] — 1) Направлення ходу, руху кого-, чого-небудь. 2) Процес цілеспрямованої дії на об'єкт, що здійснюється з метою організації його функціонування згідно заданої програми.

К. базами даних /у. базами данных/ [database c.] — основна функція СКБД, яка полягає в керуванні

створенням і веденням баз даних, доступом програм і користувачів до баз даних, пошуком і видачею інформації за їхніми запитами.

К. доступом /у. доступом/ [access c.] — сукупність заходів з визначення повноважень і прав доступу, контролю за додержанням правил розмежування доступу.

К. доступом адміністративне /у. доступом административное/ [mandatory access c.] — принцип керування доступом, який полягає в тому, що керувати потоками інформації між користувачем і об'єктами дозволено тільки користувачам авторизованим, а звичайні користувачі не мають можливості створити потоки інформації, які могли б призвести до порушення встановлених правил розмежування доступу.

К. доступом до інформації /у. доступом к информации/ [access c.] — сукупність взаємопов'язаних заходів, спрямованих на ідентифікацію осіб і звернень до інформації, перевірку повноважень осіб і звернень, реєстрацію звернень до інформації, що підлягає захисту, реагування на звернення до інформації (дозвіл доступу або відмова доступу до інформації).

К. доступом довірче /у. доступом доверительное/ [discretionary access c.] — принцип керування доступом, який полягає в тому, що звичайним користувачам дозволено керувати (довіряють керування) потоками інформації між іншими користувачами й об'єктами свого домена (наприклад, на підставі права володіння об'єктом) без утручання адміністратора.

К. доступом за сукупністю атрибутів /у. доступом по совокупности атрибутов/ [inference c.] — керування доступом до інформації про окремий атрибут, яка отримується шляхом аналізу інформації про сукупність атрибутів (отримується інформаційно-аналітичним шляхом).

К. доступом мандатне (повноважне) /у. доступом мандатное (полномочное)/ [mandatory access c.] — розмежування доступу суб'єктів до об'єктів, засноване на конфіденційності (характеризується міткою — див. Мітка грифа) інформації, що міститься в об'єктах доступу, та офіційному дозволі (допуску) суб'єктів доступу звертатися до інформації такого рівня конфіденційності.

К. доступом обмежуюче (дискреційне) /у. доступом ограничивающее (дискреционное)/ [discreti-

onary access c.] — розмежування доступу між пойменованими суб'єктами доступу та пойменованими об'єктами доступу. Суб'єкт з певним правом доступу може передавати це право будь-якому іншому суб'єкту.

К. ключами /у. ключами/ [key management] — 1) У криптології — загальна назва для операцій, що виконуються над криптографічними ключами на всіх етапах життєвого циклу ключів (передвикористання, використання та поствикористання), тобто для процесів генерації, початкової ініціалізації, інсталяції, розподілу, збереження, контролю використання, зміни, анулювання, архівації та знищення. 2) Сукупність процесів генерації, реєстрації, сертифікації, початкової ініціалізації, розподілу, збереження, використання, зміни, виведення з використання, архівації та знищення ключів. Схеми керування ключами для криптосистем симетричних та асиметричних дещо різняться. Для симетричних криптосистем традиційними є дві схеми: прямий обмін ключами (point-to-point) та обмін через посередника (з використанням центра генерації ключів або центра ретрансляції ключів). Для асиметричних криптосистем традиційними є сертифікатні схеми або схеми, що базуються на ідентифікаторах (identity-based) керування ключами. Системи керування ключами відкритими для асиметричних криптосистем називають ще інфраструктурою відкритих ключів.

К. потоками /у. потоками/ [flow c.] — сукупність функцій і процедур, які забезпечують неможливість передавання інформації каналами прихованими, тобто в обхід комплексу засобів захисту. В більш вузькому значенні часто розуміється сукупність процедур, які забезпечують неможливість передавання інформації від об'єкта системи комп'ютерної з більш високим рівнем доступу до об'єкта комп'ютерної системи з більш низьким рівнем доступу.

К. системою захисту інформації /у. системой защиты информации/ — процес, який забезпечує організацію спільної роботи всіх елементів системи захисту інформації та реалізацію виробленої стратегії захисту, а також надає засоби реалізації організаційно-розпорядчих заходів по захисту інформації у системі обчислювальній.

К. шифруванням /у. шифрованием/ — процес періодичної зміни коду ключа, що забезпечує кожний раз оригінальне представлення інформації при використанні одного і того ж алгоритму шифрування або

пристрою.

КІБЕРЕКОНОМІКА /киберэкономика/ (від кібернетика і економіка) — поняття зв'язане з економічною активністю, спрямованою на створення продукції інформаційної і послуг в Інтернеті і глобальних комерційних мережах, а саме: електронна торгівля, маркетинг, реклама, публікації, інвестиції і т. ін.

КІБЕРНЕТИКА /кибернетика/ [cybernetics] (від грец. *κυβερνητική* — мистецтво керування) — мистецтво керування) — 1) Наука про загальні закони управління і зв'язку в природі й суспільстві. 2) Прикладна інформатика в галузі створення і використання автоматичних або автоматизованих систем керування різної складності, від керування окремим об'єктом до найскладніших систем управління цілими галузями промисловості, банківськими системами, системами зв'язку і навіть співтовариствами людей.

КІБЕРСПЕЙС /киберспейс/ [cyberspace] — кібернетичний простір. Термін, утворений від слова кібернетика і вживається для позначення сфери діяльності, зв'язаної із застосуванням комп'ютерної техніки і супермагістралей інформаційних.

КІЛЬКІСТЬ /количество/ [amount, quantity, content] — ступінь змінювання вимірюваних властивостей, явищ, їхні мірні характеристики.

К. інформації /к. информации/ [a. of information, information c.] — міра інформації, що повідомляється появою події певної ймовірності; міра оцінки інформації, що міститься в повідомленні; міра, що характеризує зменшення невизначеності, що міститься в одній випадковій величині відносно іншої. Визначається за формулою $J_i = -k \cdot \ln(p_i)$ або за формулою ентропії

$$H = -\sum_{i=1}^{n} p_i \log_2 p_i,$$

де k — коефіцієнт, що залежить від вибраної системи числення; p_i — ймовірність передавання і-того значення повідомлення; n — можлива кількість значень повідомлення.

КІНОАПАРАТ /киноаппарат/ [cine-camera] (від грец. *κινέω* — рухаю і апарат) — оптико-механічний

прилад, призначений для реалізації процесу фіксації серії послідовних зображень (кадрів) об'єкта спостереження через задані проміжки часу, що визначаються частотою кадрів за секунду. Кожний кадр містить зображення об'єкта в момент зйомки. Число кадрів коливається від одиниць за хвилину і навіть годину для зйомки повільно плинних процесів до сотень тисяч на секунду — для надшвидкісної спеціальної зйомки. Будова к. близька до будови апарата фотографічного з тою принциповою різницею, що в процесі кінозйомки плівка стрибкоподібно пересувається за допомогою грейферного механізму перед об'єктивом на один кадр. Закриття об'єктива на час пересування плівки здійснюється заслінкою (обтюратором), обертання якого перед об'єктивом синхронізовано з роботою грейфера.

КЛАС /класс/ [class] (від лат. classis — розряд, група) — сукупність, розряд, група предметів або явищ, що мають спільні ознаки, якість.

К. ВГБ /к. ТГБ/ [assurance c.] — верхній рівень формальної структури вимог гарантій безпеки. Містить наступні елементи: назву класу [class name]; опис класу [class introduction]; розділи ВГБ [assurance family]. Вимоги розподілені на 7 класів ВГБ: керування проектом; дистрибуція; розробка; документація; процесу розробки; тестування; оцінка захисту.

К. ВГБ: дистрибуція /к. ТГБ: дистрибуция/ [c. ADO: Delivery and Operation] — клас ВГБ, що включає наступні розділи ВГБ: постачання; установка, настройка, запуск.

К. ВГБ: документація /к. ТГБ: документация/ [c. AGD: Guidance Documents] — клас ВГБ, що включає наступні розділи ВГБ: керівництво адміністратора; керівництво користувача.

К. ВГБ: керування проектом /к. ТГБ: управление проектом/ [c. ACM: Configuration Management] — клас ВГБ, що включає наступні розділи ВГБ: засоби керування проектом; керування версіями; конфігурація проекту.

К. ВГБ: оцінка захисту /к. ТГБ: оценка защиты/ [c. AVA: Vulnerability Assessment] — клас ВГБ, що включає наступні розділи ВГБ: аналіз схованих каналів; аналіз можливостей неправильного використання

засобів захисту; аналіз стійкості засобів захисту; аналіз продукту на наявність уразливостей.

К. ВГБ: процес розробки /к. ТГБ: процесс разработки/ [с. ALC: Life Cycle support] — клас ВГБ, що включає наступні розділи ВГБ: безпека середовища розробки; виправлення помилок і ліквідація уразливостей; технологія розробки; засоби розробки.

К. ВГБ: розробка /к. ТГБ: разработка/ [с. ADV: DeVelopment] — клас ВГБ, що включає наступні розділи ВГБ: загальні функціональні специфікації; архітектура захисту; форма подання продукту на сертифікацію; структура засобів захисту; часткові специфікації засобів захисту; відповідність описів різного рівня; політика безпеки.

К. ВГБ: тестування /к. ТГБ: тестирование/ [с. ATE: TEsts] — клас ВГБ, що включає наступні розділи ВГБ: повнота тестування; глибина тестування; методика тестування; незалежне тестування.

К. захищеності /к. защищенности/ [protection c.] — певна сукупність вимог із захисту засобів обчислювальної техніки (автоматизованої системи) від несанкціонованого доступу до інформації.

К. захищеності засобів обчислювальної техніки /к. защищенности вычислительной техники/ [protection c. of computer systems] — характеристика засобів обчислювальної техніки, що впливають на захищеність і описуються певною групою вимог, що варіюються за рівнем і глибиною в залежності від класу захищеності.

К. ФВБ /к. ФТБ/ [functional c.] — в "критеріях Загальних" — верхній рівень формальної структури вимог безпеки функціональних. Містить наступні елементи: назву класу [class name]; опис класу [class introduction]; розділи ФВБ [functional families]. Функціональні вимоги розподілені на 11 класів ФВБ: аудит; причетність до приймання/передавання; криптографія; захист інформації; ідентифікація і автентифікація; керування безпекою; конфіденційність роботи в системі; надійність засобів захисту; контроль за використанням ресурсів; контроль доступу до системи; пряма взаємодія). Зміст класів функціональних вимог відрізняється своєю всеохоплюючою повнотою і багаторівневим підходом до забезпечення безпеки. Окремі класи вимог спрямовані на забезпечення безпеки самих засобів захисту, контролю за експлуатацією системи,

забезпечення конфіденційності сеансів доступу до системи й організації обміну інформацією.

К. ФВБ: аудит /к. ФТБ: аудит/ [с. FAU: security AUdit] — клас ФВБ, що включає наступні розділи ФВБ: автоматичне реагування на спроби порушення безпеки; реєстрація й облік подій; аналіз протоколу аудита; доступ до протоколу аудита; відбір подій для реєстрації й обліку; протокол аудита.

К. ФВБ: захист інформації /к. ФТБ: защита информации/ [с. FDP: user Data Protection] — клас ФВБ, що включає наступні розділи ФВБ: політики керування доступом; засоби керування доступом; автентифікація інформації; експорт інформації із системи; політики керування інформаційними потоками; засоби керування інформаційними потоками; імпорт інформації; захист інформації при передаванні внутрішніми каналами; знищення залишкової інформації; відкіт; контроль цілісності інформації в процесі зберігання; захист внутрішньосистемного передавання інформації при використанні зовнішніх каналів; цілісність внутрішньосистемного передавання інформації при використанні зовнішніх каналів.

К. ФВБ: ідентифікація і автентифікація /к. ФТБ: идентификация и аутентификация/ [с. FIA: Identification and Authentication] — клас ФВБ, що включає наступні розділи ФВБ: реакція на невдалі спроби автентифікації; атрибути безпеки користувачів; автентифікаційні параметри; автентифікація користувачів; ідентифікація користувачів; відповідність користувачів і суб'єктів.

К. ФВБ: керування безпекою /к. ФТБ: управление безопасностью/ [с. FMT: security ManegemenT] — клас ФВБ, що включає наступні розділи ФВБ: керування засобами захисту; керування атрибутами безпеки; керування параметрами і конфігурацією засобів захисту; відкликання атрибутів безпеки; обмеження терміну дії атрибутів безпеки; адміністративні ролі.

К. ФВБ: контроль доступу до системи /к. ФТБ: контроль доступа к системе/ [с. FTA: TOE Access] — клас ФВБ, що включає наступні розділи ФВБ: обмеження на використання атрибутів безпеки; обмеження числа одночасних сеансів; блокування сеансу роботи із системою; об'яви, попередження, запрошення і підказки; протокол сеансів роботи із системою; керування сеансами роботи із системою.

К. ФВБ: контроль за використанням ресурсів /к. ФВБ: контроль за использованием ресурсов/

[с. FRU: Resource Utilisation] — клас ФВБ, що включає наступні розділи ФВБ: стійкість до відмов; розподіл ресурсів на основі пріоритетів; квотування ресурсів.

К. ФВБ: конфіденційність роботи в системі /к. ФТБ: конфиденциальность работы в системе/ [с. FPR: PRivacy] — клас ФВБ, що включає наступні розділи ФВБ: анонімність користувачів; використання псевдонімів; анонімність сеансів роботи з системою; захист від моніторингу сеансів роботи із системою.

К. ФВБ: криптографія /к. ФТБ: криптография/ [с. FCS: Cryptographic Support] — клас ФВБ, що включає наступні розділи ФВБ: керування ключами; криптографічні засоби.

К. ФВБ: надійність засобів захисту /к. ФТБ: надежность средств защиты/ [с. FPT: Protection of the TSF] — клас ФВБ, що включає наступні розділи ФВБ: тестування апаратно-програмної платформи; захист від збоїв; готовність засобів захисту до обслуговування віддалених клієнтів; конфіденційність інформації, що передається, при роботі з віддаленими клієнтами; цілісність інформації, що передається, при роботі з віддаленими клієнтами; захист внутрішніх каналів інформаційного обміну між засобами захисту; фізичний захист; безпечне відновлення після збоїв; розпізнавання повторного передавання інформації та імітація подій; моніторинг взаємодій; розподіл доменів; синхронізація; час; погодженість обміну інформацією між засобами захисту; реплікація інформації, що використовується засобами захисту; самотестування засобів захисту.

К. ФВБ: причетність до приймання/передавання /к. ФТБ: причастность к приему/передаче/ [с. FCO: COmmunication] — клас ФВБ, що включає наступні розділи ФВБ: попередження відмови від факту передавання інформації; попередження відмови від факту приймання інформації.

К. ФВБ: пряма взаємодія /к. ФТБ: прямое взаимодействие/ [с. FTP: Trusted Path/channels] — клас ФВБ, що включає наступні розділи ФТБ: пряма взаємодія між засобами захисту; пряма взаємодія між користувачами.

КЛАСИФІКАТОР /классификатор/ [classifier] — систематизоване зведення найменувань класифікаційних груп та їхніх кодових позначень. К. є одним з основних засобів забезпечення автоматизованих інфор-

маційних систем лінгвістичних.

КЛАСИФІКАЦІЯ /классификация/ [classification] (від лат. classis — розряд, клас і facio — роблю) — процес розподілу об'єктів (предметів, явищ, процесів, понять) за класифікаційними групами у відповідності з певними ознаками.

К. інформації /к. информации/ [information c.] — процес віднесення відселектованої інформації (див. селекція інформації) до конкретної відомості кадастру інформаційного.

КЛІЄНТ /клиент/ [client, customer] (від лат. cliens [clientis] — підопічний) — 1) Особа, що доручила ведення своєї справи адвокатові, нотаріусові тощо. 2) Постійний відвідувач, замовник тощо. 3) Спеціальне програмне забезпечення користувача Інтернету. Див. також клієнт поштовий.

К. поштовий /к. почтовый/ — програма, яку використовує користувач для написання, читання, прийому, відправлення й інші операції з листами. За допомогою цієї програми користувач підключається і працює з поштовими і News-серверами.

КЛЮЧ /ключ/ [key] — 1) Пристрій для відкривання замка. 2) Сукупність символів, що використовується для ідентифікації елемента множини, наприклад,запису у файлі або запису бази даних (в індексно-послідовному файлі або в базі даних К. є обов'язковим елементом запису). 3) Сукупність символів, що використовується для підтвердження повноважень на доступ до деякої інформації. 4) У криптології — сукупність даних, які визначають вибір конкретного перетворення з усієї множини перетворень, які реалізуються шифром. 5) У прикладній криптології — символ або група символів (або електричний чи механічний прилади, що трактуються як символи), які управляють операціями зашифровування та розшифровування. 6) Послідовність символів (або їхніх електричні чи механічні еквіваленти) в автоматичних чи автоматизованих криптосистемах, які змішуються з відкритим текстом для вироблення шифртексту. 7) Синонім для всього ключового матеріалу або синхропосилок (cryptovariable). 8) Послідовність випадкових чи псевдовипадкових біт, які використовуються для ініціалізації та періодичної зміни операцій в криптографічних пристроях, які використовуються для шифрування, розшифрування, автентифікації інформації або для

генерації інших ключів.

К. виробництва ключів /к. производства ключей/ [key production k.] —- ключ, який використовується в процесі генерації інших ключів.

К. відкритий /к. открытый/ [public k.] — ключ, призначений для виконання перетворення криптографічного будь-яким елементом криптосистеми асиметричної. Обернене криптографічне перетворення може бути виконано тільки з застосуванням відповідного ключа приватного.

К. головний /к. главный/ [major k., master k.] — ключ, що знаходиться на найвищому рівні ієрархії в ієрархічних схемах керування ключами. Застосовується як ключ шифрування ключів, в той час як для його захисту уже не можливо застосовувати методи захисту криптографічні. Звичайно, розповсюджується ручним способом, захищається фізичними або організаційними методами захисту та відноситься до довгострокових ключів. Інша назва — майстер-ключ.

К. груповий /к. груповой/ [group k.] — ключ, спільний для групи абонентів системи.

К. даних /к. данных/ [data k.] — ключі, які використовуються для операцій криптографічного перетворення над даними користувача. В системі зв'язку це, звичайно, короткострокові або ключі сеансові, однак особисті ключі криптосистем асиметричних, які використовуються для підпису цифрового є, звичайно, довгостроковими ключами.

К. до механічного замка /к. к механическому замку/ [mechanical k.] — пристрій для управління механізмом замка. Буває з індивідуальним або груповим (для певної серії замків) секретом. К. ставить сувальди і пружини в таке положення, щоб стало можливим пересування ригеля. Кожний ключ роблять такої форми, щоб утруднити підробку.

К. довгостроковий /к. долговременный/ [long-lived k., long-term k.] — ключ, криптоперіод якого має відносно велике значення. До к. д., звичайно, відносяться майстер-ключі, ключі шифрування ключів, деякі ключові параметри криптоалгоритмів (наприклад, вузли заміни шифру ГОСТ 28147-89), відкриті ключові параметри схем формування ключів, ключі шифрування даних, які зберігаються в базах даних тощо. Від-

несення ключів до довгострокових здійснюється згідно з принципами керування ключами в системі зв'язку та прийнятої стратегії безпеки в системі автоматизованої.

К. еквівалентні /к. эквивалентные/ [equivalent k.] — ключі, відмінні один від одного, для яких даний криптоалгоритм для будь-якої (або майже будь-якої) пари однакових вхідних текстів породжує однакові криптограми. У симетричних критпоалгоритмах це може трапитися, наприклад, в тому випадку, коли в процесі розширення ключа або утворення ключів циклових із різних ключів отримуються однакові значення. При побудові криптоалгоритму намагаються уникнути або зменшити кількість к. е., оскільки вони зменшують простір ключовий шифру.

К. захисту /к. защиты/ [protection k.] — код, який присвоюється програмі і повинен збігатися з ключами захисту пам'яті всіх блоків, що виділені програмі.

К. захисту пам'яті /к. защиты памяти/ [storage protection k.] — код, який присвоюється блоку пам'яті, що виділений програмі, і використовується при зверненні програми до пам'яті з метою її захисту. К. з. п. повинен збігатися з ключем захисту; у противному випадку завдання завершується в аварійному режимі.

К. керування доступом /к. управления доступом/ [access control k.] — ключ, що пред'являється процесом системі керування базами даних і порівнюється нею з відповідним замком з метою запобігання несанкціонованому доступу до даних.

К. комплементарні /к. комплементарные/ [complementary k-s] — пара ключів для виконання зашифровування та розшифровування.

К. короткостроковий /к. кратковременный/ [short-term k.] — ключ, криптоперіод якого має відносно невелике значення.

К. приватний /к. собственный/ [private k.] (лат. privatus — особистий) — ключ, призначений для перетворення криптографічного у криптосистемі асиметричній, виключно тим її елементом, який є власником цього ключа. Зворотне криптографічне перетворення може бути виконане із застосуванням відповідного

ключа відкритого.

К. сеансовий /к. сеансовый/ [session k.] — криптографічний ключ, який використовується тільки під час одного сеансу зв'язку. Після закінчення сеансу зв'язку знищується або виводиться з використання.

К. секретності /к. секретности/ [privacy k.] — ключ, значення якого система обчислювальна використовує для визначення того, чи повинен ресурс захищений бути доступним тому процесові, який видав дане значення ключа.

К. системний /к. системный/ [system k.] — ключ, що забезпечує захист системних засобів від доступу несанкціонованого.

К. скомпрометований /к. скомпрометированный/ [compromised k.] — ключ, конфіденційність або цілісність якого порушена.

К. слабкі /к. слабые/ [weak k-s] — специфічні ключі, які зменшують стійкість даного шифру (або складність шифру (cipher complexity)) порівняно з іншими ключами. Для шифру DES існує 4 к. с., які генерують однакові підключі для всіх циклів; 12 так званих напівслабких ключів (semi-weak keys), які генерують тільки два різних підключі та незначну кількість напівслабких ключів (demi-semi-weak keys), які у свою чергу генерують чотири різних підключі. Незважаючи на дуже незначну кількість к. с. серед усіх 2^{56} ключів DES, їх треба відкидати при генеруванні ключів. Якщо для шифру не існує к. с., то говорять про лінійний простір ключовий шифру. Це, наприклад, заявлено для шифру SkipJack та шифру MARS.

К. сполучені /к. сопряженные/ [matched k-s] — ключі зашифровування та розшифровування.

К. цикловий /к. цикловый/ [round k.] — ключ, який використовується на кожному циклі шифрування в симетричному блочному алгоритмі шифрування, побудованому за схемою Фейстела. Виробляється за певним правилом із ключа шифрування.

К. шифрування ключів /к. шифрования ключей/ [key-encryption-k.] — ключі, який використовується в транспорту інших ключів див. транспортування ключів або захисту інших ключів, що зберігаються в

системі інформаційній.

К.-автоключ /к.-автоключ/ [key-auto-k.] — див. шифр автоключа.

КОГНІТАРІАТ /когнитариат/ [cognitariat] (англ. cognition — пізнання) — слово для позначення нової суспільної сили — інтелектуалів, від знань яких будуть залежати майбутні долі суспільства інформаційного і цивілізації у цілому.

КОГНІТОЛОГІЯ /когнитология/ [cognitology] (англ. cognition — пізнання) — група наукових дисциплін, що займаються вивченням та моделюванням процесів пізнання. До них відносяться когнітивна психологія, інтелект штучний, філософія пізнання, лінгвістика і нейрофізіологія.

КОД /код/ [code] (франц. code, від лат. codex — звід законів) — 1) Система символів для передавання, оброблення й зберігання (запам'ятовування) інформації. 2) Множина слів (кодових комбінацій) в деякому алфавіті, поставлена у взаємно-однозначну відповідність іншій множині (що кодується). 3) Ключ до способу зашифровування чи розшифровування тексту (див. шифр). 3) Позначення об'єкта обліку знаком або системою знаків за правилами, встановленими певною системою кодування. 4) Програма на машинній мові.

К. ASCII — американський стандартний код для обміну інформацією (від American Standard Code for Information Interchange).

К. ISO /к. ISO/ — стандартний символьний код обміну інформацією, в якому кожний символ кодується сімома бітами (від International Organization for Standartization). Використовується для обміну даними між основною пам'яттю ЕОМ і зовнішніми пристроями і для передавання даних лініями зв'язку.

К. m із n /к. m из n/ [m-out-of-n c.] — надмірний код, в якому для кодування кожного символу використовується n двійкових розрядів, із яких m завжди мають значення 1, а усі решта — 0. Те ж, що код з постійною вагою.

К. автентифікації /к. аутентификации/ [authentication c.] (від лат. identicus — тотожний і ... і лат. ... ficatio, від facio — роблю) — контрольне поле, що додається до блока даних для автентифікації повідомлень.

Прикладом коду автентифікації є код автентифікації повідомлень (MAC).

К. Айкена /к. Айкена/ [Aiken c.] — спосіб двійкового кодування десяткових цифр, при якому код цифр 0–4 співпадає з двійковим кодом чисел 0–4, а код цифр 5–9 — з двійковим кодом чисел 11–15 відповідно.

К. алфавітно-цифровий (буквено-цифровий) /к. алфавитно-цифровой (буквенно-цифровой/ [alphanumeric c.] — код, набір знаків якого складається з букв, цифр та інших знаків.

К. Бодо /к. Бодо/ [Baudot c.] — п'ятиелементний код, призначений для передавання букв, цифр і інших знаків по каналах зв'язку телеграфного.

К. внутрішній /к. внутренний/ [internal c.] — код подання даних, прийнятий для окремого пристрою або групи пристроїв ЕОМ.

К. Грея /к. Грэя/ [Gray c.] — двійковий код рефлексивний, кодові комбінації якого одержують за наступними правилами: кодова комбінація коду двійкового натурального складається з такою ж комбінацією зсунутою вправо на один розряд, при цьому молодший розряд зсунутої комбінації відкидається.

К. двійковий /к. двоичный/ [binary c.] — код з основою 2. Алфавітом коду є цифри 0 і 1. Використовується для подання даних в ЕОМ.

К. двійковий з виправленням помилок /к. двоичный с исправлением ошибок/ [binary error-correction c.] — код двійковий, надмірність якого забезпечує автоматичне виявлення і виправлення помилок деяких типів в даних, що передаються.

К. двійковий з виявленням помилок /к. двоичный с обнаруженим ошибок/ [binary error-detecting c.] — код двійковий, надмірність якого забезпечує автоматичне виявлення помилок деяких типів в даних, що передаються.

К. двійковий натуральний /к. двоичный натуральный/ [natural binary c.] — зважений код, комбінації якого одержують при піднесенні числа 2 до степенів із натуральними показниками.

К. двійковий обміну інформацією (ДКОІ) /к. двоичный обмена информацией (ДКОИ)/ — код

двійковий восьмибітовий, призначений для внутрішнього оброблення і вводу-виводу символьних даних.

К. двійково-десятковий /к. двоично-десятичный/ [binary decimal c.] — представлення чисел, при якому кожна десяткова цифра записується чотирьохбітовим двійковим еквівалентом. Використовується для операцій над цілими числами великої розрядності.

К. двійково-десятковий для обміну розширений /к. двоично-десятичный для обмена расширенный/ [EBCDIC] — міжнародний восьмибітовий код, що використовується для подання двійково-десяткових даних при вводі-виводі інформації (від Extended Binary-Coded Decimal Interchange Code).

К. достовірності /к. достоверности/ [Message Authentication Code (MAC)] — результат застосування до повідомлення варіанта хеш-функції з ключем. Найчастіше в ролі такої функції виступає алгоритм DES в режимі зчеплення блоків або алгоритм ГОСТ 28147-89 в режимі вироблення імітовставки.

К. з виправленням помилок /к. с исправлением ошибок/ [error-correcting c.] — див. код двійковий з виправленням помилок і код Хемінга.

К. з виявленням помилок /к. с обнаруженим ошибок/ [error-checking (error-detecting, self-checking) c.] — див. код двійковий з виявленням помилок.

К. з контролем на парність /к. с контролем на четность/ [parity-check c.] — двійковий код, в якому до кожної комбінації кодової приєднується додатковий контрольний розряд, що допомагає зберегти прийняту в системі одну і ту ж парність двійкових блоків.

К. з мінімальною відстанню /к. с минимальным расстоянием/ [minimum-distance c.] — код, в якому перехід від одного допустимого значення до наступного супроводжується мінімальними змінами в комбінації кодовій. Дозволяє виявляти в даних, що передаються, тільки поодинокі помилки.

К. з надмірністю /к. с избыточностью/ — те ж, що код надмірний.

К. з постійною вагою /к. с постоянным весом/ [constant ratio c.] — код, в якому всі знаки являють комбінації двійкових цифр, що мають постійне співвідношення нулів і одиниць.

К. завадостійкий /к. помехоустойчивый / — те ж, що код з виправленням помилок, код коректуваль-

ний.

К. захисту файла /к. защиты файла/ [file c.] — в операційній системі UNIX — ціле число, біти якого описують клас файла і право доступу користувача до нього.

К. збалансований /к. сбалансированный/ [balanced c.] — код в цифровій лінії передавання, в якому сума значень n рівнів сигналу має скінченні значення.

К. зважений /к. взвешенный/ [weighted c.] — код подання чисел, в якому кожній позиції присвоєна певна вага.

К. змінної довжини /к. переменной длины/ [variable-length c.] — 1) Код, в якому фіксоване число символів вихідного повідомлення кодується в змінне число вихідних символів. 2) Код із змінною довжиною комбінації кодової.

К. КОІ-7 /к. КОИ-7/ — двійковий семибітовий код обміну інформацією між ЕОМ і зовнішніми носіями інформації і передавання даних лініями зв'язку.

К. КОІ-8 /к. КОИ-8/ — двійковий восьмибітовий код обміну інформацією між ЕОМ і зовнішніми носіями інформації.

К. контрольний /к. контрольный/ [check c.] — код, який дозволяє автоматично виявляти, локалізувати і виправляти помилки в даних, що передаються.

К. коректувальний /к. корректирующий/ [correcting c.] — код, який дозволяє виявляти і виправляти помилки при передаванні і обробленні інформації. Див. також код з виправленням помилок.

К. криптографічний /к. криптографический/ [cryptic c., cryptographic c.] — одна з форм шифру заміни, яка оперує зі смисловими одиницями тексту. При цьому останні замінюються кодовими термінами.

К. ланцюговий (згортковий) /к. цепной (сверточный)/ [chain c.] — код, послідовні значення якого можуть бути одержані циклічною перестановкою груп двійкових розрядів слова, що кодується.

К. машинний /к. машинный/ [computer (machine) c.] — 1) Код двійковий, що використовується для кодування машинних команд за правилами, передбаченими в даному типі ЕОМ. 2) Програма на машинній

мові.

К. надмірний /к. избыточный/ [redundant c.] — 1) Код, що має більшу кількість кодових комбінацій, ніж це потрібно для кодування символів повідомлень. Додаткові кодові комбінації можуть використовуватися для контролю правильності передавання даних або для кодування нової інформації. 2) Код, комбінації якого містять більшу кількість розрядів, ніж це потрібно для кодування символів алфавіту. Надмірні розряди використовуються для виявлення (виправлення) помилок.

К. незвідний /к. неприводимый/ [irreducible c.] — код, в якому комбінації кодові будуються так, що ні одна з них не є початком іншої, більш довгої.

К. необоротний /к. необоротный/ [irreversible c.] — код, при використанні якого неможливо повністю відновити текст, що передається, в його початковому вигляді.

К. нерівномірний /к. неравномерный/ — код, комбінації кодові якого мають неоднакову довжину. Див. також код змінної довжини.

К. нероздільний /к. неразделимый/ — код надмірний, у якому інформаційна й контрольна частини представлені в неявному вигляді.

К. обернений (інверсний) /к. обратный (инверсный)/ [inverse c.] (від лат. inversio — перегортання, перестановка) — код двійковий для відображення від'ємних чисел у вигляді порозрядного доповнення до найбільшого значення в даній системі подання чисел.

К. обміну інформацією /к. обмена информацией/ — див. коди ASCII, ДКОІ, ISO, KOI-7, KOI-8.

К. оборотний /к. обратимый/ [reversible c.] — код, в якому існує взаємно-однозначна відповідність між повідомленнями, що кодуються, і комбінаціями кодовими, що їх відображають.

К. оптимальний /к. оптимальный/ [optimum c.] (від лат. optimus — найкращий) — код, при використанні якого по каналу зв'язку за фіксований відрізок часу передається максимальна кількість інформації.

К. пароля /к. пароля/ [password c.] — пароль, позначений системою знаків за правилами, встановленими вибраною системою кодування. При виборі к. п. виходять з того якою повинен бути його розмір

(довжина паролю), стійкість до несанкціонованого підбору та способи застосування.

К. передавання /к. передачи/ [transmission c.] — код, що використовується для кодування інформації, що передається лініями зв'язку.

К. поліноміальний /к. полиномиальный/ [polynomial c.] — код з виправленням помилок, в якому контрольні розряди є остачею від ділення на поліном, який називається утворюючим.

К. постійної довжини /к. постоянной длины/ [fixed-length c.] — код рівномірний, код з постійною довжиною комбінації кодової.

К. префіксний /к. префиксный/ [prefix c.] — код, що складається зі слів різної довжини, причому ніякий більш короткий код не є початком (префіксом) більш довгого.

К. прозорий /к. прозрачный/ [transparent c.] — код, який допускає інверсію символів, що надходять на вхід декодера.

К. прямий /к. прямой/ [direct c.] — код двійковий подання чисел, в якому незалежно кодуються знак і значення числа.

К. рефлексивний /к. рефлексивный/ [reflexive c.] (від лат. reflexio — вигин, відображення) — код двійковий, в якому комбінації, що відповідають сусіднім числам, відрізняються тільки в одному розряді.

К. рівномірний /к. равномерный/ [equal-length (constant-length) c.] — код, в якому всі комбінації кодові мають однакову довжину. Див. також код постійної довжини.

К. самоконтролюючий /к. самоконтролируемый/ [selfcheching c.] — код надмірний, декодування якого автоматично приводить до виявлення помилок.

К. семантичний /к. семантический/ [semantic c.] (від грец. $\sigma\eta\mu\alpha\nu\tau\iota\kappa\acute{o}\varsigma$ — означальний) — складна семантична система, яка з достатньо великим наближенням моделює зміст мови природної.

К. телеграфний міжнародний /к. телеграфный международный/ — те ж, що код Бодо.

К. унітарний /к. унитарный/ [unitary c.] (франц. unitaire, від лат. unitas — єдність) — код, що скла-

дається з однієї цифри, що повторюється необхідне число разів.

К. Хаффмена /к. Хаффмена/ [Huffman c.] — код префіксний, в якому довжина комбінації кодової обернено пропорційна частоті появи елемента, що кодується (чим частіше зустрічається елемент, тим коротша кодова комбінація).

К. Хеммінга /к. Хэмминга/ [Hamming c.] — код з мінімальною надмірністю, що забезпечує виправлення поодиноких помилок.

К. циклічний /к. циклический/ [cyclic c.] (від грец. *κύκλøς* — круг, коло, круговерть) — лінійний код, в якому якщо w є словом коду, то кодовими словами будуть і всі результати циклічного зсуву w.

К. цифровий /к. цифровой/ [numeric c.] — код, набір знаків якого містить тільки цифри.

КОДЕК /кодек/ [endec] — блок апаратури цифрового передавання мовних сигналів по телефонних каналах (кодер-декодер).

КОДЕР /кодер/ [coder] — 1) Те ж, що кодувальний пристрій. 2) Програміст, який складає програми за готовими детальними специфікаціями.

КОДУВАННЯ /кодирование/ [coding, encoding] — 1) Операція ототожнення символів чи груп одного коду із символами чи групами символів іншого коду. 2) Ототожнення даних з їхніми комбінаціями кодовими; установлення відповідності між елементом даних та кодовою комбінацією (словом коду). 3) Процес присвоєння кодового позначення (коду) об'єкта обліку.

К. блочне /к. блочное/ [block c.] — спосіб кодування, при якому кожний блок, що передається, кодується окремо.

К. буквене /к. буквенное/ [alphabetic c.] — кодування даних, при якому кодові комбінації складаються тільки з букв деякого алфавіту.

К. буквено-цифрове /к. буквенно-цифровое/ [alpha-numeric c.] — кодування даних, при якому кодові

комбінації складаються з букв, цифр та інших знаків деякого алфавіту.

К. даних /к. данных/ [data c.] — див. кодування.

К. двійкове /к. двоичное/ [binary e.] — 1) Процес подання символів алфавіту у вигляді ланцюжка двійкових знаків. 2) Кодування числа у вигляді двійкового ланцюжка, в якому і-тий біт, починаючи з кінця, має вагу 2.

К. двійково-десяткове /к. двоично-десятичное/ [binary-to-decimal notation] — спосіб кодування десяткових чисел, при якому кожна цифра представляється чотирма двійковими розрядами (двійковою тетрадою).

К. з надмірністю /избыточное к./ [redundant c.] — кодування з допомогою коду надмірного.

К. інформації /к. информации/ [information c.] — перетворення інформації у вигляді умовних сигналів з метою автоматизації її зберігання, оброблення, передавання і вводу-виводу.

К. логічне /к. логическое/ [logical c.] — процес подання символів алфавіту послідовностями логічних значень.

К. манчестерське /к. манчестерское/ [manchaster c.] — в системах передавання даних — спосіб кодування, за допомогою якого сигнали даних і синхронізуючі сигнали об'єднуються в єдиний послідовний потік.

К. необоротне /к. необратимое/ [irreversible encryption] — кодування, при якому вихідні дані неможливо відновити, незважаючи на точне знання методу кодування.

К. оптимальне /к. оптимальное/ [optimal c.] (від лат. optimus — найкращий) — 1) Кодування, що забезпечує оптимальні умови передавання повідомлень по даному каналу зв'язку. 2) Кодування, при якому елементарні символи в закодованому повідомленні зустрічаються в середньому з однаковою частотою.

К. цифрове /к. цифровое/ [digital c.] — кодування, при якому кодоване повідомлення записується у вигляді послідовності цифр і чисел.

КОЕФІЦІЄНТ /коэффициент/ [factor, ratio, coefficient] (від лат префікса co... і efficiens (efficientis) — той,

що виробляє) — 1) Сталий або відомий множник при іншій, звичайно, змінній або невідомій величині. 2) Відношення двох значень фізичної величини.

К. звукопоглинання /к. звукопоглощения/ [sound absorption c.] — відношення енергії звукових хвиль, поглинутої в матеріалі, до звукової енергії, що падає на поверхню матеріалу.

К. корисної дії антени /к. полезного действия а./ [antenna efficiency f.] — відношення потужності радіовипромінювання, що створюється антеною, до потужності сигналу радіочастотного, що підводиться до антени. Визначає втрати електричної енергії в антені.

К. підсилення антени /к. усиления антенны/ [antenna gain] — відношення потужності на вході еталонної антени до потужності, що підводиться до реальної антени, за умови, що обидві антени створюють в даному напрямку на однаковій відстані рівні значення напруженості поля або таку ж щільність потоку потужності. Визначається добутком коефіцієнта спрямованої дії антени на коефіцієнт корисної дії антени.

К. прямокутності амплітудно-частотної характеристики радіоприймача /к. прямоугольности амплитудно-частотной характеристики радиоприемника/ — відношення ширини смуги пропускання радіоприймача по рівню 0,707 до ширини смуги пропускання по рівню 0,1. Якщо коефіцієнт прямокутності визначається по відношенню до інших рівнів коефіцієнта підсилення, то це оговорюється окремо.

К. спрямованої дії антени /к. направленного действия антенны/ [antenna directivity f.] — відношення квадрата напруженості поля, що створюється антеною в даному напрямку, до середнього значення квадрата напруженості поля в усіх напрямках. Визначає величину енергетичного виграшу, який забезпечує спрямована антена у порівнянні з неспрямованою.

К. шуму радіоприймача /к. шума радиоприемника/ — значення, яке показує у скільки разів відношення сигнал/шум на вході приймача більше відношення сигнал/шум на виході лінійної частини приймача (на вході детектора). Для ідеального радіоприймача коефіцієнт шуму дорівнює 1.

КОЛІЗІЯ /коллизия/ [collision] (лат. collisio, від collido — стикаюся — 1) Зіткнення протилежних сил,

інтересів, прагнень. 2) Розходження між правовими нормами, що регулюють однакові правовідносини.

К. хеш-функції (клешня вкорочуючої функції) /к. хэш-функции (клешня укорачивающей функции)/ [collision] — пара різних повідомлень, для яких значення хеш-функції f є рівними, тобто для $M_1 \neq M_2$, $f(M_1) = f(M_2)$.

КОЛОНІАЛІЗМ /колониализм/ [colonialism] (франц. colonialisme, від лат. colonia — поселення) — політика гноблення та експлуатації за допомогою військового, політичного та економічного примусу інших країн.

К. культурний /к. культурный/ [cultural c.] — політика встановлення залежності населення слаборозвинених країн від агентств інформаційних великих держав, що виливають більшу частину усіх новин. Внаслідок к. к. виникають спотворення інформації про моральні, культурні або політичні цінності одних країн на противагу іншим. Захистом від к. к. є неодмінна демократизація інформаційних джерел і структур, що виражається в заснуванні національних інформаційних агентств і впровадженні механізмів для кооперування й взаємодопомоги країн, що розвиваються, а також скорочення монополії з метою рівноправного й справедливого використання усіх комунікативних засобів, включаючи супутники зв'язку.

КОМБІНАЦІЯ /комбинация/ [combination] (від лат. combinatio — поєднання) — взаємно зумовлене розташування чого-небудь.

К. кодова /к. кодовая/ [code c., code word] — слово коду; скінченна послідовність знаків алфавіту, поставлена у взаємно-однозначну відповідність кодованому значенню.

К. розрядів /к. разрядов/ [bit pattern] — сукупність двійкових розрядів, що створюють кодову комбінацію або маску.

КОМЕНТАР /комментарий/ [comment(ary)] (від лат. commenarium — записки. тлумачення)— 1) Тлумачення певного тексту або книги. 2) Вид програми радіомовлення, в якій приводиться думка (або декілька різних думок) фахівців, які розкривають суть проблеми. В к. фахівці висловлюють свої міркування у відповідності до того, що вони вважають важливим донести до слухачів і що відповідає меті психологічного

впливу. Розрізняють коментарі до подій і коментарі проблемні. Тривалість к. складає 4–6 хвилин.

К. до подій /к. к событиям/ — коментар, який дає оцінку тих чи інших подій.

К. проблемний /к. проблемный/ — коментар, який розглядає важливе для слухачів питання, досліджує широку панораму подій, дії уряду або командування противника, глибоко аналізує факти.

КОМП'ЮТЕР /компьютер/ [computer] (англ. computer, від лат. computo — рахую, обчислюю) — електронна обчислювальна машина. Див. ЕОМ.

К. базовий /к. базовый/ [base c.] — основний (вихідний) комп'ютер сімейства ЕОМ. Решта машин даного сімейства є розвитком базового.

К. персональний /к. персональный/ — див. ЕОМ персональна.

КОМПЛЕКС /комплекс/ [complex] (від лат. complexus — поєднання, зв'язок) — 1) Сукупність предметів чи явищ, що становлять єдине ціле. 2) Два чи більше вироби, не з'єднаних на підприємстві-виробнику складальними операціями, але призначені для виконання взаємозв'язаних експлуатаційних функцій.

К. засобів і механізмів захисту /к. средств и механизмов защиты/ — організаційні, технічні, програмні, соціальні, правові та інші засоби і механізми, що забезпечують локалізацію, запобігання і ліквідацію загроз інформаційній безпеці особистості, суспільства, держави.

К. засобів автоматизації (КЗА) /к. средств автоматизации (КСА)/ — територіально-зосереджений комплекс апаратних і програмних засобів, що виконують спільне завдання автоматизованого оброблення інформації: система обчислювальна , вузол комутації, пункт абонентський, система телеоброблення даних і т. ін.

К. засобів захисту (КЗЗ) /к. средств защиты (КСЗ)/ [trusted computing base (TCB)] — 1) Сукупність програмних і технічних засобів, що створені і підтримуються для забезпечення захисту засобів обчислювальної техніки або автоматизованих систем від доступу несанкціонованого до інформації. 2) Сукупність програмно-апаратних засобів, в тому числі програм пристроїв запам'ятовуючих постійних, які забезпечують реалізацію політики безпеки інформації. У системі комп'ютерній будь-який її компонент, який вна-

слідок якого-небудь впливу здатний спричинити порушення політики безпеки, повинен розглядатися як частина КЗЗ.

К. засобів зв'язку /к. средств связи/ — сукупність організаційно, функціонально та конструктивно взаємопов'язаних засобів зв'язку.

К. засобів радіоперехоплення /к. средств радиоперехвата/ — сукупність організаційно, функціонально та конструктивно взаємопов'язаних засобів, призначених для виявлення, приймання та реєстрації радіовипромінювання і добування з них семантичної інформації, ознак сигналів демаскуючих і формування зображень об'єктів при перехопленні сигналів телевізійних або факсимільних. Типовий к. з. р. включає: приймальні антени; радіоприймач; аналізатор технічних характеристик сигналів (див. аналіз сигналів технічний); радіопеленгатор; пристрої реєструючі.

К. обчислювальний (багатомашинний обчислювальний) (ОК) /к. вычислительный (многомашинный вычислительный) (ВК)/ [computer (multiple computer) с.] — сукупність двох або більше ЕОМ, що працюють як єдина система.

К. приймальні спеціальні /к. приемные специальный/ — апаратно-програмні засоби на основі радіоприймачів і ПЕОМ, обладнаних апаратними засобами оброблення сигналів, призначені для перехоплення радіосигналів із складною структурою, які застосовуються у стільниковому, пейджинговому та інших видах мобільного зв'язку, а також для перехоплення факсимільних передач, побічного випромінювання ПЕОМ тощо.

К. радіоконтролю автоматизований /к. радиоконтроля автоматизированный/ — апаратно-програмний комплекс на основі приймачів скануючих і ПЕОМ, призначений для швидкого панорамного аналізу радіочастотного спектра в діапазоні частот.

К. радіомоніторингу приміщень автоматизовані /к. радиомониторинга помещений автоматизированные/ — комплекси радіоконтролю автоматизовані, призначені для пошуку засобів несанкціонованого зняття акустичної інформації. Типовий комплекс включає: скануючий приймач із широкосмуговими анте-

нами; комутатор антен для комплексів, що контролюють декілька приміщень; комп'ютер або мікропроцесор; спеціальне програмне забезпечення комплексу; контролер вводу інформації з виходу радіоприймача в комп'ютер і формування тестового сигналу; перетворювач спектра, акустичний корелятор. Комплекс при мінімальній участі оператора визначає і запам'ятовує рівні й частоти радіосигналів у контрольованому приміщенні, виявляє в результаті кореляційного оброблення спектрограм нові випромінювання, із використанням тестового акустичного сигналу розпізнає потай встановлені в приміщенні радіомікрофони і визначає їхні координати. Можливості комплексу можна розширити, якщо включити до його складу блок контролю проводових ліній, що дозволяє виявляти підслуховуючі пристрої, приєднані до кабелів.

К. телевізійного спостереження /к. телевизионного наблюдения/ — сукупність засобів телевізійної техніки, призначених для дистанційного спостереження рухомих об'єктів. До складу к. т. с. входить відеокамера з передавачем телевізійного радіосигналу (відеопередавачем) та телевізійний приймач. Для запису зображення рухомих об'єктів використовуються відеомагнітофон. Основними характеристиками к. т. с. є чутливість передавальної трубки (пристрою із зарядовим зв'язком) відеокамери та її роздільна здатність. Чутливість визначається чутливістю матеріалу фотокатода (мішені), а розділення — кількістю рядків розкладення зображення. Сучасні передавальні телевізійні трубки мають чутливість, що забезпечує телевізійне спостереження об'єктів при їхній освітленості від сотих часток до десятків тисяч люксів. Роздільна здатність сучасних к. т. с. складає 350–650 ліній. Чим вище розділення, тим менша тривалість сигналу елемента зображення і тим ширший спектр телевізійного сигналу. Ширина спектра телевізійного відеосигналу, що передається з частотою кадрів 25 Гц і розділенням в 625 ліній, складає 6(5; 5,5) МГц, телевізійного радіосигналу (каналу) — 8 МГц. Для телевізійного спостереження в інфрачервоному діапазоні застосовують к. т. с. з телевізійними камерами з приладами з зарядовим зв'язком, які є чутливими до інфрачервоних променів. З метою забезпечення потайного спостереження передавальна частина к. т. с. камуфлюється під побутові прилади або особисті речі.

К. технічних засобів /к. технических средств/ [hardware] — 1) Сукупність організаційно, функціо-

нально та конструктивно взаємопов'язаних технічних засобів. 2) В системах інформаційно-обчислювальних сукупність засобів обчислювальної техніки: ЕОМ, зовнішніх пристроїв, терміналів, ліній зв'язку, які забезпечують технічний процес підготовки (добування), зберігання, обробки і передавання інформації.

К. технічних засобів охорони /к. технических средств охраны/ — сукупність взаємопов'язаних технічних засобів охорони, призначених для вирішення певної групи задач у системі охорони об'єкта. До структури типового комплексу ТЗО автономної системи охорони входять: охоронні та пожежні сигналізатори (датчики); шлейфи сигналізації; прилади приймально-контрольні; звукові та світлові сигналізатори. В системах централізованої охорони передбачена можливість автоматичного передавання на пункт централізованої охорони сигналів тривоги і сповіщень про працездатність з приймально-контрольного пункту (комплексів охоронно-пожежної сигналізації) або безпосередньо від сигналізаторів каналами проводового зв'язку або радіоканалами.

КОМПЛЕКСУВАННЯ /комплексирование/ [complexing] — об'єднання в єдине ціле сукупності предметів чи явищ.

К. засобів обчислювальної техніки /к. средств вычислительной техники/ — комплекс робіт, спрямований на формування конфігурації системи обчислювальної, що відповідає завданню замовника. Виконується шляхом компонування і взаємоув'язки технічних і програмних засобів та розробки документації технічної.

К. каналів витоку інформації /к. каналов утечки информации/ — комплексне використання каналів витоку інформації, засноване на наступних принципах: канали, що комплексуються, доповнюють один одного за своїми можливостями; ефективність комплексування підвищується при зменшенні залежності між джерелами інформації каналів і ознаками демаскуючими в різних каналах. К. к. в. і. забезпечує: збільшення ймовірності виявлення і розпізнавання об'єктів за рахунок розширення їхніх поточних структур ознакових; підвищення вірогідності інформації семантичної і точності вимірювання ознак, особливо у випадку добування інформації з недостатньо надійних джерел. Коли виникають сумніви у вірогідності

інформації, то з метою виключення дезінформації, одержані відомості і дані повторно перевіряють іншим каналом. Можливі два основних види к. к. в. і. — забезпечення витоку інформації від одного джерела декількома паралельно функціонуючими каналами (комплексування каналів витоку інформації паралельне) і від різних джерел (комплексування каналів витоку інформації від різних джерел).

К. каналів витоку інформації від різних джерел /к. каналов утечки информации от разных источников/ — комплексування каналів витоку інформації, що забезпечує можливість добування інформації від різних джерел, наприклад, з документів або від фахівців, що беруть участь у створенні цієї інформації. Знаходить застосування, коли джерела інформації не мають достовірної інформації або займаються дезінформацією. При комплексному використанні двох каналів імовірність впровадження дезінформації можна оцінити за формулою:

$$P_d = P_1 P_2 + r\sqrt{P_1(1-P_1)P_2(1-P_2)},$$

де P_1 і P_2 — значення ймовірності появи дезінформації в першому і другому каналах; r — коефіцієнт кореляції між інформацією в цих каналах. При r=1 каналами здійснюється витік інформації однакового змісту або про однакові ознаки, при r=0 — джерела незалежні. Для зменшення ризику одержання дезінформації необхідно зменшувати коефіцієнт кореляції між джерелами інформації.

К. каналів витоку інформації паралельне /к. каналов утечки информации параллельное/ — комплексування каналів витоку інформації, що забезпечує розповсюдження однієї і тієї ж інформації різними напрямками одним або різними носіями. Так як імовірність впливу завад в різних каналах на однакові елементи інформації мала, то в цьому випадку підвищується достовірність сумарної інформації після її оброблення у відповідному органі. При незалежності завад в n-каналах витоку інформації ураження одного і того ж елемента інформації при комплексуванні n каналів P_n розраховується за формулою:

$$P_n = \prod_{i=1}^{n} P_i,$$

де Pi — ймовірність ураження елемента інформації в і-тому каналі. Якщо джерело не має достовірної інформації або займається дезінформацією, то даний варіант комплексування не підвищує достовірність підсумкової інформації. Для забезпечення такої можливості використовується комплексування каналів витоку інформації від різних джерел.

КОМПЛЕКТ /комплект/ [kit, set] (від лат. completus — повний) — 1) Повний набір інструментів, інших предметів, що мають певне призначення. 2) Те ж, що й комплекс, але для виробів, що мають експлуатаційне призначення допоміжного характеру.

К. спорядження солдата-піхотинця з врахуванням вимог інформаційної війни /к. снаряжения солдата-пехотинца с учетом требований информационной войны/ — спорядження, яке забезпечує солдатові ефективність, захищеність, мобільність і автономність дій на полі бою. До складу комплекту повинні входити засоби ураження противника в ближньому бою, зв'язку і управління, забезпечення живучості і виживання. Такий комплект перетворює солдата в самостійну систему зброї. Найбільш перспективний проект к. с. передбачає інтеграцію в єдиний комплект п'яти основних підсистем: багатофункціонального захисного шолома, індивідуального комп'ютера і радіостанції, інтерфейсу із системами зброї, індивідуального захисту, мікроклімату і кондиціювання.

КОМПОЗИЦІЯ /композиция/ [composition] (від лат. compositio — складання, створення) — метод послідовного об'єднання об'єктів (процесів, явищ) в єдине ціле за певними правилами.

К. шифрів (добуток шифрів) /к. шифров (произведение шифров)/ — криптографічне перетворення, яке полягає у зашифровуванні тексту відкритого за допомогою одного шифру, а потім застосуванні до отриманого шифртексту послідовно ще одного чи декількох шифрів.

КОМПОНЕНТ /компонент/ [component] (від лат. componens (componentis) — той, що складає) — 1) Складова частина чогось. 2) Складова частина пристрою, програми, системи, даних.

К. навіюючого впливу операціональний /к. внушающего влияния операциональный/ — складова частина моделі навіюючого впливу, що описує вплив об'єкта. У складному акті взаємодії суб'єкта й об'єкта

виділяють два етапи: підготовчий і виконавчий. На підготовчому етапі суб'єкт впливу спочатку психологічно готує об'єкт до наступного сприйняття змісту навіювання, тобто знижує його опірність навіюванню і підвищує навіюваність. Для цього він використовує прийоми релаксації (психофізичного розслаблення), а також спирається на дещо життєво значиме для об'єкта навіювання, що укоренилося в його психіці. Потім суб'єкт "вводить" у психіку об'єкта і закріплює в ній необхідні йому зразки мислення, психічних станів, поведінки. Виділяють наступні якості суб'єкта, які дозволяють знизити опірність об'єкта до навіювання: авторитет суб'єкта; демонстрація доброзичливості суб'єкта до об'єкта; демонстрація психологічної переваги суб'єкта над об'єктом; демонстрація віри суб'єкта у зміст навіювання; емоційне подання змісту навіювання.

К. навіюючого впливу процесуальний /к. внушающего влияния процессуальный/ — складова частина моделі навіюючого впливу, що описує процес прийняття об'єктом змісту навіювання. В цілому цей процес скорочений порівняно з процесом переконування: в ньому функціонують тільки сприйняття й запам'ятовування, діяльність мислення "випадає" або ослабляється. Тобто, процес навіювання включає ненавмисне сприйняття і запам'ятовування без попереднього осмислення змісту навіювання. Особливо некритично навіюючий вплив сприймається тоді, коли в його змісті є посилання на довірче джерело, важливий документ, авторитетну особу і т.ін. В цьому випадку об'єкт навіювання сприймає цю чи іншу інформацію без використання свого інтелектуального механізму "аналіз-синтез".

К. навіюючого впливу результативний /к. внушающего влияния результативный/ — складова частина моделі навіюючого впливу, що описує реакцію у відповідь на навіюючий вплив. Суб'єкт навіюючого впливу завжди реагує на його зміст. Мета навіювання — вплинути на об'єкт таким чином, щоб його реакція відповідала меті психологічної операції. Для цього необхідно збільшити ступінь автоматизму реакції суб'єкта впливу у відповідь, яка у свою чергу залежить: від змісту навіювання (його складності, конкретності, особистої значимості і т. ін.); від психічного стану об'єкта навіювання (страх, депресія, апатія і деякі інші ситуативні стани, особливо в умовах війни, сприяють некритичному і неусвідомлюваному сприйняттю навіюючого впливу); від часового інтервалу між впливом і реакцією у відповідь (із збільшенням часового

інтервалу автоматизм реакцій у відповідь на навіюючий вплив зменшується, оскільки відбувається підсилення критичності і загальної розумової діяльності об'єкта).

КОМПРОМЕТАЦІЯ /компрометация/ [compromise] (від франц. compromromettre — знеславлювати, підривати репутацію) — порушення політики безпеки; несанкціоноване ознайомлення.

К. інформації /к. информации/ [information c.] — витік або розголошення інформації конфіденційної, чи одержання її неавторизованим користувачем.

КОМУНІКАБЕЛЬНІСТЬ /коммуникабельность/ [communicability] (франц. communicable — те, що з'єднується, від лат. communico — з'єдную, повідомляю) — здатність до спілкування, товариськість. В комунікативістиці к. характеризує суспільну природу засобів масової інформації і з цих позицій здійснюється критичний аналіз діяльності мас-медіа з наміром виявнити конкретні наслідки їхнього впливу на суспільне життя, на свідомість і психіку різних груп населення, а також на місце тих чи інших країн у публічній сфері простору інформаційного світового (глобального).

КОМУНІКАТИВІСТИКА /коммуникативистика/ [communicology, communication science] (ам.) — наука, що вивчає гуманітарні аспекти розвитку інформаційних засобів і систем, характер, форми й результати їхнього впливу на суспільне життя. Предметом дослідження к. є різні форми й засоби, функції і потенції інформаційно-соціальних зв'язків — від наскальних малюнків, ритуальних танців і барабанних мов первісних племен до комп'ютерного дизайну, відеодисків і телефаксів. Проте переважна увага приділяється найновішій фазі в розвитку інформаційних зв'язків і систем, коли головну роль генератора комунікацій масових взяли на себе автоматизовані аудіовізуальні засоби і лінії зв'язку, які створили нові форми й темпи розповсюдження новин і їхнього впливу на традиційні інформаційні дискурси (див. дискурсивний) разом з новими типами культури масової. Часто к. називають ще комунікологією й порівнюють її структуру з великою парасолькою, спицями якої поряд із журналістикою є стилістика, рекламознавство, театрознавство, теле- і радіомовлення, риторика та популярна культура. Опорне значення мають також інформатика і кібернетика, що встановлюють загальні закономірності формування й перетворення інформаційних зв'язків

за допомогою теоретичних концепцій і методів, які засновуються на точних статистичних даних і широкого застосування для досліджень комп'ютерної техніки з відповідним програмним забезпеченням.

КОМУНІКАТОР /коммуникатор/ [communicator] — 1) Особа або група осіб, які створюють і передають повідомлення. 2) Засіб масової інформації. 3) В техніці — механізм, що передає інформацію або переключає канали її передавання.

КОМУНІКАЦІЯ /коммуникация/ [communication] (від лат. communico — роблю загальним, поєдную) — 1) Дисципліна, що поєднує методи, пристрої та середовища для передавання інформації. 2) В інформатиці — передавання даних з одного комп'ютера до іншого через середовище комунікаційне, наприклад, телефонну чи мікрохвильову лінію, через космічний канал зв'язку або кабель. Є два основних методи у комп'ютерному зв'язку: тимчасовий зв'язок між комп'ютерами через модеми і постійний (або напівпостійний) — між станціями робочими в мережі. Апаратура і програми, що застосовуються у модемних комунікаціях, відмінні від тих, котрі використовуються у мережах, але зв'язані з ними. Комунікації "модем-модем" можуть використовувати телефонні лінії загального користування та інші подібні середовища як в одному, так і в обох напрямках зв'язку між комп'ютерами. В мережі більш широко використовують спеціалізовані телефонні лінії та комунікаційні системи, а у мережах обчислювальних локальних кабелі — "комп'ютер-комп'ютер". Через потенційно великі потоки інформації, у мережах також застосовують складне транспортне обладнання і процедури виявлення помилок, щоб обробляти чи передавати (приймати) повідомлення від санкціонованих користувачів. 3) В комунікативістиці — соціально-культурна взаємодія людей, груп і організацій, держав і регіонів за допомогою інформаційних зв'язків. К. інтерпретується в залежності від теоретичних позицій, інтересів і задач дослідників. Маклюенізм [macluhanism] висуває на перший план вивчення к. як технічних засобів зв'язку. Соціологічний напрям [sociological school] зосереджує увагу на комунікабельність інформаційних засобів міжособистістних, міжгрупових і міжнародних спілкувань (контактів). Концепції теологічного профілю акцентують значення к. для створення ком'юніті [community] — співтовариства людей, об'єднаних релігійною вірою й принципами релігійної етики. Теоретики семіотичного

напрямку [semiotic trend] займаються аналізом мовної атрибутики комунікаційно-інформаційних мов.

К. масова /к. массовая/ [mass c.] — процес встановлення зв'язку й передавання інформації групі людей одночасно за допомогою спеціальних засобів — мас-медіа. Виділяють п'ять основних особливостей цього процесу: масовість аудиторії; гетерогенність аудиторії; використання високошвидкісних і репродукційних засобів зв'язку й інформації; швидке розповсюдження інформації; відносно невелика споживча вартість інформації.

КОМУНІКОЛОГІЯ /коммуникология/ [communicology] — див. комунікативістика.

КОМУТАТОР /коммутатор/ [switch] (від лат. commuto — змінюю) — пристрій для комутації двох і більше пристроїв.

К. системи відеоконтролю /к. системы видеоконтроля/ — комутатор, призначений для приєднання декількох (4–16) камер телевізійних до одного монітора з послідовним переключенням в ручному або автоматичному режимах.

КОМУТАЦІЯ /коммутация/ [switching] (від лат. commutatio — зміна) — переключення, встановлення зв'язку.

К. автоматична /к. автоматическа/ [automatic s.] — комутація каналів або пакетів в мережі обчислювальній, яка здійснюється автоматично приладами зв'язку у відповідності з одержаною адресною інформацією.

К. віртуальних каналів /к. виртуальных каналов/ [virtual channel s.] — в обчислювальних мережах вид комутації, який поєднує переваги комутації пакетів і комутації каналів. З'єднання в основному здійснюються на рівні транспортному, а користувач звільнюється від необхідності контролювати послідовність проходження інформації мережею.

К. каналів (ліній зв'язку) /к. каналов (линий связи)/ [circuit (line) s.] — комутація, яка забезпечує приєднання каналів вторинної мережі електрозв'язку для створення каналу передавання даних.

К. пакетів /к. пакетов/ [packet s.] — 1) Комутація повідомлень даних, при якій повідомлення прийма-

ються, накопичуються і передаються у вигляді пакетів даних. 2) Метод динамічного розподілу комунікаційних ресурсів між взаємодіючими об'єктами.

К. повідомлень /к. сообщений/ [message s.] — комутація, при якій здійснюється приймання повідомлень даних, їхнього накопичення і наступне передавання.

К. цифрова /к. цифровая/ [digital s.] — комутація в мережі передавання даних, при якій з'єднання встановлюється виконанням операцій над цифровими сигналами без їхнього перетворення в аналогову форму.

К. часова /к. временная/ [time-division s.] — метод комутації каналів з часовим мультиплексуванням, що ґрунтується на розподілі комутованих даних різноманітних каналів по часових інтервалах усередині кадру.

КОМФОРТ /комфорт/ [comfort] (від англ. comfortable — зручний, затишний) — 1) Сукупність побутових вигод. 2) Стан, сприятливий для нормальної життєдіяльності організму.

КОНВЕРГЕНЦІЯ /конвергенция/[convergence] (лат. convergenttio, від convergo — сходжуся, наближаюся) — збіг ознак, властивостей у явищах, між собою не пов'язаних, незалежних.

К. в інформаційній індустрії технологічна /к. в информационной индустрии технологическая/ — конвергенція, викликана тим, що переведена в цифрову форму інформація може передаватися будь-якими засобами комунікацій — телефонними й кабельними лініями, через супутники, мобільний і безпроводовий зв'язок. Внаслідок технологічної конвергенції розпочалося розмивання границь між традиційно різними секторами індустрії інформаційної — комп'ютерною, телекомунікаційною, засобів масової інформації і т.ін. Див. також конвергенція галузей інформаційної індустрії. Технологічна конвергенція й можливість прориву на нові ринки привели до масових об'єднань компаній в двох напрямках: об'єднуються фірми, які зайняті виробництвом змісту (інформаційні агентства, видавничі будинки, кіностудії), і телекомунікаційні оператори, які володіють засобами доставки змісту населенню; зливаються компанії, що володіють різними частинами інфраструктури інформаційної, — телефонні оператори дальнього й місцевого зв'язку, виро-

бники комп'ютерів, програмного забезпечення, систем кабельного мовлення, супутникового й мобільного зв'язку. Мета об'єднань — збільшення капіталу, завоювання нових ринків збуту, підвищення конкурентоспроможності. Конвергенція технологій і зливання компаній, у свою чергу, приводить до лібералізації законодавчих і нормативних актів, які регулюють традиційно різні сектори інформаційної індустрії.

К. галузей інформаційної індустрії /к. отраслей информационной индустрии/ — процес об'єднання різних технологій, ринків, форм регулювання різноманітних галузей індустрії інформаційної. В цьому випадку здійснюється розмивання границь між секторами інформаційної індустрії, такими як виробництво телекомунікаційного обладнання, комп'ютерів, надання телекомунікаційних мережних послуг, розроблення програмного забезпечення, мультимедійні (аудіовізуальні) розподільчі мережі, виробництво змісту. В умовах конвергенції підвищується регулююча роль держави в таких галузях, як керування радіочастотним спектром з метою розподілу частот між конкурентами, забезпечення технічними стандартами для сумісності систем, сприяння досягненню національних інтересів в сфері політики інформаційної.

КОНС'ЮМЕРИЗМ /консьюмеризм/ [consumerism](англ. consumer — споживач товарів) — в комунікативістиці — термін, який вживається для позначення тенденції до споживацької психології, що розвивається в масовій аудиторії внаслідок впливу нав'язливого рекламування нових товарів і культу речовизму, що створюється в умовах комерціалізації засобів масової інформації.

КОНСОРЦІУМ /консорциум/ [consortium] (від лат. consortio — співучасть, спільність) — одна з форм капіталістичних монополій; угода групи банківських або промислових монополій для спільного здійснення великих фінансових операцій.

К. W3C /к. W3C/ [World Wide Web C. (W3C)] — міжнародний, не залежний від виробників консорціум, створений на комерційній основі, який співробітничає з виробниками стандартів з метою розвитку WEB-протоколів Інтернету, таких, як HTTP, HTML і URL.

КОНСТРУКЦІЯ /конструкция/ [construction] (від лат. constructio — побудова, складання) — 1) Будова, взаємне розташування частин машини, апарата, приладу тощо; структура. 2) Споруди складної будови, а

також частини споруд.

К. захисту об'єкта інженерні /к. защиты информации инженерные/ — елементи підсистеми інженерного захисту, призначені для механічного запобігання проникненню зловмисника до джерел інформації. В найбільш загальному випадкові до інженерних конструкцій і споруд відносяться: природні і штучні перепони (бар'єри) на можливому шляху пересування зловмисника до джерел інформації або інших цінностей; двері і вікна будівель і приміщень; пункти контрольно-пропускні для контрольованого пропускання на територію, що охороняється, людей і транспорту; шафи і робочі столи з ящиками, що закриваються на ключ; сховища, металеві шафи і сейфи.

КОНТАКТ /контакт/ [contact] (від лат. contactus — дотик) — безпосереднє спілкування, стикання з будь-ким.

К. розвідувальний /к. розведывательный/ [intelligence c.] — безпосереднє спілкування (стикання) розвідника (або його технічного засобу) з джерелом інформації, при якому розвідник безпосередньо або дистанційно може викрасти, знищити або змінити інформацію. К. р. може здійснюватися за певних умов — просторових, енергетичних, часових.

КОНТЕЙНЕР /контейнер/ [container] (англ. container, від contain — вміщувати) 1) Пристрій для зберігання та транспортування будь-чого. 2) У стеганографії — відкрите повідомлення, частина якого є принципово випадковою або шумовою (наприклад, дані вимірів, випадкові завади в графічних та звукових файлах, похибки заокруглення при різних перетвореннях даних).

К. порожній /к. пустой/ — контейнер без вбудованого прихованого повідомлення.

КОНТР... /контр.../ [counter...] (від лат. contra — проти) — префікс, що означає "проти".

КОНТРАСТНІСТЬ /контрастность/ [contrast](від франц. contraste — протилежність) — різко окреслена протилежність в чомусь.

К. об'єктів (цілей) /к. объектов (целей)/ [target c.] — ступінь відмінності об'єктів спостереження (цілей) на фоні місцевості, води, навколишніх предметів, що дозволяє виявити і розпізнати об'єкти (цілі)

візуально, за допомогою інфрачервоних приладів, РЛС, магнітометрів та інших технічних засобів розвідки. Розрізняють оптичну, теплову (інфрачервону), радіолокаційну та магнітну к. о.

К. радіолокаційна /к. радиолокационная/ [radar c.] — різниця у відбитті радіохвиль яким-небудь окремим об'єктом і оточуючими його предметами та фоном. К. р. цілі залежить від ступеня її відбивної здатності в порівнянні з фоном.

КОНТРОЛЬ /контроль/ [check] (франц. controle, від contrerole) — подвійний список) — 1) Перевірка, облік, спостереження за чим-небудь. 2) Установи, особи, що перевіряють діяльність будь-якої іншої організації або відповідної особи, звітність тощо. 3) Заключна функція керування.

К. автоматичний (вбудований) /к. автоматический (встроенный)/ [automatic (built-in) c.] — контроль, що виконується автоматично апаратними засобами.

К. алгоритмічний /к. алгоритмический/ [algorithmic c.] — контроль програмний, суть якого в тому, що задача, вирішена за будь-яким алгоритмом, перевіряється повторно по грубішому алгоритму з достатнім ступенем точності. Продуктивність ЕОМ при к. а. вище, проте він має такі ж недоліки як і контроль програмно-логічний та, крім того, обмежене застосування, так як не завжди вдається знайти для основного алгоритму скорочений.

К. апаратний /к. аппаратный/ [automatic, hardware c.] — функціональний контроль, що здійснюється за допомогою апаратних засобів. Виявляє збої або несправності безпосередньо у момент їхнього виникнення. В автоматизованих системах досягається методами контролю по модулю, дублюванням обладнання і т. ін.

К. даних /к. данных/ [data c.] — перевірка вірогідності і цілісності даних. Розрізняють синтаксичний, семантичний і прагматичний контроль.

К. діагностичний /к. диагностический/ [diagnostic c.] — перевірка функціонування ЕОМ, яка виконується за допомогою діагностичних програм і дозволяє виявляти і локалізувати несправності в обладнанні.

К. достовірності /к. достоверности/ — в системах автоматизованих — процес контролю достовірності оброблення інформації (даних). Методи контролю при обробленні інформації в системах оброблення

інформації автоматизованих класифікують по різних параметрах: за кількістю операцій, що охоплюється контролем, — одиночний (одна операція), груповий (група послідовних операцій), комплексний (контролюється, наприклад, процес збирання даних); за частотою контролю — безперервний, циклічний, періодичний, разовий, вибірковий, по відхиленню; за часом контролю — до виконання основних операцій, одночасно з ними, у проміжку між основними операціями, після них; за видом обладнання контролю — вбудований, контроль за допомогою додаткових технічних засобів, безапаратний; за рівнем автоматизації — "ручний", автоматизований, автоматичний. Розрізняють методи контролю достовірності системні, програмні і апаратні. Всі перелічені методи контролю базуються на використанні певної надмірності: структурної, часової або інформаційної, яка у свою чергу може бути природною або штучною.

К. достовірності апаратний /к. достоверности аппаратный/ — метод контролю достовірності оброблення інформації із застосуванням апаратних засобів, що виконують практично ті ж функції, що засоби контролю достовірності програмного. Проте вони працюють швидше і дозволяють виявляти помилки ближче до місця їхнього виникнення, а також помилки, які недоступні для програмних методів.

К. достовірності з природною інформаційною надмірністю /к. достоверности с естественной информационной избыточностью/ — контроль достовірності з виявленням об'єктивно існуючих зв'язків між елементами оброблення, які дозволяють робити висновок про достовірність інформації.

К. достовірності з часовою надмірністю /к. достоверности с временной избыточностью/ — контроль достовірності, заснований на можливості неодноразового повторення певного контрольованого етапу оброблення даних. Як правило, етап оброблення повторюють неодноразово і результати оброблення порівнюють між собою. У випадку виявлення помилки здійснюють виправлення і повторне оброблення.

К. достовірності зі структурною надмірністю /к. достоверности с структурной избыточностью/ — контроль достовірності за рахунок уведення у склад автоматизованої системи оброблення даних додаткових елементів, що реалізують резервування інформаційних масивів і програмних модулів, виконання одних і

тих же функцій різними програмами, схемний контроль у технічних засобах і т. ін.

К. достовірності зі штучною інформаційною надмірністю /к. достоверности с искусственной информационной достоверностью/ — контроль достовірності, здійснюваний за допомогою введення додаткових інформаційних розрядів у цифровому представленні даних і додаткових операцій у процедурі їхнього оброблення, які мають математичний або логічний зв'язок з алгоритмом оброблення даних. На основі аналізу результатів додаткових операцій і процедур оброблення даних, а також додаткових інформаційних розрядів виявляється наявність або відсутність помилок певного типу, а також можливість їхнього виправлення.

К. достовірності програмний /к. достоверности программный/ — метод контролю достовірності оброблення інформації на основі реалізації додаткових операцій, що мають математичний або логічний зв'язок з алгоритмом оброблення даних. Порівняння результатів цих додаткових операцій з результатами оброблення даних дозволяє встановити з певною ймовірністю наявність або відсутність помилок.

К. достовірності системний /к. достоверности системный/ — метод контролю достовірності оброблення інформації на основі сукупності системних заходів, таких як: оптимізація структури оброблення; підтримання характеристик обладнання в заданих межах; підвищення культури оброблення інформації; навчання і стимулювання обслуговуючого персоналу; створення оптимального числа копій і (або) передісторій програм вихідних і поточних даних; визначення оптимальної величини пакетів даних і швидкості первинного оброблення, процедур доступу до масивів даних і т. ін.

К. доступу (за доступом) /к. доступа (к. за доступом)/ [access c.] — високонадійний процес, що забезпечує визначення і обмеження доступу користувачів, програм або процесів (узагалі суб'єктів) до ресурсів та об'єктів системи обчислювальної згідно з моделлю захисту. Може бути реалізований шляхом організації звернення до таблиці, що зберігається в пам'яті і в якій перелічені права суб'єктів доступу. В ході виконання процесу може здійснюватися реєстрація всіх спроб доступу несанкціонованого в журналі

контрольному.

К. доступу до апаратури /к. доступа к аппаратуре/ — сукупність заходів по недопущенню порушника до внутрішнього монтажу, ліній зв'язку, технологічних органів керування. Здійснюється за допомогою засобів контролю розкривання апаратури не тільки в інтересах захисту інформації від НСД, але і для дотримання технологічної дисципліни з метою забезпечення нормального функціонування апаратури (системи).

К. за модулем N (за залишком) /контроль по модулю N (за остатком)/ [modulo-N с.] — контроль за надмірністю, що ґрунтується на використанні залишку від ділення контрольованих даних, які розглядаються як числа, на N.

К. за надмірністю (з введенням надмірності) /к. по избыточности (с введение избыточности)/ [redundancy с.] — розпізнавання помилкових комбінацій кодових і виправлення даних за рахунок надмірності.

К. захисту інформації /к. защиты информации/ — процес визначення (вимірювання) показників ефективності захисту інформації і порівняння цих показників з нормативними. Складовою частиною к. з. і. є контроль технічного захисту інформації. Застосовують наступні види контролю: попередній, періодичний, постійний.

К. захисту інформації періодичний /к. защиты информации периодический/ — контроль захисту інформації з метою систематичного спостереження за рівнем захисту. Здійснюється вибірково (стосовно до окремих тем робіт, структурних підрозділів або всієї організації) на основі планів, затверджених керівником організації, а також вищими органами. Найбільш часто повинен проводитися періодичний контроль на хімічних підприємствах, так як незначні порушення в технологічному процесі можуть призвести до витоку демаскуючих речовин. Для визначення концентрації демаскуючих речовин регулярно беруться біля підприємства проби повітря, води, ґрунту, снігу, рослинності. Періодичний (щоденний, щотижневий, щомісячний) контроль повинен проводитися співробітниками організації стосовно джерел інформації, з якими

вони працюють. Загальний (в межах всієї організації) періодичний контроль здійснюється два рази на рік з метою ретельної перевірки працездатності всіх елементів і системи захисту інформації в цілому.

К. захисту інформації попередній /к. защиты информации предварительный/ — контроль захисту інформації, що здійснюється при будь-яких змінах складу, структури і алгоритму функціонування системи захисту інформації, в тому числі: після встановлення нового технічного засобу захисту або зміни організаційних заходів; після проведення профілактичних і ремонтних робіт засобів захисту; після усунення виявлених порушень в системі захисту.

К. захисту інформації постійний /к. защиты информации постоянный/ — контроль захисту інформації, який здійснюється вибірково силами служби безпеки з притягненням співробітників організації з метою об'єктивної оцінки рівня захисту інформації і, насамперед, виявлення слабких місць в системі захисту. Такий контроль здійснює психологічний вплив на співробітників організації, що примушує їх більш ретельно виконувати вимоги забезпечення захисту інформації.

К. ієрархічний /к. иерархический/ [hierarchical c.] — метод контролю повноважень, при якому повноваження кожного об'єкта контролюються об'єктом з більш високими повноваженнями, в результаті чого створюється ієрархія повноважень.

К. на парність (парності) /к. на четность (четности)/ [parity c.] — метод контролю даних, при якому сума за модулем 2 двійкових одиниць в машинному слові, включаючи контрольний розряд, повинна мати певне значення — бути завжди парною або непарною.

К. передавання /к. передачи/ [transfer c.] — контроль правильності виконання процедури передавання даних і вірогідності інформації, що передається. Одним з методів к. п. є контроль на парність.

К. підрахунком /к. подсчетом/ [count c.] — перевірка правильності передавання даних підрахунком кількості переданих повідомлень і порівнянням його з вказаним числом.

К. приміщень на відсутність закладних пристроїв /к. помещений на отсутствие закладных устройств/ — сукупність заходів забезпечення безпеки інформації у приміщенні шляхом недопущення вста-

новлення закладних пристроїв та виявлення, локалізації і вилучання уже встановлених закладних пристроїв. Найбільш доцільні наступні види заходів: оперативний візуальний огляд приміщення; профілактичний періодичний контроль з використанням технічних засобів пошуку і локалізації закладних пристроїв; разовий контроль приміщень перед проведенням в ньому нарад з питань, інформація по яких має високий гриф секретності; перевірка приміщення після проведення в ньому капітального ремонту; перевірка різноманітних нових предметів, розташованих в приміщенні представницьких подарунків, предметів інтер'єру, радіоелектронних засобів і т. ін.; радіомоніторинг приміщення протягом робочого часу.

К. програмний /к. программный/ [program c.] — вид контролю функціонального, що здійснюється за допомогою програмних засобів. К. п. поділяється на програмно-логічний, алгоритмічний і тестовий.

К. програмно-апаратний /к. программно-аппаратный/ — контроль функціонування ЕОМ, який виконується як програмними, так і апаратними засобами.

К. програмно-логічний /к. программно-логический/ — контроль програмний, найбільш розповсюджена форма якого ґрунтується на подвійному обрахунку з порівнянням одержаних результатів. К. п.-л. дозволяє надійно виявляти збої, і для його здійснення не потрібно додаткового обладнання. Проте при цьому більш ніж вдвоє знижується продуктивність ЕОМ, не виявляються систематичні збої, неможливо вказати місце відмови або збою, потрібна додаткова ємність пам'яті для програми обчислень.

К. семантичний /к. семантический/ [semantic c.] — контроль програми на наявність семантичних (смислових) помилок. Здійснюється програмістом до виконання програми або автоматично під час її виконання. Якщо в програмі не передбачені спеціальні засоби, семантичні помилки можуть призвести до аварійного завершення завдання.

К. синтаксичний /к. синтаксический/ [syntactic c.] — контроль виразів вихідної програми, що виконується транслятором на етапі синтаксичного аналізу й має за мету виявлення синтаксичних помилок.

К. системний /к. системный/ [system c.] — контроль загального функціонування обчислювальної

системи в процесі її експлуатації.

К. тестовий /к. тестовый/ [test c.] (від англ. test — випробування) — перевірка працездатності комплексу засобів автоматизації за допомогою випробувальних програм. К. т. не завжди виявляє збої.

К. технічного захисту інформації / к. технической защиты информации/ — сукупність заходів організаційних і технічних, що проводяться з метою перевірки виконання встановлених вимог і норм захисту інформації технічного.

К. функціональний /к. функциональный/ [functional c.] — метод забезпечення контролю функціонування системи автоматизованої з метою своєчасного виявлення відмов, помилок і збоїв апаратури, програмного забезпечення і помилок людини, виключення їхнього впливу на подальший процес оброблення інформації та встановлення місця розташування елемента, блока програми, робочого місця, що відмовили, з метою наступного швидкого відновлення системи. Існуючі методи к. ф. обчислювальних систем можуть бути розділені на програмні, апаратні і комбіновані (поєднання програмного з апаратним).

КОНТРПРОТИДІЯ /контрпротиводействие/ (від57 контр... і протидія) — запобігання дії, що перешкоджає іншій дії.

К. електронна /к. електронное/ [electronic protection] — сукупність заходів війни електронної, спрямованих на підвищення живучості і пониження втрат своїх сил і засобів від впливу керованої зброї і засобів електронної протидії противника.

КОНТРРОЗВІДКА /контрразведка/ [counterespionage, secret (security) service) (від контр... і розвідка) — 1) Діяльність спеціальних органів держави з метою боротьби проти розвідок інших держав (попередження замахів, шпіонажу, диверсійної та підривної діяльності). 2) Протидія розвідці агентурній конфронтуючої сторони. 3) Назва самих органів.

КОНТРСУГЕСТІЯ /контрсуггестия/ (від контр... і сугестія) — див. опірність навіюванню.

КОНТРШПІОНАЖ /контршпионаж/ (від контр... і шпіонаж)— сукупність заходів контррозвідки, спрямованих на недопущення попадання секретних матеріалів в руки представників іноземних служб розвіду-

вальних.

КОНФЕРЕНЦІЇ /конференции/ [conference] (лат. conferentia, від confero — збираю в одне місце) — спосіб взаємодії декількох користувачів Інтернету. Існують у текстовій, аудіо в відео-формі. Текстові: News — асинхронне спілкування користувачів через читання-написання листів заданої тематики. Загальна кількість — декілька десятків тисяч. News — ефективний спосіб вирішення професійних питань; реального часу — Chat, тобто одночасний зв'язок декількох абонентів або діалог у текстовому режимі. Можливий як при використанні браузера, так і через спеціального поштового клієнта (mIRC, Pirch). Аудіо і відео конференції можливі при наявності каналів із пропускною спроможністю більш 30 в 100 Кбит/с відповідно. Необхідні мікрофони, відеокамери, програмне забезпечення для проведення конференцій: IPhone, WebPhone, NetMeeting. IPone в WebPhone дозволяють телефонувати з комп'ютера на звичайний телефонний номер.

КОНФІГУРАЦІЯ /конфигурация/ [configuration] (лат. configuratio, від configuro — надаю правильної форми) — компонування системи з чітким визначенням характеру, кількості, взаємозв'язків й основних характеристик її функціональних елементів; сукупність апаратних засобів і з'єднань між ними; перелік засобів, що включаються в даний комплекс, систему.

К. обчислювальної системи /к. вычислительной системы/ [configuration] — сукупність функціональних частин системи обчислювальної й зв'язків між ними, зумовлена основними технічними характеристиками цих частин, а також характеристиками завдань оброблення даних.

К. операційної системи /к. операционной системы/ [operating system c.] — сукупність значень змінних параметрів операційної системи, визначена характером задач прикладних, які в даний час виконуються під керуванням цієї операційної системи.

КОНФІГУРУВАННЯ /конфигурирование/ — настройка системи операційної на конкретну конфігурацію обладнання і адаптація до потреб користувача, що виконуються при завантаженні ОС за вказівками, заданими в файлі конфігурації.

КОНФІДЕНЦІЙНІСТЬ /конфиденциальность/ [confidentiality, privacy] (від лат. confidentia — довір'я)

— властивість не підлягати розголосові; довірчість, секретність, суто приватність, секретність.

К. адміністративна /к. административная/ [mandatory c.] — послуга безпеки, що забезпечує конфіденційність інформації відповідно до принципів керування доступом адміністративного.

К. довірча /к. доверительная/ [discretionary c.] — послуга безпеки, що забезпечує конфіденційність інформації відповідно до принципів керування доступом довірчого.

К. інформації /к. информации/ [information c.] — властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і (або) процесом. Інформація зберігає конфіденційність, якщо дотримуються встановлені правила ознайомлення з нею.

КОНФОРМІЗМ /конформизм/ [conformism] — пристосовницьке відношення до статус-кво (становища, що існувало або існує в якийсь визначений момент), пасивне сприйняття існуючої реальності, відсутність власної позиції в суспільному житті, некритичне наслідування установкам культури масової, що розповсюджується засобами масової інформації.

КОНЦЕПЦІЯ /концепция/ [concept, conception] (від лат. conceptio — сприйняття) — система поглядів на певне явище; спосіб розуміння, тлумачення певних явищ, основна ідея будь-якої теорії.

К. інформаційного суспільства /к. информационного общества/ — систематизована сукупність поглядів на суспільство інформаційне та шляхи входження в інформаційне суспільство. При створенні к. і. с., як правило використовується комплексний підхід, заснований на формуванні балансу інтересів держави, суспільства, особистості, а також підприємницьких кіл. Кожна країна розроблює концепцію входження в інформаційне суспільство, виходячи з власних конкретних умов: розвиненості інфраструктури телекомунікаційної, індустрії змісту, законодавчої бази і т.ін. Проте аналіз різноманітних програм (див. програма входження в інформаційне суспільство) і концепцій дозволяє виявити інваріантні положення, які і складають ядро будь-якої к. і. с.: створення к. і. с. є необхідністю, способом підвищення конкурентоспроможності країни на світових ринках і надання своїм громадянам можливостей для освіти і зайнятості в інформаційному віці; програми й концепції створюються від імені держави і розраховані для впливу на конкретні сторо-

ни життя; в інформаційному суспільстві державні органи використовують інформаційно-телекомунікаційні технології для реструктуризації, підвищення ефективності своєї роботи, відкритої інформаційної взаємодії з громадськістю; інформаційне суспільство надає нові можливості для розвитку демократії, урахування суспільної думки, контролю за державним апаратом; глобальна природа інформаційного суспільства потребує узгодження національних політик, міжнародне співробітництво набуває найважливішого значення; роль держави полягає у створенні адекватної законодавчої бази і адміністративного регулювання, що сприяє наданню інвестицій, розвитку справедливої конкуренції в галузях інформаційної індустрії, удосконаленню системи освіти, координації зусиль різних суб'єктів суспільства, організації міжнародної кооперації, проведенню науково-дослідних робіт; к. і. с. має яскраво виражену соціальну спрямованість (в них багато уваги приділяється питанням дистанційної комп'ютерної освіти, телемедицини, наданню соціальних державних послуг через телекомунікації); к. і. с. зв'язана з концепцією стійкого розвитку, яка передбачає перехід до таких форм виробничої й соціальної діяльності, які зберігають баланс у системі "людина-суспільство-природа".

К. інформаційної безпеки держави /к. информационной безопасности государства/ [national information security c.] — систематизована сукупність відомостей про безпеку інформаційну держави та шляхи її забезпечення. В концепції проводиться системна класифікація факторів дестабілізуючих і загроз інформаційних безпеці особистості, суспільства і держави; обґрунтовуються основні положення по організації забезпечення інформаційної безпеки держави; розроблюються пропозиції по способах і формах забезпечення інформаційної безпеки. Основу забезпечення інформаційної безпеки держави складають засоби і способи захисту державної таємниці. Для конкретної особистості такими способами і засобами можуть бути: судовий захист прав і свобод у використанні інформації; адміністративний захист її життєво важливих інтересів в інформованості з боку територіальних або відомчих органів інформаційної безпеки; автономний захист своїх прав і свобод в основному із застосуванням технічних засобів захисту, особистої, сімейної і професійної таємниці. Це ж характерно і для суспільних об'єднань, організацій (підприємств). Разом з

тим, при наявності у них власних органів інформаційної безпеки суттєво розширюються їхні можливості у сфері автономного захисту.

К. інформаційної війни /к. информационной войны/ [information warfare c.] — система поглядів на війну інформаційну та шляхи її ведення. За останніми оцінками к. і. в. повинна передбачати: заглушення (у воєнний час) елементів інфраструктури державного і воєнного управління (ураження центрів командування і управління); електромагнітний вплив на елементи інформаційних і телекомунікаційних систем (боротьба радіоелектронна); одержання розвідувальної інформації шляхом перехоплення і декодування (дешифрування) інформаційних потоків, що передаються каналами зв'язку, а також побічним випромінюванням і за рахунок спеціально впроваджених в приміщення і технічні засоби електронних пристроїв перехоплення інформації (розвідка радіоелектронна); здійснення несанкціонованого доступу до інформаційних ресурсів (шляхом використання програмно-апаратних засобів зламу систем захисту інформаційних і телекомунікаційних мереж противника) з наступним їхнім спотворенням, знищенням або викраденням чи порушенням нормального функціонування цих систем (так звана "хакерна війна"); формування і масове розповсюдження інформаційними каналами противника або глобальними мережами інформаційної взаємодії дезінформації або тенденційної інформації для впливу на оцінки, наміри і орієнтацію населення і осіб, що приймають рішення (війна психологічна); одержання необхідної інформації шляхом перехоплення і оброблення відкритої інформації, що передається незахищеними каналами зв'язку, циркулюючої в інформаційних системах, а також опублікованої в засобах масової інформації.

КООПЕРАЦІЯ /кооперация/ [co-operation] (лат. cooperatio, від coopero — співробітничаю) — 1) Форма організації праці, за якої певна кількість людей спільно бере участь в одному й тому ж або різних, або зв'язаних між собою, виробничих процесах. 2) Добровільні об'єднання людей для спільної господарської діяльності.

К. інформаційна /к. информационная/ [information c.] — форма забезпечення інформаційної безпеки між рівноправними суб'єктами процесу інформаційного (фізичними, юридичними, міжнародними),

що включає сукупність їхніх взаємоузгоджених дій, спрямованих на одержання відомостей про фактори дестабілізуючі і загрози інформаційні та захист від них доступними законними способами і засобами.

КОПІЮВАННЯ /копирование/ [copying] — 1) Процес одержання копій; відтворення даних з збереженням вихідної інформації. 2) Один із методів маніпулювання даними і управляючими командами. Застосовується для одержання несанкціонованих копій як з програмного забезпечення ЕОМ (даних і інформації), так і з топологій інтегральних мікросхем. Ефективність (небезпека) застосування к. зумовлена наступними обставинами: високою щільністю даних і інформації, записаних на матеріальному носії або тих, що знаходяться в пам'яті ЕОМ (мереж ЕОМ); швидкістю і простотою процесу к.; достатньо широкими можливостями дублювання масивів без залишення будь-яких слідів.

КОПІЯ /копия/ [copy] (від лат. copia — запас, велика кількість) — 1) Точне відтворення оригіналу. 2) Точне відтворення будь-якого документа.

К. відновлення /к. восстановления/ — те ж, що копія дублююча.

К. дублююча (контрольна, резервна) /к. дублирующая (контрольная, резервная)/ — копія файла, передбачена для використання у випадку пошкодження основного екземпляра файла (оригіналу).

КОРИСНІСТЬ /полезность/ [utility] — властивість будь-чого приносити добрі наслідки, матеріальну вигоду, прибутки і т. ін.

К. розвідувальної інформації /п. разведывательной информации/ [intelligence information u.] — властивість інформації сприяти розширенню пізнання та розуміння питань, прямо чи побічно зв'язаних з забезпеченням національної безпеки. Вона повинна вирішити ту проблему, яка стоїть уже в даний момент. К. р. і. визначається багатьма якостями, найважливішими з яких є повнота та вірогідність інформації. Проте іноді повнота та вірогідність можуть бути частково принесені в жертву своєчасності розвідувальної інформації.

КОРИСТУВАЧ /пользователь/ [user, subscriber] — 1) Той, хто користується будь-чим. 2) Фізична особа,

яка може взаємодіяти з комп'ютерною системою через наданий їй інтерфейс.

К. авторизований /п. авторизованный/ [authorized u.] — користувач, що володіє певними повноваженнями.

К. випадковий (разовий) /п. случайный (разовый)/[casual u.] — користувач обчислювальної системи, який працює з системою нерегулярно, епізодично.

К. віддалений (дистанційний) /п. удаленный (дистанционный)/ [rename u.] — користувач обчислювальної системи, який здійснює доступ до програм і даних з віддаленого термінала.

К. зареєстрований /п. зарегистрированный/ [authorized u.] — 1) Користувач обчислювальної системи, який має пріоритетний номер в даній системі колективного користування. 2) Користувач, включений в графік роботи на ЕОМ.

К. зв'язку /п. связи/ — фізичні і юридичні особи, які є споживачами послуг зв'язку.

К. інтерактивний (діалоговий, оперативний) /п. интерактивный (диалоговый, оперативный)/ [interactive (on-line) u.] — користувач обчислювальної системи, який працює на терміналі в інтерактивному (діалоговому) режимі.

К. кінцевий (параметричний) /п. конечный (параметрический)/ [end (ultimate) u.] — користувач обчислювальної системи, який звертається до системи обчислювальної для одержання інформації або вирішення прикладних задач.

К. незареєстрований /п. незарегистрированный/ [unauthorized u.] — 1) Користувач обчислювальної системи, який не стоїть на обліку в даній системі колективного користування. 2) Користувач, який працює на ЕОМ не по графіку.

К. обчислювальної системи /п. вычислительной с./ — 1) Фізична або посадова особа, яка має право використання ресурсів системи обчислювальної для виконання своїх службових обов'язків (для одержання інформації або вирішення різних завдань). Розрізняють наступні категорії к.: аналітик, програміст системний, програміст прикладний, адміністратор автоматизованої системи, оператор ЕОМ, користувач кінцевий.

2) Програма або система, що використовує ресурси іншої системи.

К. привілейований /п. привилегированный/ [privileged (authorized) u.] — користувач обчислювальної системи, який має порівняно з іншими користувачами більші права і привілеї при роботі з системою обчислювальною (наприклад, більш високий пріоритет).

К. термінала /п. терминала/ [terminal u.] — користувач обчислювальної системи, який взаємодіє з ЕОМ за допомогою термінала.

КОРПОРАТИВНИЙ /корпоративный/ [corporative] — той, що належить до корпорації, властивий, характерний якійсь корпорації; вузькогруповий, відособлений.

КОРПОРАЦІЯ /корпорация/ [corporation] (від лат. corporatio — спілка) — товариство, спілка, сукупність осіб, об'єднаних на основі цехових, кастових, комерційних та інших інтересів; загальна назва акціонерних товариств.

КРЕКЕР /крекер/ [cracker] — особа, яка порушує систему захисту автоматизованої системи з корисливими інтересами.

КРИЗА /кризис/ [crisis] (від грец. *κρίσις* — вихід, рішення, поворотний пункт) — різкий, крутий перелом в будь-чому; важкий перехідний стан; важке положення.

К. інформаційна /к. информационный/ [information c.] — перехідний, нестійкий стан будь-якої системи, пов'язаний із серйозними порушеннями в організації потоків інформаційних та здійсненні процесів інформаційних.

КРИПТО... /крипто.../ [crypto...] (від грец. *κρυπτός* — секретний, прихований) — у складних словах означає "секретно" або належність до якогось прихованого стану.

КРИПТОАНАЛІЗ /криптоанализ/ [cryptanalysis] (від крипто... і аналіз) — 1) Наука, що займається вивченням і розробкою методів, способів та засобів дешифрування. 2) Процес оброблення шифрограми з метою визначення застосованого шифру та відповідного ключа, що необхідні для виділення вихідної

інформації (тексту відкритого).

К. диференційний /к. дифференциальный/ [differential c.] — метод криптоаналізу, що складається з аналізу впливу різниць в парах відкритого тексту на різниці в парах відповідних шифртекстів. Під "різницею" розуміється результат операції складання за модулем ($\oplus$) над парами відкритого або шифртексту. К. д. є частковим випадком атаки криптоаналітичної з вибраним відкритим текстом.

К. лінійний /к. линейный/ [linear c.] — метод криптоаналізу, що складається з аналізу лінійного зв'язку між бітами відкритого тексту та бітами відповідного шифртексту. К. л. є частковим випадком атаки криптоаналітичної з відомим відкритим текстом та атаки криптоаналітичної лише з відомим шифртекстом.

К. прикладний /к. прикладной/ [applied c.] — метод криптоаналізу шляхом викрадення всієї інформації про криптосистему (в тому числі і ключів).

К. теоретичний /к. теоретический/ [c.] — криптоаналіз шляхом аналізу криптосистеми за допомогою наукових методів.

КРИПТОАНАЛІТИК /криптоаналитик/ [cryptanalyst] (від крипто... і аналітик) — фахівець, що займається розробленням атак криптоаналітичних на криптосистеми. Опонент криптографові.

КРИПТОГРАМА /криптограмма/ [cryptogram] (від крипто... і ...грама (грец. $\gamma\rho\alpha\mu\mu\alpha$ — літера, написання)) — 1) Шифртекст, підготовлений для відправки каналами зв'язку. 2) Тайнопис.

КРИПТОГРАФ /криптограф/ [cryptographer] — фахівець, що займається розробкою криптосистем.

КРИПТОГРАФІЧНИЙ ПРИМІТИВ /криптографический примитив/ [cryptography primitive] — елемент (операція або процедура) для вирішення деякої задачі криптографічного захисту інформації. В якості к. п. можуть виступати генератор псевдовипадкової послідовності, процедура обчислення хеш-функції, алгоритм криптографічного перетворення і т.ін.

КРИПТОГРАФІЯ /криптография/ [cryptography] (від крипто... і ...графія (грец. $\gamma\rho\alpha\varphi$ — пишу, креслю, малюю)) — 1) Наука, що займається вивченням і розробкою методів створення криптосистем. 2) Спосіб

тайнопису, заснований на використанні шифру.

К. квантова /к. квантовая/ [quantum c.] (нім. Quant, від лат. quantum — скільки) — галузь криптографії, що вивчає криптографічні перетворення інформації на основі принципу невизначеності квантової механіки.

К. напівпрозора /к. полупрозрачная/ [translucent c.] — принцип побудови криптосистем з відновленням ключів, запропонований M. Bellare та R. Rivest'ом.

КРИПТОЛОГІЯ /криптология/[cryptology] (від крипто... і ...логія, що від грец. $\lambda\acute{o}\gamma\phi\varsigma$ — слово, вчення) — наука, складовими якої є криптографія та криптоаналіз. За іншим визначенням криптологія включає також стеганографію.

КРИПТОНІМ /криптоним/ — псевдонім агента або кодове найменування операції (програми), що присвоюється з метою забезпечення безпеки.

КРИПТОПЕРЕТВОРЕННЯ /криптопреобразования/ [cryptographical transformation] — 1) Див. перетворення криптографічне. 2) Сукупність операцій шифрування даних, а також формування коду автентифікації, імітовставки, хеш-коду та підпису цифрового.

КРИПТОПЕРІОД (КРИПТОПЕРІОД КЛЮЧА) /криптопериод (криптопериод ключа)/ [cryptoperiod] — період часу впродовж якого ключі на законній основі використовуються в криптосистемі законними абонентами. К. використовується для обмеження обсягу інформації (відносно даного ключа), яка доступна криптоаналітикові; обмеження потенційних збитків від компрометації даного ключа; обмеження використання даного ключа при закінченні його терміну дії; обмеження часу обчислень для проведення атак криптоаналітичних.

КРИПТОСИСТЕМА /криптосистема/ [cryptosystem] (від крипто... і система) — 1) Див. система криптографічна. 2) Система для перетворення криптографічного інформації, що містить у собі п'ять компонентів: множину вхідних текстів (відкритих текстів), множину шифртекстів, множину ключів, сім'ю шифруючих

(зашифровуючих та розшифровуючих) перетворень.

К. асиметрична /к. ассиметрическая/ [asymmetric c., asymmetric key c.] — криптосистема, у якої ключі зашифровування і розшифровування розрізняються таким чином, що за допомогою обчислень практично неможливо вивести один ключ з іншого.

К. з відкритим ключем /к. с открытым ключом/ [asymmetric key c., public-key c.] — криптосистема, в якій використовується два ключі — секретний (приватний) і відкритий, причому ні один із ключів не може бути обчислений з іншого за певний час. Секретний ключ тримається в таємниці, в той час як відкритий ключ може бути розісланий всім абонентам, з якими здійснюється взаємодія. Користуючись відкритим ключем будь-який з абонентів може послати захищене повідомлення авторові відкритого ключа. При цьому розшифрувати це повідомлення можна тільки секретним ключем, який відповідає відкритому. Такі криптосистеми називають також двоключовими або асиметричними. Вони засновуються на так званих важкооборотних (односторонніх, односпрямованих) функціях та забезпечують тільки практичну стійкість. Одним з основних застосувань к. з в. к. є керування ключами та створення електронного цифрового підпису.

К. з відновленням ключів /к. с восстановлением ключей/ [key recovery c.] — криптосистема, в якій разом з ключами, що застосовуються для шифрування повідомлень абонентами, у деякої сторонньої особи (арбітра) присутня додаткова інформація про ці ключі, яка може використовуватися для їхнього відновлення.

К. з депонуванням ключів /к. с депонированием ключей/ [key escrowed c.] — криптосистема з відновленням ключів, в якій один ключ зберігається у довірених осіб, а інформація про сеансові ключі, за допомогою яких шифруються повідомлення, зашифровується на цьому ключі та передається разом з шифртекстом. Ці криптосистеми застосовуються в стандарті США Escrowed Encryption Standard (EES).

К. з довідною стійкістю /к. с доказуемой стойкостью/ [provably secure] — криптосистеми, відносно яких існує формальний доказ того, що складність проведення їхнього криптоаналізу (для певної моде-

лі порушника) еквівалентна складності вирішення деякої важкої задачі (наприклад, задачі дискретного логарифма). Відомо, що до таких криптосистем відноситься криптосистема Діффі-Хеллмана.

К. із секретним ключем /к. с секретным ключом/ — криптосистема, у якої один і той же ключ використовується для зашифровування і розшифровування інформації. Такі криптосистеми також називаються одноключовими, симетричними, звичайними, двосторонніми або класичними. В них використовується шифрування блокове і потокове.

К. інволютна /к. инволютная/ [involute c.] — криптосистема, у якої процедура зашифровування та розшифровування є однаковими. Зрозуміло, що тільки симетричні криптосистеми можуть бути к. і.

К. Мессі-Омури /к. Месси-Омуры/ — криптосистема асиметрична, для передавання конфіденційних повідомлень, стійкість якої заснована на проблемі дискретного логарифма в мультиплікативній групі кінцевого поля. Нехай $GF(q)$ — деяке поле Галуа, відоме і абонентам системи й супротивникові. Для передавання повідомлення від абонента A до B, A випадково обирає число $e_A \in [0, q-1]$, $(e_A, q-1 = 1$ та за допомогою алгоритму Евкліда обчислює $d_A \cdot e_A \equiv 1 \; mod \; q-1$ і зберігає їх в секреті. Таким ж чином B отримує e_B та d_B. Для передачі повідомлення M A передає B $M^{e_A} \in GF(q)$. B обчислює $M^{e_A e_B} \in GF(q)$ і передає його A. A "знімає" свій шифр $M^{e_A e_B d_A} = M^{e_B} \in GF(q)$ і передає результат B. B отримує повідомлення $M^{e_B d_B} = M \in GF(q)$. Криптосистема не стійка відносно атак криптоаналітичних.

К. на основі еліптичних рівнянь /к. на основе эллиптических уравнений/ [elliptic curve c.] — криптосистема, побудована на основі еліптичних кривих, які представляють математичний об'єкт, що може бути визначеним над будь-яким полем (скінченним, дійсним, раціональним або комплексним). У криптографії звичайно використовують скінченні поля. Еліптична крива представляє собою множину точок (x, y), що задовольняють наступному рівнянню: $y^2 = x^3 + ax + b$, а також нескінченно віддалена точка. Для точок на кривій достатньо легко вводиться операція додавання, яка відіграє ту ж роль, що операція множення в криптосистема RSA та Ель-Гамаля. В реальних криптосистемах використовується рівняння $y^2 = x^3 + ax + b \mathrm{mod} p$, де p — просте. Проблема дискретного логарифма на еліптичній кривій полягає у

наступному: дана точка G на еліптичній кривій порядку r (кількість точок на кривій) та інша точка Y на ці й же кривій. Необхідно знайти єдину точку x таку, що $Y = xG$, тобто Y є x-та степінь G.

К. Поліга-Хеллмана /к. Полига-Хеллмана/ — криптосистема симетрична, у якої ключі зашифровування/розшифровування розрізняються, але таким чином, що один отримуєть з іншого за допомогою поліноміального алгоритму, або "легко". Функції зашифровування/розшифровування подаються формулами:$C = M^e \ mod \ p$, $M = C^d \ mod \ p$, де p — просте число, $e \cdot d \equiv 1 \ mod \ p - 1$, M — текст відкритий, C — шифртекст. Замість полів Галуа $GF(p)$ криптосистема також може бути побудована над полем Галуа $GF(2^n)$, де $2^n - 1$ — число Мерсена.

К. ручна /к. ручная/ [manual c.] — криптосистема, в якій криптоперетворення відбуваються ручним способом без використання криптообладнання (crypto-equipment) або автоматизованих пристроїв.

К. симетрична /к. симметрическая/ [classical c., one-key c., secret-key c., symmetric c.] — криптосистема, у якої ключі зашифровування (розшифровування) або однакові, або легко виводяться один з одного, забезпечуючи таким чином спільний ключ.

КРИПТОСТІЙКІСТЬ /криптостойкость/ [cipher strength, cryptosecurity, cryptological hardness, resistance to cryptoanalysis] (від крипто... і стійкість) — характеристика шифру, що показує його стійкість до дешифрування і визначається часом та обчислювальними ресурсами, які необхідні для дешифрування.

К. абсолютна /к. абсолютная/ [perfect secrecy, unconditionally secure]— криптостійкість, що визначається за умов наявності у криптоаналітика нескінченного часу та нескінченних обчислювальних можливостей. Досягнення к. а. за Шеноном означає, що відкритий та шифртекст є статистично незалежними. Шеноном показано, що к. а. досягається тільки тоді, якщо довжина ключа є не меншою від довжини відкритого тексту та ключ обирається з ключового простору дійсно випадково. Інша назва криптостійкість у теоретико-інформаційному сенсі.

К. практична /к. практическая/ [computationally secure, effectively unbreakable] — криптостійкість, яка визначається для шифру, який не є ідеальним шифром, тобто може бути дешифрований за скінченний

час. Інша назва криптостійкість у обчислювальному сенсі.

К. в обчислювальному сенсі /к. в вычислительном смысле/ — те ж, що криптостійкість практична.

К. у теоретико-інформаційному сенсі /к. в теоретико-информационном смысле/ — те ж, що криптостійкість абсолютна.

КРИТЕРІЙ /критерий/ [criteria, criterion] (від грец. *κριτήριον* — засіб судження) — мірило для визначення, оцінки предмета, явища; ознака, взята за основу класифікації.

К. безпеки комп'ютерних систем /к. безопасности компьютерных систем/ [Trusted Computer System C. (TCSC)] — стандарт інформаційної безпеки, розроблений міністерством оборони США у 1983 році з метою визначення вимог безпеки, що пред'являються до апаратного, програмного і спеціального забезпечення комп'ютерних систем і вироблення відповідної методології аналізу політики безпеки, що реалізується в комп'ютерних системах воєнного призначення. Інша назва — "Жовтогаряча книга". У критеріях пропонуються три категорії вимог безпеки — політика безпеки, аудит і коректність, в рамках яких сформульовані шість базових вимог безпеки: політика безпеки, мітки — в рамках політики безпеки; ідентифікація і автентифікація, реєстрація і облік — в рамках аудита; контроль коректності функціонування засобів захисту, безперервність захисту — в рамках коректності. Перші чотири вимоги спрямовані безпосередньо на забезпечення безпеки інформації, а дві останні — на якість самих засобів захисту. "Жовтогаряча книга" передбачає чотири групи критеріїв, які відповідають різним ступіням захищеності: від мінімальної (група D) до формально доведеної (група A). Кожна група включає один або декілька класів. Групи D (мінімальний захист) і A (верифікований захист) містять по одному класу [класи D1 (мінімальний захист) і A1 (формальна верифікація) відповідно], група C (дискреційний захист) — класи C1 (дискреційний захист) C2 (керування доступом), а група B (мандатний захист) — B1 (захист із застосуванням міток безпеки), B2 (структурований захист), B3 (домени безпеки), що характеризуються різними наборами вимог безпеки. Рівень безпеки збільшується від групи D до групи A, а всередині групи — із збільшенням номера класу.

К. гарантій /к. гарантий/ — група критеріїв для визначення рівня гарантій реалізації засобів захисту,

які в "критеріях Європейських" складаються з двох компонентів: критеріїв ефективності й критеріїв коректності. До складу критеріїв ефективності входять: відповідність набору засобів захисту проголошеним цілям захисту; взаємна узгодженість різних засобів і механізмів захисту; здатність засобів захисту протистояти атакам; можливість практичного використання недоліків архітектури засобів захисту; простота використання засобів захисту; можливість практичного використання функціональних недоліків засобів захисту. До складу критеріїв коректності входять: на стадії процесу розробки — специфікації вимог безпеки, розробка архітектури, створення робочого проекту, реалізація; середовище розробки — засоби керування конфігурацією, мови програмування й компілятори, безпека середовища розробки; експлуатаційна документація — керівництво користувача, керівництво адміністратора; середовище експлуатації — доставка й установка, запуск і експлуатація.

К. для визначення грифа конфіденційності інформації /к. для определения грифа конфиденциальности информации/ — результати прогнозу наслідків попадання інформації до конкурента або зловмисника, в тому числі: величина економічних і моральних збитків, що можуть бути нанесені організації; реальність створення передумов для катастрофічних наслідків в діяльності організації, наприклад, банкрутства тощо.

К. ефективності інформаційної боротьби /к. эффективности информационной борьбы/ — кількісна міра відображення ступеня переваги інформаційної однієї з протиборчих сторін. Визначається співвідношенням інформованості протиборчих сторін. Числове значення к. е. і. б. визначається за формулою:

$$F = K_1/K_2.$$

В чисельникові формули — показник інформованості першої, а в знаменникові — другої конфронтуючої сторони. Перевага першої сторони над другою досягається у випадку, якщо $F > 1$.

К. ефективності системи захисту інформації /к. эффективности системы защиты информации/ — кількісна міра для порівняння варіантів системи захисту інформації. Критерій може бути у вигляді

одного показника, який враховує основні характеристики системи, або являти собою сукупність часткових показників. Єдиний загальний критерій ефективності називається глобальним коефіцієнтом ефективності системи захисту інформації.

К. ефективності системи захисту інформації глобальний /к. эффективности системы защиты информации глобальный/ — кількісна міра у вигляді одного показника для вибору раціонального варіанта системи захисту інформації, що забезпечує досягнення поставлених цілей, вирішує поставлені задачі при повному наборі вхідних впливів із врахуванням обмежень. Найчастіше використовується критерій у вигляді відношення ефективність/вартість. Під ефективністю розуміють ступінь виконання системою завдань (див. ефективність захисту інформації), під вартістю — витрати на захист.

К. Європейські безпеки інформаційних технологій /к. Европейские безопасности информационных технологий/ [Information Technology Security Evaluation C. (ITSEC)] — стандарт інформаційної безпеки, розроблений в країнах Європи (Франція, Німеччина, Нідерланди і Великобританія) у 1991 році. "Європейські критерії" розглядають наступні задачі засобів інформаційної безпеки: захист інформації від несанкціонованого доступу з метою забезпечення конфіденційності; забезпечення цілісності інформації за допомогою захисту її від несанкціонованої модифікації або знищення; забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні. Для вирішення проблеми визнання засобів захисту ефективними в критеріях уведене поняття гарантій засобів захисту. Гарантії включають в себе два аспекти: ефективність, що відображає відповідність засобів безпеки завданням, що вирішуються, і коректність, що характеризує процес їхнього розроблення і функціонування. Загальна оцінка рівня безпеки системи складається з функціональної потужності засобів захисту (див. критерії функціональні) і рівня гарантій їхньої реалізації (див. критерії гарантій).

К. Загальні безпеки інформаційних технологій /к. Единые безопасности информационных технологий/ [Common C. for Information Technology Security Evaluation (CCITSE)] — стандарт інформаційної безпеки (версія 2.1 стандарту видана у серпні 1999 року), що узагальнює зміст і досвід використання

"Оранжевої книги". В ньому розвинені "критерії Європейські", втілена в реальні структури концепція типових профілів захисту "критеріїв Федеральних" США і відповідно до "критеріїв Канадських" представлена однакова основа для формулювання розробниками, користувачами й оцінювачами інформаційних технологій (експертами з кваліфікації) вимог, метрик і гарантій безпеки. Матеріали стандарту являють собою енциклопедію вимог і гарантій з інформаційної безпеки, які можуть відбиратися й реалізовуватися у функціональні стандарти (профілі захисту) забезпечення інформаційної безпеки для конкретних систем, мереж і засобів як користувачами (по відношенню до того, що вони хочуть одержати в продукті, що пропонується), так і розробниками і операторами мереж (по відношенню до того, що вони гарантують в продукті, що реалізується). Основними компонентами безпеки "Загальних критеріїв" є: потенційні загрози безпеці обчислювальних систем і завдання захисту; політика безпеки; продукт інформаційних технологій; профіль захисту; проект захисту; функціональні вимоги безпеки; вимоги гарантій безпеки; рівні гарантій. Стандарт "Загальних критеріїв" описує тільки загальну схему проведення аналізу кваліфікаційного і сертифікації, але не регламентує процедуру їх здійснення. Питаннями методології кваліфікаційного аналізу й сертифікації присвячений окремий документ авторів "Загальних критеріїв" — "методологія Загальна оцінки безпеки інформаційних технологій", який є додатком до стандарту.

К. Канадські безпеки комп'ютерних систем /к. Канадские безопасности компьютерных систем/ [Canadian Trusted Computer Product Evaluation C. (CTCPEC)] — національний стандарт інформаційної безпеки, розроблений Центром безпеки відомства безпеки зв'язку Канади (Canadian System Security Centre Communication Security Establishment) в 90 роках. "Канадські критерії" використовуються для розроблення вимог безпеки, специфікацій засобів захисту й сертифікації програмного забезпечення робочих станцій, багатопроцесорних обчислювальних систем, персональних і багатокористувальницьких операційних систем, систем керування базами даних, розподілених, мережних, вбудованих, проблемно-орієнтованих та інших систем. В "Канадських критеріях" пропонується оригінальний підхід до опису взаємодії користувачів з комп'ютерною системою, інваріантний по відношенню до політики безпеки. Усі компоненти системи, що

знаходяться під керуванням ядра безпеки, називаються об'єктами. Об'єкти можуть знаходитися в одному з наступних трьох станів: об'єкт-користувач, об'єкт-процес, пасивний об'єкт, і в залежності від стану, позначають користувачів, процеси й об'єкти відповідно. При описі критеріїв конфіденційності і цілісності (довільного й нормативного керування доступом і цілісністю) в "Канадських критеріях" використовується поняття тег. У критеріях застосований дуальний принцип подання вимог безпеки у вигляді функціональних вимог до засобів захисту і вимоги до гарантій їхньої реалізації. "Канадські критерії" є добре збалансованим конгломератом "Жовтогарячої книги" і "критеріїв Федеральних", посилених вимогами гарантій реалізації політики безпеки, і поряд з іншими стандартами послужили основою для розроблення критеріїв Загальних безпеки інформаційних технологій.

К. оцінки захищеності /к. оценки защищенности/ [security avaluation c.] — сукупність вимог (шкала оцінки), що використовується для оцінки ефективності функціональних послуг безпеки і коректності їхньої реалізації.

К. Федеральні безпеки інформаційних технологій /к. Федеральные безопасности информационных технологий/ [Federal C. for Information Technology Security (FCITS)] — стандарт інформаційної безпеки, розроблений Національним інститутом стандартів і технологій США (NIST) і Агентством національної безпеки США (NSA) в 90-х роках для використання в Американському федеральному стандарті з оброблення інформації (Federal Information Processing Standard), який повинен був замінити "Жовтогарячу книгу". "Федеральні критерії" охоплюють практично весь спектр проблем, зв'язаних із захистом та забезпеченням безпеки, так як включають усі аспекти конфіденційності, цілісності і працездатності. Основними об'єктами застосування вимог безпеки критеріїв є продукти інформаційних технологій і системи оброблення інформації. Ключовим поняттям концепції інформаційної безпеки "Федеральних критеріїв" є поняття профілю захисту. Відповідно до "Федеральних критеріїв" процес розробки систем оброблення інформації здійснюється у вигляді послідовності наступних основних етапів: розробка і аналіз профілю захисту; розробка і аналіз кваліфікаційний IT-продуктів; компонування й сертифікація системи оброблення інформації. "Фе-

деральні критерії" регламентують тільки перший етап цієї схеми — розробку й аналіз профілю захисту. Процес створення IT-продуктів і компонування систем оброблення інформації залишаються за межами цього стандарту.

К. функціональні /к. функциональные/ — група критеріїв для визначення функціональної потужності засобів захисту, які в "Європейських критеріях" розглядаються на трьох рівнях деталізації. На першому рівні розглядаються цілі забезпечення безпеки, другий рівень містить інформацію про специфікації функцій захисту, у третій — механізми, що реалізують їх. Специфікації функцій захисту розглядаються з точки зору наступних вимог: ідентифікація і автентифікація; керування доступом; підзвітність; аудит; повторне використання об'єктів; цілісність інформації; надійність обслуговування; безпека обміну даними. Більшість вимог співпадають з вимогами "Жовтогарячої книги". Вимоги безпеки обміну даними регламентують роботу засобів, що забезпечують безпеку даних, які передаються каналами зв'язку, і включають наступні розділи; автентифікація; керування доступом; конфіденційність даних; цілісність даних; неможливість відмови від здійснених дій. Набір функцій безпеки специфікується з використанням посилань на класи-шаблони, що визначені раніше. В "Європейських критеріях" їх десять. П'ять з них (F-C1, F-C2, F-B1, F-B2, F-B3) відповідають класам "Жовтогарячої книги" з аналогічним позначенням. Інші п'ять класів відображають точку зору розробників стандарту на проблему безпеки: клас F-IN призначений для систем з великими проблемами при забезпеченні цілісності, що є типовим для систем керування базами даних; клас F-AV характеризується підвищеними вимогами до забезпечення працездатності; клас F-DI розрахований на розподілені системи оброблення інформації; клас F-DC приділяє особливу увагу вимогам до конфіденційності інформації, що передається; клас F-DX пред'являє підвищені вимоги і до цілісності і до конфіденційності інформації (в ньому об'єднані вимоги класів F-DI і F-DC з додатковими можливостями шифрування і захисту від аналізу трафіка.

КУЛЬТУРА /культура/ [culture] (лат. cultura — догляд, освіта, розвиток) — сукупність матеріальних і

духовних цінностей, створених людством протягом його історії.

К. інформаційна /к. информационная/ [information c.] — це рівень досягнутого в розвитку інформаційного суспільства людей, а також характеристика сфери інформаційної життєдіяльності людей, в якій можна відмітити ступінь досягнутого, кількість і якість створеного, тенденції розвитку, ступінь прогнозування майбутнього. У вузькому значенні, стосовно людини (особистості) інформаційна культура розглядається як уміння цілеспрямовано працювати з інформацією і використовувати для її одержання, оброблення й передавання комп'ютерну інформаційну технологію, сучасні технічні засоби і методи.

К. масова /к. массовая/ [mass c.] — продукт суспільств індустріального і постіндустріального, що вступають сьогодні в новий етап свого розвитку в атмосфері електронно-комунікаційної революції. Основні атрибути м. к. зумовлені процесами індустріалізації і комерціалізації засобів масової інформації: переважання споживацького відношення до інформативно-культурних цінностей, що набувається в дозвільно-розважальних цілях як предмет купівлі-продажу; багаторазове репродукування (відтворення) цих предметів і їхня стереотипізація (див. стереотип) за допомогою новітніх технічних засобів; акцент на клішованих модних формах і стилях, що рекламуються; усередненість і ефемерність смаків і зниження естетичних рівнів та інтелектуальних критеріїв; потяг до взаємного наслідування й однаковості в засвоєнні цих тенденцій, що закріплюються за допомогою ЗМІ усіх типів, але особливо ефективно завдяки аудіовізуальним засобам зв'язку. Головна структуроутворююча інтегральна якість к. м. — комунікаційна масовість. Масовість є великою соціальною силою, що підпорядковує собі психіку і спосіб життя мільйонів і мільярдів жителів планети. Розвиток інформаційних зв'язків інтегрує к. м. особливо інтенсивно. Вивчення процесів к. м. необхідне для виявлення важелів розумного й виваженого керування ними в інтересах забезпечення інформаційної безпеки особистості, суспільства й держави.

КУР'ЄР (ЗВ'ЯЗКОВИЙ) /курьер (связник)/ [courier (messenger)] — посильний, що відповідає за доставку і збереження секретних документів і матеріалів (розвідувальних даних). К. може бути і мимовільним: коли один "друг" просить доставити пакет або конверт іншому "другові".

КУРАТОР /куратор/ [curator] (лат. curator, від curo — піклуюся) — 1) Особа, що їй доручено загальний нагляд за якоюсь роботою. 2) Співробітник розвідки, залучена до співробітництва особа або агент-груповод, який безпосередньо керує роботою одного або декількох агентів.

Л

ЛАЗЕР /лазер/ [laser] (англ. laser як абревіатура від light amplification by stimulated emission of radiation — підсилення світла за допомогою індукованого випромінювання) — прилад для генерування або підсилення монохроматичного світла. Л. в сучасній техніці найчастіше використовуються як джерела енергії. Наприклад, низькоенергетичні л. використовуються у волоконно-оптичних лініях зв'язку, лазерних принтерах, засобах лазерного підслухування, запису та відтворення інформації (на компакт-дисках, магнітооптичних тощо) при вимірюванні відстаней. Високоенергетичні л. — в локації оптичній, хірургії, при зварюванні, бурінні, а також при вибухових роботах та при створенні лазерної зброї.

ЛАЗІВКА /лазейка/ [loophole] — в обчислювальній техніці — недоробка, помилка в програмному забезпеченні або апаратурі, що дозволяє обійти процеси керування доступом.

ЛЕГЕНДА /легенда/ [legend] (від лат. legenda — те, що має бути прочитане) — вигадана біографія (і ім'я), яку співробітник розвідки (нелегал) видає за свою з метою конспірації. Підкріплюється підробленими або чужими документами.

Л. відступна /л. отступная/ — метод організації, координації, проведення і контролю над проведенням таємної операції розвідувальної, при якому на випадок провалу офіційна влада може легко "відхреститися" від причетності держави до такої операції.

ЛИСТІВКА /листовка/ — засіб впливу психологічного друкованими засобами у вигляді інформаційно-пропагандистського друкованого видання, яке має невеликий обсяг (не більше двох сторінок), стислий і доступний текст, яскраве типографське оформлення. Вимоги до листівок: концентрованість змісту; аргументованість викладення матеріалу; простота й дохідливість матеріалу; композиційна чіткість викладення

матеріалу; привабливість і яскравість оформлення. В залежності від змісту розрізняють листівки інформаційні, аналітичні і спеціальні. В залежності від жанрового оформлення листівки поділяються на текстові і ілюстративні.

Л. аналітична /л. аналитическая/ — найбільш розповсюджений вид листівок. На відміну від листівок інформаційних, які характеризуються простим викладенням промовистих фактів, л. а. роз'яснюють будь-яку одну проблему. Основний тип подавання в них матеріалу — викладення, обговорювання, роз'яснення. Вони обов'язково включають тезис, який підтверджується відповідною аргументацією.

Л. ілюстративні /л. иллюстративные/ — листівки, в яких основу складають ілюстрації, а текст є допоміжним елементом і служить для більш глибокого розуміння суті замислу художника. Відмітна риса таких листівок — яскравість, наочність, виразність.

Л. інформаційна /л. информационная/ — листівка, призначена для доведення до адресата відповідного повідомлення, інформації про будь-яку подію, обстановку в певному районі, стан або дії конкретних людей. Для л. і. характерний такий стиль викладення, при якому вплив на читача здійснюється не стільки за допомогою логічних аргументів, скільки шляхом підбору фактів.

Л. маскувальні /л. маскировочные/ — листівки спеціальні, зміст і поліграфічне оформлення яких маскується під відповідне видання (періодичні друковані видання противника, його накази, інструкції, іншу службову документацію).

Л. публіцистичні /л. публицистические/ — найбільш розповсюджений вид листівок текстових, зміст яких носить, як правило, загальний характер і відрізняється гострим (публіцистичним) стилем. Див. також публіцистика.

Л. спеціальні /л. специальные/ — особливий тип листівок, які включають: листівки-документи, листівки маскувальні, листівки-перепустки, листівки-лозунги.

Л. текстові /л. текстовые/ — листівки, в яких основне смислове навантаження несе текст. Т. л. бувають

двох видів: публіцистичні і художні.

Л. художні /л. художественние/ — листівки текстові, в яких застосовують різноманітні літературні жанри: вірші, прозу, пародію, драматургію і т.ін. Л. х. впливають, у першу чергу, на почуття, настрої, душевний стан людей. Вони часто відрізняються сентиментальністю і розраховані на те, щоб викликати у читача тугу за домом, сім'єю або почуття страху за своє життя.

Л.-документи /л.-документы/ — листівки спеціальні, що містять тексти урядових документів, офіційних заяв, розпоряджень, звернень, ультиматумів. Вони відрізняються однозначністю змісту, можуть представляти собою факсиміле оригіналів різноманітних документів.

Л.-лозунги (заклики) /л.-лозунги (призывы)/ — листівки спеціальні, що містять лаконічні тексти у формі закликів із метою спонукати читачів до бажаних конкретних дій. Вони мають, як правило, невеликий формат, їхній текст набирають великим шрифтом і друкують у декількох фарбах. Л.-л. можуть також виготовляти у вигляді плакатів і розклеювати в доступних для огляду місцях.

/ л.-пропуска/ — листівки спеціальні, що являють собою своєрідний документ для військовослужбовців противника, які здаються в полон. Окрім заклику до здавання в полон, вони містять правила здавання, гарантії безпеки, роз'яснення порядку поводження з військовополоненими.

ЛІНЗА /линза/ [lens](нім. Linse, букв. — сочевиця) — прозоре тіло, обмежене правильними, здебільшого сферичними поверхнями, призначене для перетворення світлового пучка. Розрізняють шість форм оптичних лінз: двоопукла, плоско-опукла, вгнуто-опукла, двовгнута (двоввігнута), плоско-вгнута (плоско-ввігнута), опукло-вгнута (опукло-ввігнута). Перші три лінзи називають збиральними (додатними), інші три розсіювальними (від'ємними). Пряма лінія, що проходить через центри кривизни поверхонь перпендикулярно до них (вісь симетрії поверхонь), називається оптичною віссю л. Якщо на збиральну л. падає паралельний пучок променів паралельно її оптичній осі, то на виході промені зберуться в точці, що лежить на цій осі, — фокусі. Відстань між фокусом л. і її оптичним центром називається фокусною відстанню. Якщо паралельні промені падають під кутом до оптичної осі, то вони зберуться в точці, що лежить на пло-

щині, що проходить через фокус перпендикулярно до оптичної осі. Ця площина називається фокальною площиною.

Л. насадна /л. насадочная/ [accessory l., adapter l.] — лінза (в оправі), що приєднується до передньої частини оправки об'єктива фото- або кіноапарата з метою зміни його фокусної відстані. Позитивна л. н. зменшує цю відстань, негативна — збільшує.

ЛІНІЯ /линия/ [line] (від лат. linea) — 1) Елемент зображення. 2) Рядок програми, тексту, екрана дисплея. 3) Частина ланцюга передавання даних, зовнішня по відношенню до апаратури передавання даних.

Л. абонентська /л. абонентская/ [custom l.] — лінія зв'язку, яка з'єднує пункт абонентський з центром обчислювальним.

Л. зв'язку /л. связи/ [communication circuit, communication l., communication link] — сукупність технічних пристроїв і середовища розповсюдження сигналів, що забезпечує створення одного (одноканальна л. з.) або кількох (багатоканальна л. з.) каналів зв'язку (передавання сигналів у заданих напрямках з необхідною якістю і надійністю). В залежності від сигналів, що використовуються, л. з. можуть бути електричними, звуковими (акустичними) або оптичними (світловими). В залежності від засобів та середовища, що використовуються, електричні л. з. поділяються на лінії радіозв'язку (радіорелейні, іоносферні, метеорні, космічного радіозв'язку), проводові, комбіновані. Існують лінії прямого зв'язку і л. з. з ретрансляційними підсилювальними та комутаційними пунктами.

Л. зв'язку волоконно-оптична /л. связи волоконно-оптическая/ [optical l.] — лінія зв'язку, у якій сигнали передаються по кабелю волоконно-оптичному.

Л. зв'язку кабельна /л. связи кабельная/ [cable communication l.] — лінія зв'язку проводова, основним елементом якої є кабель (симетричний або коаксіальний). Л. з. к. поділяються на підземні, підводні та військово-польові.

Л. зв'язку повітряна /л. связи воздушная/ [aerial l.] — лінія зв'язку проводова, основним елементом якої є два провідники з однаковими електричними властивостями. В залежності від типу несучих констру-

кцій л. з. п. поділяються на стовпові, несучими конструкціями яких є дерев'яні або залізобетонні опори, і стоякові, несучими конструкціями яких є металеві стійки, встановлені, наприклад, на дахах будинків. Для ізоляції проводів повітряних ліній один від одного і відносно землі їх закріплюють на ізоляторах.

Л. зв'язку проводова /л. связи проводная/ [wireline] — лінія зв'язку, призначена для передавання електричних сигналів проводами. Л. з. п. поділяються на повітряні і кабельні. Основними параметрами л. з. п. є ширина спектра частот, що пропускається ними, і власне загасання.

Л. зв'язку радіорелейна /л. связи радиорелейная/ [relay (repeater) l.] — лінія зв'язку, що являє собою ланцюжок приймально-передавальних станцій, кожна з яких установлюється в межах прямої видимості іншої. Всі станції л. з. р. поділяються на кінцеві, проміжні і вузлові. Кінцеві станції розташовуються на початку і у кінці лінії. На цих станціях уводиться і виділяється інформація, забезпечується розподіл інформації між споживачами. Проміжні станції призначені для ретрансляції сигналів. Вузлові радіорелейні станції — це проміжні станції, на яких здійснюється розгалуження сигналів за різноманітними напрямками, виділення частини інформації, що передається, і введення нової інформації. Діапазон частот, призначений для передавання інформації одного виду, об'єднується в ствол радіочастотний. Для кожного ствола з метою виключення взаємного впливу виділяються дві робочі частоти — для передавання і приймання. Прийняті кожною станцією сигнали на частоті приймання, підсилюються і перетворюються на частоті передавання та випромінюються у напрямку наступної станції.

Л. зв'язку тропосферна /л. связи тропосферная/ [troposcatter link] — різновид лінії зв'язку радіорелейної, що використовує явище розсіювання ультракоротких радіохвиль у неоднорідностях тропосфери, що викликаються нерівномірністю станів різних точок тропосфери, безперервним перемішуванням і зміщенням повітряних мас в результаті нерівномірного розігрівання Сонцем різноманітних ділянок поверхні Землі і шарів тропосфери. Для забезпечення стійкого тропосферного радіозв'язку застосовуються антени з високим коефіцієнтом підсилення (40–50 дБ), потужні передавачі (1–10 кВт) і високочутливі приймачі. Л. з. т. найчастіше мають протяжність 140–150 км.

ЛІЦЕНЗІАР /лицензиар/ [licensor] — державна організація, якій надане право видавати ліцензії.

ЛІЦЕНЗІАТ /лицензиат/ [licentiate] — особа чи орган, якому встановленою державою організацією видано відповідне свідоцтво (ліцензія).

ЛІЦЕНЗІЯ /лицензия/ [license] (від лат. licentia — свобода, право) — 1) Офіційний документ, який надає дозвіл на право здійснення діяльності в даній галузі. Ліцензування підприємницької діяльності, пов'язаної з розробленням, виготовленням, ввезенням, вивезенням, реалізацією та використанням засобів криптографічного захисту інформації, а також з наданням послуг із криптографічного захисту інформації здійснюється в Україні Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. 2) Дозвіл на право продажу або надання послуг.

Л. на проведення робіт, зв'язаних з використанням відомостей, що складають державну таємницю /л. на проведение работ, связанных с использованием ведомостей, составляющих государственную тайну/ — ліцензія, яка надає право допуску підприємств, закладів і організацій до проведення робіт, зв'язаних з використанням відомостей відповідного ступеня секретності, створенням засобів захисту інформації, а також із здійсненням заходів і (або) надання послуг захисту таємниці державної. Ліцензія видається на основі спеціальної експертизи підприємства, закладу і організації і державної атестації їхніх керівників, відповідальних за захист відомостей, що складають державну таємницю, при виконанні ними наступних умов: виконання вимог нормативних документів щодо забезпечення захисту відомостей, які складають державну таємницю, в процесі виконання робіт, зв'язаний з використанням таких відомостей; наявність у їхній структурі підрозділів захисту державної таємниці і спеціально підготовлених співробітників для роботи із захисту інформації, кількість і рівень кваліфікації яких достатній для забезпечення захисту державної таємниці; наявність у них засобів захисту інформації сертифікованих.

ЛОБІЮВАННЯ /лоббирование/ (від англ. lobby — крита прощадка для прогулянок) — комплекс різноманітних прийомів та методів (прямих і непрямих) впливу на владні (в основному) структури з метою досягнення поставленої мети. В технологію л. включають не тільки традиційні заходи інформаційно-

психологічного впливу, але і ряд забезпечуючих дій.

ЛОГАРИФМ /логарифм/ [logarithm] (лат. logarithmus, від грец. $\lambda\acute{o}\gamma\varnothing\varsigma$, тут — відношення і $\grave{\alpha}\rho\iota\vartheta\mu\acute{o}\varsigma$ — число) — показник степеня, до якого треба піднести число a, щоб одержати число N.

Л. дискретний /дискретный л./ — див. проблема дискретного логарифма.

ЛОЗУНГ /лозунг/ [slogan, catchword, watchword] (від нім. Losung — заклик) — заклик, у якому чітко, стисло виражено провідну ідею або вимогу.

ЛОКАТОР /локатор/ [locator] (від лат. loco — уміщую) — пристрій, яким визначають місце, де перебувають об'єкти (цілі), за допомогою відбитих від них або випромінювання ними хвиль акустичних (звукових) чи електромагнітних.

Л. інфрачервоний /Л. инфракрасный/ [infrared (IR) l.] — те ж, що теплолокатор.

Л. нелінійний /л. нелинейный/ [nonlinear l.] — засіб виявлення елементів закладок за нелінійними властивостями напівпровідникових елементів. Принцип роботи н. л. полягає в тому, що при опроміненні частини простору, в якому розташовані напівпровідникові елементи закладних пристроїв високочастотною хвилею з частотою f у відбитій хвилі з'являються гармоніки з частотами $2f$, $3f$ і т. д. За характеристиками 2 і 3-ї гармонік відбитої хвилі приймається рішення про наявність в опроміненому просторі нелінійних елементів. В залежності від режиму випромінювання н. л. поділяють на локатори з безперервним і імпульсним випромінюванням. Проникаюча глибина хвилі локатора залежить від потужності і частоти випромінювання. Застосування л. н. забезпечує високу ймовірність виявлення закладних пристроїв в залізобетонних стінах, але гарантоване їхнє виявлення можливе тільки в результаті наступного обстеження ймовірного місцезнаходження.

Л. оптичний /л. оптический/ [optical radar] — див. станція локаційна лазерна.

ЛОКАЦІЯ /локация/ [location] (лат. locatio — розміщення, розподіл, від loco — розміщую)— визначення місцезнаходження цілей (об'єктів) за сигналами (наприклад, хвилями акустичними, електромагнітними), що випромінюються самими цілями (пасивна локація), або за відбитими від них сигналами, що посилаю-

ться спеціальними пристроями (локація активна). Розрізняють звукову (наприклад, гідролокація), локацію оптичну (лазерну) та радіолокацію.

Л. активна /л. активная/ [active l.] — локація, при якій інформацію про ціль одержують за рахунок приймання і аналізу відбитого від об'єкта сигналу, що виникає внаслідок опромінювання об'єкта зондувальним сигналом локатора (активна локація з пасивною відповіддю), або приймання від об'єкта і аналізу сигналу, що виникає в результаті ретрансляції встановленим на борті об'єкта відповідачем сигналу запиту локатора (активна локація з активною відповіддю).

Л. оптична (лазерна) /л. оптическая (лазерная)/ [optical (laser) l.] — виявлення і визначення місцеположення будь-яких об'єктів за допомогою лазерного випромінювання (когерентного електромагнітного випромінювання оптичного діапазону хвиль). Для л. о. об'єктом спостереження (ціллю) може бути будь-яке тіло або група тіл з електромагнітними властивостями, відмінними від властивостей середовища розповсюдження лазерного (оптичного) випромінювання. Об'єктами л. о. можуть бути літаки, вертольоти, кораблі, автомашини, ділянки земної поверхні, штучні супутники Землі, Місяць, планети і т.ін. Технічні засоби, призначені для лазерної локації, називають лазерними локаційними системами або станціями (ЛЛС) або оптичними (лазерними) локаторами. При л. о. інформація про ціль, що добувається в ЛЛС, переноситься оптичними локаційними сигналами, тобто відбитими електромагнітними коливаннями (випромінюваннями) оптичного діапазону, параметри яких певним чином зв'язані з координатами і характеристиками цілі. Л. о. підрозділяється в основному на активну і напівактивну. Активна л. о. здійснюється шляхом опромінювання цілі лазерною енергією і приймання частини енергії, відбитої (розсіяної) ціллю, тобто оптичного локаційного сигналу, приймальним пристроєм ЛЛС. Напівактивна л. о. відрізняється від активної тим, що лазерне випромінювання цілі здійснюється з одного пункту, а приймання відбитого оптичного локаційного сигналу здійснюється на іншому пункті.

ЛУНАКОНТРОЛЬ /эхоконтроль/ [echocheck] — метод контролю передавання даних, при якому прийняті дані повертаються на передавальний пункт і порівнюються з переданими даними.

ЛЮК /люк/ [trap door] (голл. luik — виріз, отвір) — залишені розробником недокументовані функції, використання яких дозволяє обминути механізми захисту.

Л. логічний /л. логический/ — механізм усередині системи операційної (забезпечення програмного), який дозволяє програмі зловмисника одержати привілейовану функцію або режим роботи (які йому не були дозволені). Л. л. можуть бути різноманітні помилки, що свідомо вводяться зловмисником в програмне забезпечення об'єкта. Див. також закладка програмна.

М

МАГІСТРАЛЬ /магистраль/ [unibus] (від лат. magistralis — головний) — 1) Головний кабель або головна труба в системі електричної, телеграфної, телефонної, газової, водопровідної мережі. 2) Лінія зв'язку; виділений канал передавання даних.

М. даних /м. даных/ [dataway] — канал інформаційний або інформаційна шина, якими здійснюється обмін даними.

М. міжвузлова /м. межузловая/ [interoffice trunk] — в системах передавання даних — пряма лінія між станціями або вузлами зв'язку.

МАГНІТОФОН /магнитофон/ [tape-recorder] (магніто... і фон, від грец. *μάγνης* (*μάγνητøς*) — магніт і *φωνή* — звук, голос) — радіотехнічний апарат для магнітного записування звуку (здебільшого на магнітну стрічку) та його відтворення.

МАЙСТЕР-КЛЮЧ /мастер-ключ/ [master key] — те ж, що ключ головний.

МАКРО... /макро.../ [macro...] (від грец. *μακρός* — великий, довгий) — у складних словах відповідає поняттям "великий", "довгий".

МАКРОВІРУСИ /макровирусы/ [macro virus] (від макро... і вірус) — віруси комп'ютерні, написані на мові програмування, що застосовується для написання макросів (наприклад, WordBasic). М. імітує натискання керуючих клавіш для деяких видів програм, які працюють із документами, що приводить до відсилання

документів, відкритих програмою, до випадкових (можливо несанкціонованих) адресатів. Використання м. в якості зброї інформаційної атаки дозволяє вибирати цілком конкретні адресати і функціонувати за строго заданою програмою, а також за допомогою зброї інформаційної забезпечення здійснювати транзит інформаційних ресурсів, одержаних несанкціонованим способом. Застосування м. у сполученні з іншими видами інформаційної зброї дозволяє досягнути наступних ефектів: одержання доступу до інформації конфіденційної в мережах обміну інформацією (МОІ); руйнування важливої інформації в МОІ; зниження ефективності роботи користувачів МОІ.

МАКРОС /макрос/ [macros] — послідовність команд, що запускається на виконання одним натисканням на клавішу.

МАНДАТ /мандат/ [mandate] (від лат. mandatum — доручаю) — 1) Повноваження, доручення, наказ. 2) Документ, що стверджує повноваження даної особи. 3) Елемент матриці доступу, що визначає тип доступу певного суб'єкта до певного об'єкта.

М. автентифікації /м. аутентификации/ [m. of authentication] — інформація, яка передається в процесі обміну при сильній автентифікації.

МАНІПУЛЮВАННЯ /манипулирование/ [manipulation] — 1) Здійснення маніпуляції. 2) Метод психологічного впливу, спрямований на зміну напрямку активності інших людей, який здійснюється настільки вправно, що залишається не замiченим ними. 3) Процес впливу на суспільну думку і політичну поведінку для спрямування політичної активності в необхідне русло. Мета — підштовхнути маси до схвалення непопулярних рішень та кроків влади.

М. даними /м. данными/ [data m.] — в системах керування базами даних — звертання до бази даних і виконання пошуку, читання і модифікації її записів.

М. даними і управляючими командами /м. данными и управляющими командами/ — велика група способів здійснення несанкціонованих дій в засобах комп'ютерної техніки. До методів м. д. і у. к. відносяться такі дії, як підміна даних або кодів, застосування програм типу "троянський кінь", бомб логічних і часових,

вірусів комп'ютерних, різних видів атак на комп'ютери і комп'ютерні мережі, моделювання, копіювання, подолання програмних засобів захисту і т. ін.

М. свідомістю /м. сознанием/ — маніпулювання, спрямоване на встановлення володарювання над духовним станом людей, керування ними шляхом нав'язування ідей, установок, мотивів, стереотипів поведінки, вигідних суб'єкту впливу. Виділяють три рівні м.: рівень підсилення існуючих в свідомості людей необхідних маніпуляторові ідей, установок, мотивів, цінностей, норм; рівень часткових, малих змін поглядів на цю чи іншу подію, процес, факт, що також здійснює вплив на емоційне і практичне відношення до конкретного вища; рівень корінної, кардинальної зміни життєвих установок шляхом повідомлення об'єктові сенсаційних, драматичних, надзвичайно важливих для нього відомостей. Фахівці війни психологічної вважають, що за допомогою маніпулювання можна досягнути швидкої зміни життєвих установок в основному на перших двох рівнях впливу. Кардинальні зміни поглядів однієї людини, групи людей або соціальної спільноти потребують, за їхньою думкою, комплексного впливу на свідомість протягом тривалого часу. Установлено також, що більш обізнаними людьми важче маніпулювати. Тому об'єкту маніпулювання подають сурогат — урізану, скорочену інформацію, і тільки таку, що відповідає меті впливу психологічного. М. с. включає ряд способів, деякими з яких є: спосіб інформаційного перевантаження; спосіб дозування інформації; it спосіб великої брехні; спосіб своєчасної брехні; спосіб змішування правдивих фактів із найрізноманітнішими припущеннями, гіпотезами, слухами; спосіб зволікання; спосіб зворотного удару і т. ін.

МАНІПУЛЯТОР /манипулятор/ — 1) Людина, що робить різні маніпуляції. 2) Суб'єкт маніпулювання свідомістю.

МАНІПУЛЯЦІЯ /манипуляция/ [keying, manipulation] (франц. manipulation) — 1) Складний прийом, дії над будь-чим при роботі руками, ручним способом. 2) Будь-яка складна дія.

М. амплітудна /м. амплитудная/ [amplitude m.] — маніпуляція несучої, при якій параметром, що

змінюється, є амплітуда коливань.

М. несучої /м. несущей)/ [keying, manipulation] — модуляція несучої сигналом дискретним.

М. фазова /м. фазовая/ [phase-shift k.] — маніпуляція несучої, при якій параметром, що змінюється, є фаза коливань.

М. фазова відносна /м.m1004 фазовая относительная/ [differential phase-shift k.] — маніпуляція фазова, при якій значення сигналу модулюючого визначає значення фази несучої радіочастотного сигналу посилки, що передається, відносно фази попередньої несучої цієї ж частоти посилки.

М. частотна /м. частотная/ [frequency-shift k.] — маніпуляція несучої, при якій параметром, що змінюється є частота коливань.

МАРКЕР /маркер/ [mark, marker, token] (франц. marqueur, від marquer — робити мітку) — 1) Мітка в повідомленні, що передається, яка визначає його початок або кінець. 2) Мітка на носії інформації, що позначає початок або кінець даних або їхньої частини (блока). 3) Символ заданого виду, який використовується для позначення конкретної позиції на поверхні візуалізації.

М. доступу /м. доступа/ [access t., security t.] — ієрархічна ознака об'єкта доступу, яка визначається категорією конфіденційності (секретності) інформації, що міститься в блоці даних об'єкта.

МАРКЕТИНГ /маркетинг/ [marketing] (від англ. market — ринок) — 1) Система організації господарської діяльності, заснована на вивченні ринкового попиту, можливостей збуту продукції, реалізації послуг. 2) В комунікативістиці — комерційна діяльність у сфері розповсюдження й реалізації продукції індустрії інформаційної з метою досягнення максимальної вигоди на ринках збуту, що створюється з урахуванням мінливого попиту споживачів.

М. політичний /м. политический/ [political m.] — важливий вид технології політичної, що являє собою комплексну систему методів і прийомів цілеспрямованої дії на різноманітні спільноти людей з метою донести до них вигідну для суб'єкта влади або політики інформацію в найбільш доступній для сприйняття формі і по найбільш ефективних каналах. Основу м. п. складають "політичне ринкознавство", глибоке і уважне

вивчення політичних потреб виборців та інших діючих сил, створення передумов для перетворення їхніх потреб у реальний політичний "попит" на конкретного політика, політичну програму і наступне задоволення цього попиту.

МАРШРУТ /маршрут/ [route] (нім. Marschroute, від франц. marche — шлях і route — хід) — 1) Заздалегідь намічений або встановлений шлях руху людей чи транспортних засобів. 2) Шлях між двома вершинами графа. 3) Шлях передавання повідомлень між вузлами і терміналами обчислювальної мережі.

МАРШРУТИЗАТОР /маршрутизатор/ [router] — пристрій рівня мережного моделі ISO/OSI, що об'єднує декілька мереж обчислювальних локальних в одну мережу, і забезпечує передавання даних з однієї мережі в іншу. На відміну від мостів, що пересилають пакети, використовуючи таблиці фізичних адрес (наприклад, адрес Ethernet), м. пересилають пакети, використовуючи таблиці логічних адрес (наприклад, адрес IP).

МАРШРУТИЗАЦІЯ /маршрутизация/ [routing] — процес визначення шляху для передавання даних від відправника до одержувача. Алгоритми м., необхідні для оновлення таблиці маршрутизації, яка би відповідала потоковій топології мережі, реалізуються в протоколах маршрутизації. Виходячи з різних критеріїв оцінки алгоритмів м., можна виділити наступні види м.: статична, динамічна, внутрішньодоменна, міждоменна, однорівнева, ієрархічна, централізована, розподілена, одношляхова, багатошляхова, м. хостом, м. маршрутизатором, канальна (м. за станом каналу), векторна і примусова.

МАС-МЕДІА /масс-медиа/ [mass media] (від маса і медіа) — засоби масової інформації. Значення терміну свідчить про те, що багато особливостей масових засобів інформаційних зв'язків історично зумовлені розвитком культури і соціальних відносин в умовах ринкового виробництва на базі індустріального прогресу, які створили об'єктивні передумови для перетворення інформації в предмет купівлі-продажу у формах дешевого й популярного товару, наділеного трьома основними функціями: розважальність, розповсюдження новин про поточні події й рекламування новинок торгівлі та послуг. Завдяки цьому процесу в XX сторіччі преса, радіо, кіно, телебачення та інші інформаційні засоби зв'язку, розраховані на широку ау-

диторію, органічно сполучаються з різноманітними економічними структурами індустріального розвитку суспільства, що сприяє його успіху і регуляції. Унаслідок електронно-комп'ютерної революції здійснюється концентрація й монополізація інформаційних засобів, які набувають значення рушійних факторів розвитку і культури масової і масового комсьюмеризму в глобальних масштабах. В цьому можна бачити демократизацію суспільних відносин, проте монополізація інформаційних засобів, яка передбачає зосередження інформаційного капіталу в лоні приватного бізнесу, що приносить йому доходи, суперечить суспільній природі інформаційних зв'язків. До сучасних ЗМІ в комунікативістиці відносять — пресу (газети, журнали, книги), радіо, телебачення, кінематограф, звукозаписи, відеозаписи, відеотекс, телетекст рекламні щити й панелі, домашні відеоцентри, що сполучають телевізійні, телефонні, комп'ютерні та інші лінії зв'язку. Усім цим засобам властиві наступні якості, що об'єднують їх: спрямованість до масової аудиторії, приступність безлічі людей, корпоративний характер виробництва й розповсюдження інформації. Виходячи з цього ЗМІ визначають як форму соціального впливу через інформаційні повідомлення.

МАСА /масса/ [mass] (від англ. massa — шматок, брила, від грец. $\mu\acute{\alpha}\xi\alpha$ — тісто) — в комунікативістиці — термін, що використовується для позначення великої групи людей, різнорідної з точки зору належності до тих чи інших соціально-демографічних прошарків і вікових особливостей, але більш однорідної за своїми смаками, інтересами і головне — потягом до мас-медіа і культури масової, що формують для них стандартний уклад життя й мислення. Вирішальну роль у цьому процесі відіграють, з однієї сторони, розвиток капіталістичних ринкових відносин, а з іншої — найновіші електронні аудіовізуальні засоби масової інформації, що знаходяться в системній залежності від атрибутики масовості споживацького суспільства.

МАСИВ /массив/ [array] — пойменована сукупність однотипних (логічно однорідних) елементів, упорядкованих за індексами, що визначають положення елемента в масиві.

МАСКА /маска/ [mask] (франц. masque, з італ. máschera, від араб. масхара — насмішка) — спеціальна накладка з якимось зображенням.

М. вертикальні /м. вертикальные/ — маски оптичні штучні, призначені для захисту об'єктів від

спостерігання із землі.

М. деформуючі /м. деформирующие/ — маски оптичні штучні, призначені для створення у спостерігача неправильного уявлення про форму об'єкта, що підлягає захисту.

М. оптичні штучні /м. оптические искусственные/ — металеві або дерев'яні каркаси, що накриваються суцільним або сіткоподібним (транспарантним) покриттям. В залежності від форми маски і способу її розташування біля об'єкта маскування розрізняють наступні типи оптичних масок: маски-навіси; маски вертикальні; перекриття маски; маски похилі; маски радіопрозорі; маски деформуючі. М. о. ш. виготовляються у вигляді збірних маскувальних комплектів багаторазового використання, що не впливають на навколишнє середовище та можуть використовуватися разом з іншими способами захисту.

М. перекриття /м. перекрытия/ — маски оптичні штучні, що складаються з каркаса і маскувального покриття, які повністю закривають об'єкт. Застосовуються, насамперед, для захисту об'єктів, що перевозяться на відкритих платформах.

М. похилі /м. наклонные/ — маски оптичні штучні, що використовуються для приховування тіней об'ємних об'єктів, за довжиною яких з врахуванням положення сонця можна визначити висоту об'єктів при спостереженні зверху (з літаків і космічних апаратів).

М. радіопрозорі /м. радиопрозрачные/ — маски оптичні штучні, що виготовляються з радіопрозорих матеріалів (склопластику, пінопласту та ін.), як правило, у вигляді кулі, для приховання демаскуючих ознак і фізичного захисту антен.

М.-навіси /м.-навесы/ — маски оптичні штучні, призначені для приховування об'єктів, розташованих на відкритих зверху площадках та їхнього захисту від спостереження за допомогою засобів спостереження, що розташовуються на верхніх поверхах висотних будівель, височинах і горах, на літаках і космічних апаратах.

МАСКАРАД /маскарад/ [masquerade attack] — вид атаки, при якій один об'єкт системи видається за інший. Прикладом такої атаки може бути перехоплення даних процедури автентифікації об'єкта та вико-

ристання її у подальшому для здійснення незаконної авторизації.

МАСКІРАТОР /маскиратор/ — 1) Пристрій, що реалізує детерміновані статичні аналого-цифрові засекречені перетворення. Захищає мовний сигнал від прямого прослуховування. 2) Скремблер з інверсією спектру.

МАСКУВАННЯ /маскирование/[masking] (від франц. masquer — приховувати) — 1) Метод інформаційного приховування ознак об'єкта спостереження шляхом руйнування його інформаційного портрета. 2) Вид оперативного забезпечення протидії інформаційної шляхом приховування правдивої та впровадження в інформаційні мережі противника фальшивої інформації про свої сили, наміри або дії.

М. акустичного сигналу /м. акустического сигнала/ — спосіб приховування акустичного сигналу енергетичного, заснований на створенні і розповсюдженні маскувальних звукових хвиль у напрямках можливого підслухування. Гучність звуку, що сприймається людиною, залежить не тільки від його власної інтенсивності, але і від інших звуків, що діють одночасно на барабанну перетинку вуха. Відповідно до психофізіологічних особливостей сприйняття звуку людиною інтенсивність маскувальних звуків асиметрична. Асиметричність проявляється в тому, що маскувальний звук здійснює відносно невеликий вплив на тони звуку, що маскується, нижчу його власної частоти, але сильно утруднює сприйняття більш високих звуків. Тому для м. а. с. ефективні низькочастотні акустичні шумові сигнали, що створюються шумовими акустичними генераторами.

М. гідроакустичне /м. гидроакустическое/ [hydroacoustic c.] — приховування підводних човнів і надводних кораблів від гідроакустичних засобів розвідки противника. Досягається застосуванням звукоізоляційних і звукопоглинальних засобів, використанням малошумних швидкостей ходу підводного човна і укриття його під шаром скачки (шару води, який різко понижує можливості гідролокаторів з виявлення підводного човна), вимкненням механізмів, що створюють сильний шум, а також застосуванням імітаторів шуму.

М. в оптичному діапазоні /м. в оптическом диапазоне/ — сукупність заходів захисту ознак дема-

скуючих об'єкта, спрямованих на зменшення величини контраст/фон. Використовуються наступні методи маскування: маскування особливостями місцевості; маскування обробленням місцевості; маскування пофарбуванням; маскування штучними масками; маскування повітряними пінами.

М. деформуючим пофарбуванням /м. деформирующим окрашиванием/ — маскування пофарбуванням, що передбачає нанесення на об'єкт плям неправильної геометричної форми 2–3 кольорів, які імітують світлові плями навколишнього середовища. М. д. п. широко застосовується для маскування військової техніки і людей у польовому обмундируванні. Колір плям відповідає основним кольорам місцевості для сезону (літо, зима).

М. захисним пофарбуванням /м. защитным окрашиванием/ — маскування пофарбуванням об'єкта одноколірною фарбою під колір і середню яскравість фону навколишнього середовища і предметів біля об'єкта, що маскується.

М. імітаційним пофарбуванням /м. имитационным окрашиванием/ — маскування пофарбуванням, при якому колір і характер плям на поверхні об'єкта підбирається під кольори навколишньої місцевості, об'єктів або предметів в місці розташування об'єкта, що підлягає захисту. В цьому випадку забезпечується найбільше приховування.

М. обробленням місцевості /м. обработкой местности/ — маскування в оптичному діапазоні на основі додаткового оброблення місцевості з метою підвищення її маскувальних властивостей. Воно передбачає дернування (нарізання дерну) і висівання трави, створення огорож із живої рослинності, хімічного оброблення ділянок місцевості. Таке маскування спрямоване на зміну фону під основний колір об'єкта. Його застосовують коли відсутні або недостатні для маскування природні умови.

М. оптико-електронне /м. оптико-электронная/ [ЕО с.] — комплекс заходів, спрямованих на приховування військових об'єктів від оптичних (оптико-електронних) засобів розвідки противника. Здійснюється шляхом: використання маскувальних властивостей місцевості, темного часу доби, а також метеорологічних умов, які обмежують можливості цих засобів; проведення заходів з світломаскування; використання укрит-

тів, штучних масок, димів, аерозолів; улаштування фальшивих споруд та об'єктів.

М. особливостями місцевості /м. особенностями местности/ — маскування в оптичному діапазоні на основі приховування з використанням маскувальних властивостей місцевості (нерівностей ландшафту, складок місцевості, пагорбів, гір, стовбурів і крон дерев і т. ін.). Проте для реалізації цього способу необхідна наявність в місці знаходження об'єкта відповідних природних масок. Крім того, маскувальні можливості залежать від пори року. Ефективність маскування оцінюється відношенням площі, що закривається, наприклад, деревами, до загальної площі зони контрольованої.

М. повітряними пінами /м. воздушными пенами/ — маскування світлонепроникливими одно- і багатоколірними повітряними пінами, які швидко наносяться за допомогою піногенераторів на об'єкти, забезпечуючи їхнє ефективне маскування в широкому діапазоні довжин хвиль протягом декількох годин.

М. пофарбуванням /м. окрашиванием/ — маскування в оптичному діапазоні, що здійснюється шляхом нанесення на поверхню об'єкта фарб, підібраних за кольором і яскравістю, які є близькими до фону. Розрізняють наступні види м. п.: маскування захисним пофарбуванням, маскування деформуючим пофарбуванням, маскування імітаційним пофарбуванням. М. п. просте в реалізації, але ефект маскування залежить від сезону та інших змін навколишнього середовища.

М. радіоелектронне (РЕМ) /м. радиоэлектронная (РЭМ)/ [radioelectronic c.] — комплекс технічних та організаційних заходів, спрямованих на зниження ефективності розвідки радіоелектронної противника. РЕМ поділяється на маскування радіотехнічне, радіолокаційне, гідроакустичне і оптико-електронне.

М. радіолокаційне /м. радиолокационная/ [radar c.] — комплекс організаційно-технічних заходів, здійснюваних з метою перешкодити визначенню радіолокаційною станцією противника складу і дислокації об'єктів, а також зниження дальності дії по них РЛС противника. М. р. застосовується також для введення противника в оману шляхом створення фальшивих цілей для його РЛС спостереження. Базується на обмеженій роздільній здатності РЛС та на використанні різних штучних відбивачів, які на екранах РЛС

дають відмітки, що мало відрізняються від відміток об'єктів, які маскуються.

М. радіотехнічне /м. радиотехническая/ — маскування дійсної дислокації радіопередавальних пристроїв, здійснюване для зниження ефективності радіорозвідки противника. М. р. здійснюється шляхом скорочення часу роботи на передавання, випромінювання мінімально необхідної потужності, використання спрямованого передавання, зміни робочих частот, встановлення режиму радіомовчання (повного припинення роботи на передавання), використання радіодезінформації.

М. штучними масками /м. искусственными масками/ — маскування за допомогою спеціальних конструкцій — масок оптичних штучних.

МАТЕРІАЛ /материал/ [material, stuff] — 1) Те, з чого що-небудь виготовляють, виробляють, будують тощо. 2) Різноманітні відомості, дані, посібники і т. ін., що їх використовують як основу, джерело для чого-небудь, як доказ чогось.

М. акустичні /м. акустические/ [acoustical m.] — матеріали, призначені для пониження шуму і створення оптимальних умов чутності в приміщеннях; поділяються на звукопоглинальні і звукоізоляційні.

М. звукоізоляційні /м. звукоизоляционные/ [sound insulator] — матеріали акустичні, призначені для використання в конструкціях міжповерхових перекриттів, у внутрішніх стінах і перегородках, а також у вигляді віброізоляційних прокладок під машини та обладнання. М. з. виготовляють з штучних волокон (мінераловатні і скловолокнисті мати і плати), а також з еластичних газонаповнених пластмас (пінополіуретан, пінополівінілхлорид і т. ін.). Для звукоізоляції застосовують також штучні прокладки з литої або губчастої гуми.

М. звукопоглинальні /м. звукопоглощающие/ [sound-absorbing m.] — матеріали, що використовуються для перетворення кінетичної енергії звукової хвилі в теплову енергію. Звукопоглинальні властивості матеріалів оцінюються коефіцієнтом звукопоглинання. Використовуються для створення засобів звукопоглинання хвилі акустичної. За конструктивними властивостями розрізняють рихлі акустичні матеріали, плитні матеріали, акустичну штукатурку і резонансні поглиначі у вигляді панелей і щитів з дерева та

інших матеріалів.

М. магнітострикційні /м. магнитострикционные/ [magnetostrictive m.] (від магніт і лат. strictio — стиснення, натягування) — феромагнітні метали і сплави, а також ферити, що мають добре виражені магнітострикційні властивості (змінюють форму і розміри при намагнічуванні) і застосовуються для виготовлення магнітострикційних акустоелектричних перетворювачів електромагнітної енергії в механічну й навпаки (випромінювачі акустичних коливань, датчики тиску, фільтри й інші прилади).

М. п'єзоелектричні /м. пьезоэлектрические/ [piezoelectric m.] (від грец. $\pi\iota\acute{\varepsilon}\zeta\omega$) — кристалічні речовини, в яких при стисканні або розтяганні в певних напрямах виникає електрична поляризація навіть при відсутності електричного поля (прямий п'єзоефект). Наслідком прямого п'єзоефекту є зворотний п'єзоефект — поява механічної деформації внаслідок дії електричного поля. Зв'язок між механічними і електричними змінними (деформацією і електричним полем) носить в обох випадках лінійний характер. М. п. використовуються для виготовлення перетворювачів п'єзоелектричних. М. п. є природно або штучно вирощені монокристали (кварц, дігідрофосфати калію і амонію, сегнетова сіль та ін.) і полікристалічні тверді розчини, попередньо піддані поляризації в електричному полі (п'єзокераміка).

М. радіопоглинальні /м. радиопоглощающие/ — неметалічні матеріали, які в результаті взаємодії з радіохвилями здійснюють їхнє поглинання, розсіювання і інтерференцію. У відповідності до принципів дії м. р. поділяють на градієнтні (поглинальні), інтерференційні і комбіновані. Застосовуються для маскування від радіолокаційного виявлення різноманітних об'єктів; екранування радіоприймальних пристроїв; обладнання спеціальних камер, в яких випробовуються радіоелектронні засоби; біологічного захисту від впливу потужного радіовипромінювання. Розрізняють широкодіапазонні і вузькодіапазонні м. р. Широкодіапазонні матеріали ефективно поглинають електромагнітну енергію при відношенні максимальної до мінімальної довжини падаючої хвилі 3–5; вузькосмугові, якщо це відношення не перевищує 1,5–2. В ряді випадків знаходять застосування матеріали, що працюють практично тільки на фіксованій хвилі.

М. радіопрозорі /м. радиопрозрачные/ [radio transpa rent m.] — конструкційні діелектрики з дво-

сторонньою провідністю, що пропускають без суттєвих утрат і спотворень електромагнітні коливання радіочастотного діапазону. Призначаються в основному для виготовлення обтічників, що захищають антени радіолокаційних станцій та інші радіотехнічні засоби від впливу навколишнього середовища.

М. світлочутливі /м. светочувствительные/ [light-sensitive m., sensitive m.] — матеріали, що являють собою тонку желатинову плівку, що містить світлочутливі речовини, на целулоїдній плівці, скляній пластині або цупкому папері. До м. с. відносяться: фото- і кіноплівка, фотопластини, фотопапір. Характеризуються чутливістю та здатністю роздільною об'єктивною.

М. фотографічні /м. фотографические/ [photographic m.] — див. матеріали світлочутливі.

МАТРИЦЯ /матрица/ [matrix] (нім. Matrize, від лат. matrix — матка) — в математиці — сукупність чисел (елементів), розміщених у прямокутній таблиці у вигляді n стовпців і m рядків. Якщо $m = n$, то м. називається квадратною порядку n.

М. встановлення повноважень /м. установки полномочий/ — матриця, утворена в захищеній ділянці пам'яті системи обчислювальної, елементами якої є біти, що відповідають певним діям, які можуть бути виконані з термінала при зверненні до елемента даних. Якщо необхідно, то елементи матриці можуть містити і покажчик на відповідні процедури. Ці процедури виконуються при кожній спробі доступу з даного термінала до заданого елемента даних і можуть обмежувати доступ до інформації в залежності від певних умов.

М. доступу /м. доступа/ [access m.] — n-мірна таблиця, вздовж кожного виміру якої відкладені ідентифікатори об'єктів системи комп'ютерної одного типу (об'єктів-користувачів, об'єктів-процесів чи об'єктів пасивних), і містить як елементи права доступу за кожним із типів об'єктів.

МАШИНА /машина/ [machine, computer] (франц. machine, від лат. machina — пристрій, знаряддя, споруда) — сукупність механізмів, що здійснюють задані доцільні рухи для перетворення енергії, виконання робіт або для збирання й оброблення інформації.

М. абонентська /м. абонентская/ [custome c.] — ЕОМ, яка споживає або надає ресурси мережі обчи-

слювальної.

М. баз даних /м. баз данных/ [database c.] — спеціалізований комплекс засобів апаратних, програмних та мікропрограмних, призначений для виконання функцій керування базами даних. Розрізняють коміркові, допоміжні, інтегровані й асоціативні м. б. д.

М. баз даних допоміжна /м. баз данных вспомогательная/ — машина баз даних, яка реалізується виділенням обчислювальних ресурсів у вигляді автономного процесора для виконання частини або усіх функцій системи керування базою даних. Роль такої машини може виконувати універсальна або спеціалізована ЕОМ.

М. баз даних інтегрована /м. баз данных интегрированная/ [integrated database c.] — машина баз даних, що являє собою комплекс функціонально-спеціалізованих пристроїв, кожний з яких виконує одну або декілька функцій системи керування базою даних.

М. віртуальна /м. віртуальная/ [virtual m.] — функціональний еквівалент деякої уявної ЕОМ із заданою конфігурацією, який моделюється програмно-апаратними засобами конкретної реальної ЕОМ з такою ж архітектурою, яка необов'язково співпадає за конфігурацією з віртуальною.

М. інтерфейсна /м. интерфейсная/ [interface c.] — ЕОМ, яка забезпечує взаємодію вузлів мережі обчислювальної.

М. обчислювальна /м. вычислительная/ [computer] — пристрій або комплекс пристроїв, призначених для механізації або автоматизації алгоритмічного оброблення інформації. Існують три класи машин: машини обчислювальні цифрові, машини обчислювальні аналогові та машини обчислювальні гібридні.

М. обчислювальна аналогова (АОМ) /м. вычислительная аналоговая (АВМ)/ [analog c.] — машина обчислювальна безперервної дії, призначена для оброблення аналогових даних. При вирішенні певного класу задач (наприклад, диференціальних рівнянь) мають більшу швидкодію, ніж машини обчислювальні цифрові.

М. обчислювальна гібридна (аналого-цифрова) /м. вычислительная гибридная (аналого-

цифровая) / [hybrid c.] — машина обчислювальна, в якій поєднуються властивості обчислювальних машин аналогових й цифрових.

М. обчислювальна цифрова /м. вычислительная цифровая/ [digital c.] — див. ЕОМ.

М. термінальна /м. терминальная/ [terminal c.] — ЕОМ, яка забезпечує взаємодію терміналів з мережею обчислювальною.

М. термінально-комутаційна /м. терминально-коммуникационная/ — ЕОМ, яка забезпечує маршрутизацію даних в мережі обчислювальній і взаємодію терміналів з мережею.

МЕДІА /медиа/ [media] (множина від англ. medium — засіб) — в теорії суспільства масового — системи інформаційні, які залежать від головних атрибутів цього суспільства — консьюмеризму і конформізму, але разом з тим і підтримують їх із-за можливостей маніпулювання свідомістю і психікою широкої аудиторії.

М. електронні нові /м. электронные новые/ [new electronic m.] — термін, що використовується в галузі супермагістралей інформаційних для акцентування радикальних відмінностей інтерактивних телекомп'ютерних мультимедійних засобів зв'язку, на яких базуються ці супермагістралі, від попередніх видів засобів масової інформації — медіа звичайних. Вважається, що н. е. м. мають майже безмежні можливості для передавання будь-якої інформації будь-яким її відправником в різних напрямках. Це веде до такого збільшення маси інформації, що передається, і маси користувачів, при якому самі поняття медіа і комунікації масові набувають нові смислові відтінки. Якщо раніше в процесі передавання інформації за допомогою ЗМІ повинні були брати участь спеціалісти, які професіонально підготовлені для роботи з аудіовізуальною технікою, то тепер у ньому можуть брати участь усі бажаючі, якщо вони мають доступ до супермагістралі (наприклад, до Інтернету). При цьому одержувачі й відправники інформації можуть мінятися ролями, а відмінності між суспільними й приватними формами комунікації втрачають свої колишні критерії, оскільки в центрі уваги постають нові ролі служб і функцій зв'язку.

М. звичайні /м. обычные/ [conventional m.] — друковані видання, радіо й телебачення. Термін з. м. з'явився після появи медіа електронних нових.

МЕДІАКРАТІЯ /медиакратия/ [mediacracy] (від медіа і грец. *κράτøς* — сила, влада) — влада інформаційних засобів зв'язку. Термін використовується у зв'язку з поняттям суспільства інформаційного, в умовах якого під контролем медіа можуть опинитися усі сфери — від економіки, побуту, дозвілля й освіти до політики і міжнародних відносин. Незважаючи на те, що поняття м. засноване на абсолютизації ролі ЗМІ, його прийняття сприяє розповсюдженню концепцій, які стимулюють фетишизацію мас-медіа і їхню маніпулятивну діяльність, спрямовану на створення мнимих уявлень про реальність і майбутнє.

МЕЛАНХОЛІК /меланхолик/ [melancholiac, melancholiac person] (від грец. *μελαγχøλικός*) — 1) Один з видів темпераменту, якому відповідає слабкий гальмівний тип вищої нервової діяльності. 2) Людина, в якій переважає пригнічений, сумний настрій.

МЕНЕДЖМЕНТ /менеджмент/ [management] (англ. management — управління, завідування, організація) — мистецтво управління інтелектуальними, фінансовими, матеріальними ресурсами.

МЕРЕЖА /сеть/ [network] — 1) Зв'язковий орієнтований граф. 2) Засіб теледоступу — мережа передавання даних, мережа обчислювальна.

М. агентурна /с. агентурная/ [secret-service n.] — група агентів, зв'язаних між собою і підпорядкованих агенту-груповоду, який, у свою чергу, підзвітний співробітнику розвідки (резиденту) держави, на яку працює мережа. Див. також група агентурна.

М. електрозв'язку /с. електросвязи/ [computation n.] — технологічні системи, які забезпечують один або декілька видів передач: телефонну, телеграфну, факсимільну, передачу даних і інших видів документальних повідомлень, в тому числі й обмін між ЕОМ, телевізійне, звукове та інші види радіо- і проводового мовлення.

М. зв'язку /с. связи/ [communication n.] — те ж, що мережа комунікаційна.

М. зв'язку загального користування /с. связи общего использования/ — складова частина взаємозв'язаної мережі зв'язку держави, відкрита для користування всім фізичним і юридичним особам, в

послугах якої цим особам не може бути відмовлено.

М. інформаційна /с. информационная/ [information n.] — сукупність систем інформаційних автоматизованих, об'єднаних в єдину мережу за допомогою засобів передавання даних. Користувач має доступ до інформації будь-якої автоматизованої інформаційної системи, що входить до мережі.

М. інформаційна транскордонна /с. информационная трансграничная/ (лат. префікс trans... означає: "крізь", "через") — мережа інформаційна, що перетинає кордони однієї або багатьох держав.

М. інформаційно-обчислювальна (ІОМ) /с. информационно-вычислительная (ИВС)/ [information computer n.] — сукупність зв'язаних лініями зв'язку інформаційно-обчислювальних центрів, призначених для оброблення інформації.

М. інформаційно-обчислювальна корпорації /с. информационно-вычислительная корпорации/ [corporate information computer n.] — основна складова частина системи керування корпорації автоматизованої, що об'єднує наступні елементи: мережі обміну інформацією; мережі обчислювальні локальні і комплекси засобів автоматизації регіональних представництв, підключених до базової мережі; підмережі і комплекси засобів автоматизації підприємств; підмережі робочих груп і т.ін. До особливостей м. і.-о. к. можна віднести: різнорідність технічних засобів і програмного забезпечення; висока доля різнорідних мережних інформаційних технологій; широкий спектр послуг і, як наслідок, збільшення обсягів і якісної різноманітності інформації, що зберігається, обробляється і передається в мережі. Для м. і.-о. к. можуть бути актуальними: з'єднання з глобальними мережами типу Інтернет; приєднання до мереж інших корпорацій в результаті розширення співробітництва (наприклад, міжнародного). Перелічені особливості м. і.-о. к. обумовлюють високу ступінь уразливості інформації, що зберігається, обробляється й передається в такій мережі.

М. комунікаційна /с. коммуникационная/ [communication n.] — мережа передавання даних, утворена множиною взаємозв'язаних комунікаційних модулів — вузлів зв'язку і пунктів абонентських.

М. комутації пакетів (з комутацією пакетів) /с. коммутации пакетов (с коммутацией пакетов/

[packet switching n.] — мережа передавання даних, в якій повідомлення, що передається, розділяється на декілька спеціально оформлених порцій — пакетів, кожний з яких передається незалежно, часто навіть різними каналами зв'язку.

М. корпоративна /с. корпоративная/ [enterprise n.] (від лат. corporatio — спілка) — мережа обчислювальна локальна, що функціонує в масштабі великого підприємства, закладу; інтермережа відособленого використання. Див. також інтрамережа.

М. обміну інформацією (МОІ) /с. обмена информацией (СОИ)/ [information n.] — теж, що інформаційна мережа; складова частина мережі інформаційно-обчислювальної. Див. також. мережа інформаційно-обчислювальна корпорації.

М. обчислювальна /с. вычислительная/ [computer n.] — сукупність мережі передавання даних, взаємозв'язаних з нею ЕОМ та необхідних для реалізації цього зв'язку програмного забезпечення і (або) технічних засобів та призначена для розподіленого оброблення даних (інформації).

М. обчислювальна локальна (ЛОМ) /с. вычислительная локальная (ЛВС)/ [local area n. (LAN)] (лат. localis, від locus — місце) — 1) Мережа обчислювальна, яка підтримує в межах певної території один або декілька надшвидкісних каналів передавання цифрової інформації, і надається для короткочасного монопольного використання пристроям, що приєднуються. 2) Обчислювальна мережа, вузли якої розташовані на невеликій відстані один від одного.

М. передавання даних (МПД) /с. передачи данных (СПД)/ [data transmission n.] — сукупність кіл передавання даних та пристроїв комутації, що дозволяють здійснювати взаємне з'єднання кінцевого обладнання даних.

М. передавання даних інтегральна /с. передачи данных интегральная/ [integrated communication n.] — мережа комунікаційна, що забезпечує на одному і тому ж обладнанні як комутацію пакетів, так і комутацію каналів.

М. передавання даних синхронна /с. передачи данных синхронная/ [synchronous data n.] — мере-

жа передавання даних, що використовує метод синхронізації передавання між вузлами комутації або між вузлом комутації і апаратурою передавання даних.

М. приватні (особисті) віртуальні /с. частные (личные) виртуальные/ [Private Virtual Network (PVN, VPN)] — 1) Зашифрований або інкапсульований (див. інкапсуляція) процес комунікації, який безпечним чином передає дані з однієї точки в іншу. Безпека цих даних забезпечена стійкою технологією шифрування, і дані, що передаються, проходять через відкриту, незахищену, маршрутизовану мережу. 2) Розподілена мережа корпоративна, яка використовує Інтернет для передавання даних та спеціальні технології захисту каналів зв'язку між своїми вузлами. Таким чином, в Інтернеті створюється захищена підмережа, між абонентами якої організований захищений (конфіденційний, цілісний) зв'язок. Такі захищені канали найчастіше реалізуються за допомогою методів захисту криптографічних інформації, зокрема, застосуванням шифраторів IP-пакетів.

М. розподілена /с. распределенная/ [distributed n.] — мережа обчислювальна, всі пари вузлів якої з'єднані безпосередньо або через резервні канали зв'язку, що проходять через проміжні вузли.

М. транспортна /с. транспортная/ [transport n.] — частина мережі обчислювальної, яка виконує функції рівнів транспортного, мережного, канального і фізичного і має фізичні засоби з'єднання та зв'язані з ними станції.

МЕТА /цель/ [object] — те, до чого хтось прагне, чого хоче досягти; ціль.

М. інформаційної боротьби /ц. информационной борьбы/ — забезпечення необхідного ступеня власної безпеки інформаційної і максимальне пониження рівня інформаційної безпеки конфронтуючої сторони. Досягнення м. і. б. здійснюється шляхом вирішення ряду завдань, основними з яких є ураження об'єктів сфери інформаційної конфронтуючої сторони і захист власної інформації. Мета і завдання інформаційної боротьби визначають її зміст, а також і структуру теорії інформаційної боротьби. При цьому на зміст інформаційної боротьби великий вплив здійснює ряд факторів, серед яких виділяють політичний, економічний,

духовний, власне воєнний і інформаційний фактори.

М. інформаційної загрози /ц. информационной угрозы/— активізація алгоритмів, відповідальних за порушення звичного режиму функціонування, тобто за виведення системи інформаційної за межі допустимого стану.

М. психологічної війни /ц. психологической войны в./ — 1) Зміна в бажаному напрямку психологічних характеристик людей (поглядів, думок, ціннісних орієнтацій, настроїв, мотивів, установок, стереотипів поведінки), а також групових норм, масових настроїв, суспільної свідомості в цілому. 2) Спотворення інформації, що одержується політичним керівництвом, командуванням і особовим складом збройних сил противника, і нав'язування їм фальшивої або беззмістовної інформації, яка позбавляє його можливості правильно сприймати події або поточну обстановку і приймати правильні рішення. М. п. в. призводить до вирішення наступних головних завдань: запобігання можливого воєнного конфлікту; ослаблення морального духу особового складу збройних сил і цивільного населення противника; схилення його до відмови від участі в бойових діях; створення передумов для досягнення намічених воєнно-політичних цілей з мінімальними людськими втратами і матеріальними затратами. Мету і завдання психологічної війни можна класифікувати й уточнювати відповідно до умов ведення психологічної війни (мета й завдання психологічної війни у мирний, воєнний і післявоєнний час, а також в ході миротворчих операцій), об'єктів психологічної війни (військовослужбовців, цивільного населення, вищого воєнно-політичного керівництва противника і його союзників, а також світової суспільної думки й країн-союзників), часу ведення психологічної війни (стратегічні, оперативні, тактичних).

МЕТАЛОДЕТЕКТОРИ (МЕТАЛОШУКАЧІ) /металлодетекторы (металлоискатели)/ [metals detector] — засоби виявлення елементів закладок, що реагують на наявність в зоні пошуку електропровідних матеріалів, насамперед, металів, і дозволяють виявляти корпуси або інші металеві деталі закладки. Принципи роботи м. засновані на зміні і селекції змін характеристик сигналів, що наводяться у вимірювальній котушці м. полями вихрових струмів в об'єкті, що досліджується, а також змінами активного і

реактивного опорів котушки. Вихрові струми виникають при опроміненні об'єкта магнітним полем, що створюється іншою, так званою пошуковою котушкою м. На цю котушку поступає аналоговий або імпульсний сигнал від відповідного генератора м. Наведені у вимірювальній котушці сигнали підсилюються і аналізуються спеціальним мікропроцесором. Для виявлення закладок застосовуються в основному ручні м. Вимірювальна і пошукова котушки в них можуть бути виготовлені у вигляді тороїда діаметром порядку 140–150 мм, закріпленого на корпусі ручки або безпосередньо в корпусі м. М. має звуковий і світловий індикатори, регулятор настройки чутливості; живлення ручних металошукачів здійснюється від хімічних джерел струму.

МЕТОД /метод/ [method] (від грец. *μέϑøδς* — шлях дослідження, спосіб пізнання) — 1) Система принципів та способів пізнавально-теоретичної і практичної діяльності. 2) Спосіб, прийом або система прийомів для досягнення якої-небудь мети, для виконання певної операції.

М. вивчення документів /м. изучения документов/ — метод вивчення об'єктів психологічної війни на основі використання документів, в тому числі архівних. В мирний час такими документами можуть бути: офіційні державні документи ймовірного противника та інших держав; аналітичні матеріали спеціалізованих науково-дослідних організацій і закладів; архівні джерела; вітчизняна й зарубіжна преса; спеціальна література; передачі радіо й телебачення і т.ін. В бойовій обстановці найважливішими джерелами інформації психологічного характеру є відомості розвідувальні і трофейні документи, матеріали радіоперехоплення і т. ін. Фахівці знаходять в них відомості, які характеризують політичний і морально-психологічний стан військовослужбовців і населення противника, а також дані, необхідні для підготовки пропагандистських і інформаційно-довідкових матеріалів.

М. вивчення об'єктів психологічної війни /м. изучения объектов психологической войны/ — система методів, що використовується для вивчення об'єктів психологічної війни. До м. в. о. п. в. відносяться методи спостереження, експерименту, опитування, вивчення документів, радіоперехоплення, узагальнення

незалежних характеристик, узагальнення соціологічної й психологічної статистики.

М. доступу до інформації /м. доступа к информации/ — способи, прийоми забезпечення доступу до інформації. Можна поділити на три групи: проникнення розвідника до джерела інформації фізичне; залучення до співробітництва з органами розвідки осіб, які мають легальний або нелегальний доступ до інформації, що цікавить розвідку; дистанційне знімання інформації з носія (див. добування інформації дистанційне).

М. експерименту /м. эксперимента/ — специфічний метод вивчення об'єктів психологічної війни, який передбачає активне втручання фахівців психологічної війни у діяльність об'єкта, що вивчається, з метою одержання інформації. Для цього об'єкт ставиться у відповідні умови, а потім здійснюється спостереження за його діями. Загальна логіка експерименту полягає у тому, щоб поставити об'єкт вивчення у незвичайну для нього ситуацію. Розрізняють штучний і натурний експеримент. Недоліком штучного експерименту є те, що він здійснюється при обмежених можливостях (фактично його можна проводити тільки на військовополонених, або разом з бойовими частинами в ході спеціальних операцій). До того ж об'єкти майже завжди здогадуються, що їх вивчають. Натурний експеримент здійснюється в умовах, коли об'єкти вивчення знаходяться у своїх звичайних умовах, і не підозрюють про те, що за ними пильно спостерігають.

М. доступу до інформації /м. доступа к информации/ — способи, прийоми забезпечення доступу до інформації. Їх можна поділити на три групи: фізичне проникнення зловмисника до джерела інформації; залучення до співробітництва з органами розвідки або зловмисниками осіб, які мають легальний або нелегальний доступ до інформації, що цікавить розвідку; дистанційне знімання інформації з носія (див. добування інформації дистанційне).

М. енергетичного приховування /м. энергетического скрытия/ — метод приховування інформації, що передбачає застосування способів і засобів захисту інформації, які виключають або утруднюють виконання енергетичної умови розвідувального контакту див. приховування енергетичне.

М. забезпечення інформаційної безпеки /м. обеспечения информационной безопасности/ — су-

купність форм і способів, що утворюють інструмент, за допомогою якого спеціальні органи забезпечення безпеки інформаційної вирішують весь комплекс завдань з захисту життєво важливих інтересів особистості, суспільства і держави. Вони повинні мати чітке юридичне оформлення при розробці нормативних актів, що регулюють діяльність органів інформаційної безпеки. Застосування тих чи інших форм і способів залежить від того, чи є інформаційні загрози наслідком ненавмисних або навмисних дій суб'єктів інформаційного процесу. В першому випадку забезпечення інформаційної безпеки, як правило, здійснюється у формі патронату інформаційного та кооперації інформаційної, а в другому — в формі боротьби інформаційної.

М. захисту /м. защиты/ [protection m.] — система принципів і прийомів, спрямованих на реалізацію функції захисту. М. з. може бути реалізований програмним, програмно-апаратним (апаратно-програмним) або апаратним способом.

М. захисту інформації /м. защиты информации/ — сукупність способів, прийомів або системи прийомів, що запобігають несанкціонованому доступу до інформації. При наявності простих засобів зберігання і передавання інформації можуть бути використані традиційні методи її захисту від зловмисного доступу: обмеження доступу; розмежування доступу; розділення доступу (привілеїв); криптографічне перетворення інформації; контроль і облік доступу; законодавчі заходи. При автоматизованому обробленні інформації у зв'язку із збільшенням обсягів, зосередженням інформації, збільшенням кількості користувачів та іншими причинами, що зумовлюються ускладненням технічних засобів оброблення та різноманітними видами носіїв інформації, одержали розвиток як традиційні, так і нові методи захисту: функціональний контроль, що забезпечує виявлення і діагностику відмов, збоїв апаратури і програмних помилок та помилок людини; підвищення вірогідності (достовірності) інформації; захист інформації від аварійних ситуацій; контроль доступу до внутрішнього монтажу апаратури, ліній зв'язку і технологічних органів керування; розмежування і контроль доступу до інформації; ідентифікація і автентифікація користувачів, технічних засобів, носіїв інформації і документів; захист від ПЕМВН.

М. захисту інформації технічними засобами /м. защиты информации техническими средствами/

— сукупність способів забезпечення захисту інформації для певних варіантів співвідношень між джерелами, носіями інформації та зловмисниками: джерело і носій інформації локалізовані в межах розташування об'єкта захисту і забезпечена механічна перепона від контакту з ними зловмисника або дистанційного впливу на них полів його технічних засобів добування інформації; такі співвідношення енергії носія і завад на виході приймача каналу витоку такі, що зловмиснику не вдається зняти інформацію з носія з необхідною для її використання якістю; замість істинної інформації зловмисник одержує неправдиву, яку він приймає за істинну. Ці варіанти реалізуються наступними способами захисту: перешкоджання безпосередньому проникненню зловмисника до джерела інформації за допомогою інженерних конструкцій і технічних засобів охорони; приховування достовірної інформації; "підсовування" зловмиснику неправдивої (хибної) інформації. У зв'язку з цим розрізняють два основних м. з. і. т. з.: метод охорони джерел інформації і метод приховування інформації.

М. захисту інформаційний /м. защиты информационный/ — метод захисту, що полягає у спеціальному перетворенні інформації, що обробляється в обчислювальній системі.

М. захисту криптографічний /м. защиты криптографический/ [cryptographical m.] — метод захисту інформаційний, що полягає у перетворенні криптографічному інформації.

М. захисту операційний /м. защиты операционный/ — метод захисту інформаційний від доступу несанкціонованого в операційній системі.

М. захисту організаційно-правовий /м. защиты организационно-правовой/ — комплекс організаційних заходів з підтримки безпеки обчислювальної системи та відповідні закони держави в галузі безпеки інформації.

М. захисту технічний /м. защиты технический/ — метод захисту, що полягає у використанні технічних засобів.

М. захисту фізичний /м. защиты физический/ [physical protection m.] — метод захисту, що полягає

в обмеженні фізичного доступу до об'єктів інформаційної системи, що охороняються.

М. зміни інформаційного портрета /м. замены информационного портрета/ — метод інформаційного приховування інформації, яке досягається наступними способами: видалення частини елементів і зв'язків, що створюють вузол інформаційний (найбільш інформаційну частину) портрета; зміни частини елементів інформаційного портрета при збереженні незмінності зв'язків між елементами, що залишилися; видалення або зміна зв'язків між елементами інформаційного портрета при збереженні їхньої кількості. Зміни інформаційного портрета об'єкта викликають зміни зображення його зовнішнього вигляду (видових демаскуючих ознак), характеристик випромінюваних ними полів або електричних сигналів (ознак сигналів), структури і властивостей речовин. Ці зміни спрямовані на приближення ознакових структур об'єкта до оточуючого його фону, в результаті чого понижується контрастність зображення об'єкта по відношенню до фону і погіршуються можливості його виявлення і розпізнавання. Проте при зміні інформаційного портрета інформація може не сприйматися не тільки зловмисником, але і її санкціонованим одержувачем. Для санкціонованого одержувача інформаційний портрет повинен бути відновлений шляхом додаткового передавання йому видалених елементів і зв'язків або алгоритму (ключа) цих змін.

М. інженерного захисту та технічної охорони об'єктів /м. инженерной защиты и технической охраны объектов/ — див. метод охорони джерел інформації.

М. інформаційного приховування /м. информационного скрытия/ — метод приховування інформації, яке досягається зміною або створенням неправдивого (хибного) інформаційного портрета семантичного повідомлення, фізичного об'єкта або сигналу. Розрізняють два види м. і. п.: метод зміни інформаційного портрета та метод трансформації інформаційного портрета. Принципова відмінність інформаційного приховування шляхом зміни інформаційного портрета від інформаційного приховування шляхом трансформації інформаційного портрета в тому, що перший метод спрямований на утруднення виявлення об'єкта з інформацією серед інших об'єктів (фону) (маскування), а другий — на створення на цьому фоні ознак

неправдивого (фальшивого) об'єкта (дезінформацію).

М. навіювання /м. внушения/ — метод психологічного впливу на свідомість особистості або групи людей, який ґрунтується на некритичному (і часто неусвідомлюваному) сприйнятті інформації. При навіюванні спочатку здійснюється сприйняття інформації, що містить готові висновки, а потім на її основі формуються мотиви і установки певної поведінки. У процесі навіювання інтелектуальна (аналітико-синтезуюча) активність свідомості або відсутня, або вона значно ослаблена, а сприйняття інформації, настроїв, почуттів, шаблонів поведінки базується на механізмах зараження й наслідування.

М. опитування /м. опроса/ — метод вивчення об'єктів психологічної війни, який передбачає прямі відповіді об'єктів психологічного вивчення на конкретні питання фахівців психологічної війни. Опитування може бути письмовим, коли питання задають письмово; усним, коли їх задають усно; у формі бесіди (інтерв'ю), коли встановлюється особистий контакт з об'єктом вивчення. В воєнних умовах найбільш розповсюдженим і найбільш значним видом опитування є допит військовополонених (перебіжчиків).

М. охорони джерел інформації /м. охраны источников информации/ — метод захисту інформації технічними засобами, заснований на запобіганні проникнення зловмисника до джерела інформації за допомогою інженерних конструкцій і засобів охорони технічних. Іноді цей метод називають методом захисту фізичним, хоча доцільно його визначити як метод інженерного захисту та технічної охорони об'єктів.

М. оцінки ефективності інформаційної боротьби /м. оценки эффективности информационной борьбы/ — сукупність способів, прийомів визначення кількісних значень показників інформованості протидіючих сторін та розрахунку ступеня переваги інформаційної однієї з них над іншою у відповідності до мети інформаційної боротьби. В основу методу може бути покладене математичне моделювання процесу забезпечення інформацією органів управління протидіючих сторін.

М. переконування /м. убеждения/ — метод психологічного впливу на свідомість людей, спрямований до їхнього власного критичного сприйняття. Переконування орієнтується на інтелектуально-пізнавальну сферу психіки людини. При використанні м. п. спочатку домагаються від людини внутрішньої злагоди з

певними умовиводами, а потім на цій основі формують і закріплюють нові установки (або трансформують старі), що відповідають поставленій меті. Переконування здійснюють за певними правилами: логіка переконування повинна бути доступною інтелекту об'єкта впливу; переконувати треба доказово, спираючись на факти, що відомі об'єкту; крім конкретних фактів і прикладів (без них не можна переконати тих, кому бракує широти кругозору, розвиненого абстрактного мислення), інформація повинна містити й узагальнені положення (ідеї, принципи); переконуюча інформація повинна виглядати максимально правдоподібною; факти, що повідомляються, і загальні положення повинні бути такими, щоб вони викликали емоційну реакцію об'єкта впливу. Критерієм результативності переконуючого впливу є переконаність. М. п. доцільно застосовувати в наступних випадках: тоді, коли об'єкт впливу в стані сприйняти одержану інформацію; якщо об'єкт психологічно здатний погодитися з думкою, що йому нав'язується; якщо об'єкт здатний зіставляти різні точки зору, аналізувати систему аргументації; якщо логіка мислення суб'єкта впливу, та аргументація, яка ним використовується, є близькими до особливостей мислення об'єкта; якщо є час переконувати.

М. приховування інформації /м. скрытия информации/ — метод захисту інформації технічними засобами, що передбачає такі зміни структури і енергії носіїв, при яких зловмисник не може безпосередньо або за допомогою технічних засобів виділити інформацію з якістю, достатньою для використання її у власних інтересах. Розрізняють метод приховування інформаційного і енергетичного.

М. психологічного впливу /м. психологического влияния/ — способи, прийоми або система прийомів для досягнення мети впливу психологічного. Базовими м. п. в. є метод переконування і метод навіювання. Проте вони не вичерпують весь арсенал способів і прийомів психологічного впливу. Існують ще й особливі прийоми такого впливу такі, як дезінформування (обман), маніпулювання, розповсюдження чуток і міфів.

М. спостереження /м. наблюдения/ — найбільш розповсюджений метод вивчення об'єктів психологічної війни за допомогою якого здійснюється цілеспрямоване, організоване, спеціально фіксоване сприйняття дій і поведінки об'єктів в різноманітних умовах без втручання в їхній перебіг. Об'єктом для спостереження може бути особовий склад противника на полі бою, військовополонені, населення зайнятих (звільнених)

районів. М. с. доповнюється оглядом місцевості, яка залишена противником. Спостереження буває систематичним (постійним) і несистематичним (епізодичним). Проте в усіх випадках воно планується й здійснюється за певною послідовністю: чітко визначається мета спостереження; указується його об'єкт і предмет (ситуації, які дозволяють одержати необхідні відомості); формулюються основні завдання, конкретизується вид або спосіб спостереження; підготовляється певне місце для спостереження і визначається час спостереження; розроблюється процедура фіксації результатів спостереження; здійснюється збирання інформації (власне спостереження); виконується оброблення й аналіз одержаної інформації.

М. узагальнення незалежних характеристик /м. обобщения независимых характеристик/ — метод вивчення об'єктів психологічної війни, який передбачає аналіз інформації про ці чи інші об'єкти, що одержується з незалежних джерел (від різних людей). Він доповнює всі інші методи вивчення об'єктів психологічної війни та дозволяє спочатку зіставляти різні відомості про одні і ці ж об'єкти, а потім за допомогою математичного й статистичного оброблення цих відомостей формулювати достовірні висновки про їхні психологічні особливості.

М. узагальнення соціологічної і психологічної статистики /м. обобщения социологической и психологической статистики/ — метод вивчення об'єктів психологічної війни, що дозволяє завчасно виділити й осмислити важливі особливості майбутніх об'єктів психологічного впливу, дає можливість зробити слушні прогнози, будувати моделі можливих операцій психологічних. Зокрема, шляхом узагальнення результатів попередніх бойових дій вдається будувати ймовірні прогнози схильності учасників збройного протиборства до психологічних впливів і поділити їх на наступні чотири категорії: тих, хто схвалює воєнні дії і бере в них активну участь (ідейні противники протиборчої сторони, патріоти й націоналісти, авантюристи, найманці і т. ін.); особи, що схвалюють збройне протиборство, проте уникають особистої участі в ньому (такі люди попадають на фронт не за своїми внутрішніми переконаннями, а внаслідок призову резервістів, загальної мобілізації, безвихідної ситуації і т. ін.); особи, що в принципі не бажають воювати за свою державу і відкрито (або приховано) підтримують ідеологію, політику протиборчої сторони (такі особи не згідні з

існуючим в країні політичним устроєм, але пориваються на фронт з метою переходу на сторону противника, або вирушають служити в результаті мобілізації); особи, які не бажають брати участі у війні ні на цій, ні на іншій стороні із-за свого світогляду (пацифісти, деякі віруючі, занепокоєні виключно особистою безпекою і т. ін.), але потрапили на фронт в результаті мобілізації.

МЕТОДИКА /методика/ [methods] (грец. *μεθοδικά*) — сукупність взаємозв'язаних способів та прийомів доцільного проведення будь-якої роботи.

М. вивчення об'єктів психологічної війни /м. изучения объектов психологической войны/ — сукупність взаємозв'язаних принципів, методів і організаційних заходів реалізації складного й довготривалого процесу збирання, оброблення і накопичення інформації про об'єкти психологічної війни.

М. оцінки ефективності інформаційної боротьби /м. оценки эффективности информационной борьбы/ — методика, яка включає ряд взаємозв'язаних етапів оцінки ефективності інформаційної боротьби: формування кадастру інформаційного органів керування протиборчих сторін; оцінку характеристик інформації про обстановку, що поступає в органи керування, її селекцію і класифікацію; порівняльну оцінку величини показника інформованості органів керування своїми силами і засобами і силами і засобами противника.

МЕТОДОЛОГІЯ /методология/ [methodology] (від метод і ...логія, що від грец. *λόγος* — слово, вчення) — 1) Наука про методи пізнання й перетворення світу. 2) Сукупність прийомів дослідження, що їх застосовують в будь-якій науці відповідно до специфіки об'єкту її пізнання.

М. оцінки безпеки інформаційних технологій загальна /м. оценки безопасности информационных технологий общая/ [Common Evaluation Methodology for Information Technology Security (CEMITS)] — додаток до стандарту інформаційної безпеки "критерії Загальні безпеки інформаційних технологій", в якому приведена методологія аналізу кваліфікаційного і сертифікації захищених систем оброблення інформації.

М. оцінки ефективності інформаційної боротьби /м. оценки эффективности информационной борьбы/ — одна з ключових проблем розвитку теорії інформаційної боротьби, вирішення якої надає теорії

необхідну фундаментальність і відносну завершеність. Стосовно до боротьби збройної в м. о. е. і. б. можна виділити два основних рівні. Перший (вищий) рівень включає м. о. е. і. б. у війнах і збройних конфліктах в цілому, другий — окремі м. о. е. і. б. в операціях (бойових діях). Крім того, методологія (на кожному з рівнів) має загальну і спеціальну частини. Загальний рівень призначений для оцінки ефективності власне інформаційної боротьби (як самостійного виду боротьби), спеціальний — для оцінки ефективності дій, в інтересах яких ведеться інформаційна боротьба. До загальної частини методології повинні входити метод і методика оцінки ефективності інформаційної боротьби, а також показники і критерії її ефективності. На основі використання загальної частини методології можна вирішити ряд взаємозв'язаних завдань оцінки ефективності інформаційної боротьби, зокрема, таких як: оцінка ступеня інформованості органу керування за заданою сукупністю відомостей про обстановку і даних поточної інформації про значення ознак, що розкривають ці відомості; обґрунтування вимог до джерел первинної інформації (ознакової) в інтересах подальшого підвищення якості інформованості органу керування про задану сукупність відомостей; обґрунтування вимог до ступеня блокування і модифікації поточної ознакової інформації при розробці заходів протидії інформаційної; відбір найбільш інформативних ознак для розкривання відомостей кадастру інформаційного; оптимізація часового циклу оновлення поточної інформації і т. ін.

МЕТРОЛОГІЯ /метрология/ [metrology] (від грец. *μέτρøν* — міра і ...логія, що від грец. *λόγøς* — слово, вчення) — наука про вимірювання з великою точністю. Завданнями м. є встановлення систем одиниць вимірювання, створення і зберігання основних еталонів цих одиниць і забезпечення перевірки точності практичних вимірювань.

М. інформаційна /м. информационная/ [information m.] — стандартизація, нормативне закріплення понять і термінів в галузі інформації.

МЕХАНІЗМ /механизм/ [mechanism] (від грец. *μηχανή* — знаряддя, пристрій) — сукупність проміжних станів або процесів будь-яких станів.

М. захисту /м. защиты/ [security m.] — 1) Конкретні процедури і алгоритми, що використовуються

для реалізації певних функцій і послуг безпеки. 2) Сукупність засобів захисту, що функціонують разом для виконання поставленого завдання з захисту даних.

М. захисту обчислювальних систем /м. защиты вычислительных систем/ — сукупність засобів та заходів, за допомогою яких реалізується безпека обчислювальних систем.

М. інформаційної безпеки /м. информационной безопасности/ [security m.] — сукупність заходів та процесів захисту інтересів життєво важливих особистості, суспільства, держави в сфері інформаційній, що здійснюються в межах законодавства. Вони повинні розроблюватися і впроваджуватися в кожній з предметних частин інформаційної сфери. У предметній частині створення інформації захисту в першу чергу належить: громадянин, суспільство, держава від впливу недостовірної, хибної інформації; інформація як інтелектуальна власність; документована інформація як інтелектуальна і речова власність; честь і достоїнство громадянина у зв'язку із створенням і розповсюдженням недостовірної інформації або несанкціонованим розповсюдженням інформації про нього. У предметній частині формування інформаційних ресурсів, підготовки і надання користувачам інформаційних продуктів, інформаційних послуг необхідно захищати від несанкціонованого доступу: інформаційні ресурси на всіх видах носіїв, в тому числі, що містять інформацію обмеженого доступу; інформаційні системи і мережі; інформаційні технології і засоби їхнього забезпечення. У предметній частині пошуку одержання і споживання інформації насамперед повинні бути захищені: право на одержання і використання інформації. В предметній частині створення і застосування інформаційних систем, технологій і засобів їхнього забезпечення повинні розроблюватися, виходячи з вимог, що виникають в інших предметних частинах, і насамперед в галузі інформаційної безпеки, всі засоби технічного, організаційного, правового і програмного захисту. При цьому повинні захищатися: машинні носії з інформацією; бази даних (знань) в складі автоматизованих інформаційних мереж і їхніх мереж; програмні засоби в складі ЕОМ, їхніх мереж.

МИСЛЕННЯ /мышление/ [thought, thinking] — вища ступінь пізнання, процесу відображення об'єктивної дійсності. Дозволяє одержати знання про такі об'єкти, властивості реального світу, які не можуть бути

безпосередньо сприйняті на чуттєвому рівні пізнання. Результат дії м. фіксується в мові. М. властиві такі процеси, як абстрагування, аналіз і синтез, постановка певних завдань та знаходження шляхів їхнього вирішення, висування гіпотез, ідей і т. ін. Результатом процесу м. завжди є та чи інша думка. Здатність м. до узагальненого відображення дійсності виражається в здатності людини створювати загальні поняття. Утворення наукових понять зв'язане з формулюванням відповідних законів. Здатність м. до опосередкованого відображення дійсності виражається в здатності людини до акту умовиводу, логічного висновку, доказу. Ця здатність розширює межі пізнання. Вона дозволяє, відштовхуючись від аналізу фактів, доступних безпосередньому сприйняттю, пізнавати те, що недоступно сприйняттю з допомогою органів чуттів. Поняття і системи понять (наукові теорії) фіксують (узагальнюють) досвід людства, та являють концентрацію знань людей і є відправним пунктом для подальшого пізнання дійсності. М. людини вивчається різноманітними науками (фізіологією вищої нервової діяльності, кібернетикою, психологією, гносеологією і т. ін.) й різноманітними методами. Серед експериментальних досліджень велику роль відіграють методи дослідження процесів м. в формі його моделювання за допомогою різних електронно-обчислювальних пристроїв. В житті кожного індивідуума мислення не існує як чисто інтелектуальний процес, а нерозривно зв'язане з іншими психічними процесами, тобто не існує ізольовано від свідомості людини в цілому.

М. системне /м. системное/ [system t.] — уміння фахівця виявляти і об'єктивно аналізувати все різноманіття факторів і зв'язків достатньо складного об'єкта дослідження, яким є, наприклад, об'єкт розвідки. М. с. формується в результаті відповідного навчання і практики вирішення проблем, що слабо формалізуються.

МИША /мышь/ [mouse] — 1) Портативний пристрій локалізації, який функціонує в результаті переміщення його по поверхні; маніпулятор вводу графічної інформації. 2) Пристрій для обробки положення покажчика на екрані дисплея.

М. оптична /м. оптическая/ [optical m.] — миша, в якій її переміщення по спеціальний світлочутливій площадці фіксується світлочутливими (інфрачервоними) датчиками.

МІКРАТ /микрат/ — мікрознімок, створений в позитиві, зображення на якому перед відправкою знебарвлюється і робиться прозорим.

МІКРО... /микро.../ [micro...] — (від грец. *μικρός* — малий) — у складних словах означає: дуже малий, найдрібніший; пов'язаний з вивченням або вимірюванням дуже малих предметів, явищ, величин.

МІКРОВІДЕОКАМЕРА /микровидеокамера/ (від мікро... і відеокамера) — мініатюрна відеокамера, призначена для використання в системах відеоконтролю і відеоспостереження. Див. також камера телевізійна мініатюрна.

МІКРОДИСК [microfloppy disk] (від мікро... і диск) — гнучкий диск магнітний діаметром 89 мм (3,5 дюйма).

МІКРОЕЛЕКТРОНІКА /микроэлектроника/ [microelectronics](від мікро... і електроніка) — напрям електроніки, що виник на основі досягнень фізики тонких плівок, твердого тіла та спеціальних матеріалів і включає дослідження, розроблення та виробництво інтегральних схем і принципи їхнього застосування. Головною ознакою, основною тенденцією розвитку м. є комплексна інтеграція, що включає: інтеграцію елементів на кристалі й основі; інтеграцію схемних функцій в межах структурної одиниці; інтеграцію фізичних ефектів при створенні функціональних мікросхем; інтеграцію технологічних процесів; інтеграцію методів проектування та етапів створення радіоелектронних засобів. Завдяки комплексній інтеграції з'явилися сучасні інтегральні схеми, схеми інтегральні великі, схеми інтегральні надвеликі; за допомогою останніх стало можливим розробляти складні системи, проектування яких раніше було неможливим через низьку надійність, високі вартість та енергоємність. Інтегрована м. є фундаментальною базою розвитку всіх сучасних засобів радіоелектронних.

МІКРОЕОМ /микроЭВМ/ [microcomputer] (від мікро... і ЕОМ) — ЕОМ малих розмірів, яка створена на базі мікропроцесорів (мікропроцесорна ЕОМ). Розрізняють мікроЕОМ вбудовані і персональні, настільні і портативні, професійні і побутові.

М. вбудована /м. встроенная/ [built-in m.] — мікроЕОМ, яка конструктивно пристосована для роботи

у складі приладів або обладнання.

МІКРОЗНІМОК /микроснимок/ [micrograph] (від мікро... і знімок) — знімок, створений методами мікрофотографування.

МІКРОПРОЦЕСОР /микропроцессор/ [microprocessor] (від мікро... і процесор) — схема інтегральна велика, яка виконує функції процесора центрального.

М. вбудований /м. встроенный/ [built-in m.] — вбудований в пристрій мікропроцесор, який використовується в системі управління цим пристроєм.

М. комунікаційний /м. коммуникационный/ [communication m.] — спеціалізована мікроЕОМ, що виконує функції керування мережними протоколами в мережній телеобробці. Забезпечує підвищення продуктивності мережі.

МІКРОСХЕМА /микросхема/ [microcircuit] (від мікро... і схема) — 1) Елемент, вузол чи пристрій (або його частина) радіоелектронної апаратури, виготовлений засобами мікроелектроніки. 2) Електронна схема, яка реалізована у вигляді напівпровідникового кристалу; інтегральна схема, яка виконує деяку складну функцію.

М. інтегральна /м. интегральная/ [integrated circuit] — див. схема інтегральна. Розрізняють м. і. малої інтеграції, середньої інтеграції, великої інтеграції (див. схема інтегральна велика) і надвеликої інтеграції (див. схема інтегральна надвелика).

М. інтегральна аналогова /м. интегральная аналоговая/ [analog integrated circuit] — мікросхема інтегральна, призначена для перетворення й оброблення сигналів за законом безперервної функції.

М. інтегральна гібридна /м. интегральная гибридная/ [hybrid integrated circuit] — мікросхема інтегральна, в якій крім електронних елементів містяться інші компоненти схеми.

М. інтегральна цифрова /м. интегральная цифровая/ [digital integrated circuit] — мікросхема інтегральна, призначена для перетворення й обробки сигналів, що змінюються за законом дискретної функції.

МІКРОТЕЛЕФОН /микротелефон/ [handset, microtelephone] (від мікро(фон) і телефон) — телефонна

трубка з вмонтованими в ній мікрофоном і телефоном.

МІКРОТОЧКА /микроточка/ — украй малий мікрознімок, створений на основі технологій мікрофотографування.

МІКРОФІЛЬМУВАННЯ /микрофильмирование/ [microfilming] — одержання на фото- або кіноплівці фотокопій з друкованих матеріалів, креслеників, рукописів і т.ін. при значному зменшенні їхніх розмірів. М. дозволяє суттєво скоротити обсяг, що займають різноманітні документи, і швидко одержати їхні копії.

МІКРОФІША /микрофиша/ [microfiche] (від мікро... і франц. ficher — убивати, втискувати) — мікрофотокопія з плоского оригіналу (друкованого тексту, кресленика, рисунка і т. ін.), виконана на фотопапері або фотоплівці. М. виготовляються на фотоплівках з дуже високою роздільною здатністю. На одній м. розміром 6x12 см вміщується від 30 до 130 сторінок книжного тексту. Для читання м. застосовують спеціальні проекційні апарати, що створюють на вбудованому екрані збільшене зображення оригіналу.

МІКРОФОТОГРАФУВАННЯ /микрофотографирование/ [microphotography] (від мікро... і фотографування) — фотографування, призначене для створення зменшеного у розмірах фотографічного зображення тексту або іншого матеріалу. Застосовується для економії місця, яке займають дані розвідувальні, і відносно безпечного транспортування даних на великі відстані. Відомі два основні види м. — мікроточка і мікрат.

МІКРОФОН /микрофон/ [microphone, mike, telephone transmitter] (мікро... і ...фон від грец. *μικρός* — малий і *φωνή* — звук, голос) — перетворювач звукових коливань в електричні коливання такої самої частоти. М. характеризується чутливістю і діапазоном частот акустичних сигналів, що ним приймаються. Діаграма спрямованості мікрофону залежить від його конструкції. Існує велика кількість різновидів м., в яких для акустоелектричних перетворень використовуються різноманітні фізичні процеси. М. поділяються за принципом дії (вугільні, електродинамічні, електромагнітні, конденсаторні, п'єзоелектричні), за спрямованістю (неспрямовані, односторонньої спрямованості, гострої спрямованості), за смугою частот (вузькосмугові, широкосмугові), за способом застосування (повітряні, гідроакустичні, контактні), за конструкцією (широ-

кого застосування, спеціальні, камуфльовані). Можливості м. визначаються наступними характеристиками: осьовою чутливістю на частоті 1000 Гц; діаграмою спрямованості; діапазоном відтворюваних частот коливань акустичної хвилі; нерівномірністю частотної характеристики; масо-габаритними характеристиками.

М. вугільний /м. угольный/ [carbon m.] — мікрофон у вигляді круглої коробочки з гранульованим деревним вугіллям, закритої металевою пружною кришкою — мембраною. До електрода, закріпленого на дні коробочки, і мембрани подається електрична напруга, під дією якої в масі вугільного порошку протікає електричний струм. Акустична хвиля приводить мембрану мікрофона в коливальний рух, внаслідок чого змінюється ступінь стиснення вугільного порошку і площа стикання його гранул одна з одною. В результаті цього опір порошку і сила струму, що протікає через нього, змінюється у відповідності до гучності звуку, тобто здійснюється запис інформації шляхом амплітудної модуляції електричного струму. М. в. мають низьку вартість, створюють без додаткового підсилювача рівні сигналів, достатні для їхнього передавання на великі (десятки км) відстані. Проте вони вузькосмугові і потребують потужного джерела струму. Використовуються в телефонному проводовому зв'язку.

М. електретний /м. электретный/ [electret m.] (англ. electret) — мікрофон конденсаторний, мембрана якого виготовлена з полімерних матеріалів (смол), що називаються електретами, здатних в сильному електричному полі і при високій температурі заряджатися та тривалий час зберігати електричний заряд. Мембрана з електрета металізується, між пластинами після заряду виникає певна різниця потенціалів (45–130 В). Для м. е. не потрібно зовнішнього джерела живлення. Вони широко застосовуються в апаратурі звукозапису, в тому числі для підслухування.

М. електродинамічний /м. электродинамический/ [(electro)dynamic m.] — мікрофон, створений на основі перетворювача акустоелектричного електродинамічного.

М. електромагнітний /м. электромагнитный/ [electromagnetic m.] — мікрофон, створений на основі перетворювача акустоелектричного електромагнітного, в якому в результаті коливань мембрани з феромагнітного матеріалу над нерухомою котушкою з осердям в її обмотці виникає електрорушійна сила

еквівалентна інтенсивності звуку.

М. з параболічним відбивачем /м. с параболическим отражателем/ [parabolic-reflector m.] — мікрофон спрямований, в якому сам мікрофон розташований в фокусі параболічного відбивача звуку.

М. конденсаторний /м. конденсаторный/ [condenser/capacitor m.] — мікрофон, створений на основі перетворювача акустоелектричного ємнісного. М. к. являє собою капсуль, що складається з двох паралельно розташованих пластин — електродів, один з яких масивний, інший — тонка мембрана. Електроди створюють конденсатор, ємність якого залежить від площі пластин і відстані між ними. До електродів підводиться через резистор постійна напруга, що його поляризує. При дії на мембрану звукових хвиль змінюється відстань між електродами і, відповідно, ємність конденсатора. В результаті цього через резистор тече струм, амплітуда якого пропорційна звуковому тиску на мембрану. Різновидом м. к. є мікрофон електретний.

М. контактні /м. контактные/ — мікрофони, призначені для прийому структурного звуку. До них відносяться мікрофони-стетоскопи, а також ларингофони та остеофони, які сприймають і перетворюють в електричні сигнали механічні коливання (вібрації) зв'язок і хрящів гортані або кісток черепа особи, що говорить.

М. лазерний /м. лазерный/ [laser m.] — пристрій, побудований на основі лазера. Промінь лазера, відбитий від скла приміщення, в якому ведуться розмови, модулюється сигналом звукової частоти. Прийнятий фотоприймачем відбитий промінь детектується, звук підсилюється і записується. Див. також засоби лазерного підслухування.

М. п'єзоелектричний /м. пьезоэлектрический/ [piezoelectric m.] — мікрофон, створений на основі перетворювача акустоелектричного п'єзоелектричного. Дія м. п. заснована на виникненні електрорушійної сили на поверхні пластинок з п'єзоматеріалу, механічно зв'язаних з мембраною. Коливання мембрани під тиском хвилі акустичної передаються п'єзоелектричній пластині, на поверхні якої виникають заряди, величина яких відповідає рівню гучності акустичного сигналу.

М. спрямований /м. направленный/ [directional m.] — мікрофон, рівень сигналу якого змінюється

в залежності від обертання мікрофону по відношенню до джерела акустичної хвилі в горизонтальній і вертикальній площинах. М. с. бувають односторонньої і двосторонньої спрямованості. Ширина діаграми спрямованості мікрофону оцінюється в градусах на рівні 0,5 (0,707) від максимальної потужності (амплітуди) електричного сигналу на його виході. Для добування інформації (підслухування) особливий інтерес являють м. с. з гострою спрямованістю, які забезпечують збільшення дальності підслухування. Вузька діаграма спрямованості мікрофонів досягається за рахунок відповідної конструкції мікрофону, яку можна представити у вигляді акустичної антени з відповідною діаграмою спрямованості. Виділяють три основних типи м. с. з гострою спрямованістю: з акустичною антеною параболічною, з акустичною антеною трубчастою, з акустичною антенною решіткою. Максимальна дальність підслухування розмови за допомогою гостроспрямованих мікрофонів може сягати 50–100 м.

М. спрямований з акустичною антенною решіткою /м. направленный с акустической антенной решеткой/ — сукупність мікрофонів, розташованих у певному порядку на плоскій поверхні (наприклад, на стінці аташе-кейса), що дозволяє зменшити ширину еквівалентної діаграми спрямованості до 40–60 град та забезпечити зняття мовної інформації на віддалі до 50 метрів від джерела.

М. спрямований з акустичною антеною параболічною /м. направленный с акустической антенной параболической/ — мікрофон спрямований, в якому сам мікрофон розташований в фокусі параболічного відбивача звуку.

М. спрямований з акустичною антеною трубчастою /м. направленный с акустической антенной трубчатой/ – мікрофон спрямований з гострою спрямованістю, що складається з однієї трубки довжиною 0,3–1 м або набору трубок, довжини яких узгоджені з довжинами хвиль акустичного сигналу. В торці трубок прилаштовується мембрана мікрофона.

М.-стетоскоп /м.-стетоскоп/ [m.-stethoscope] — пристрій, що реєструє вібраційні коливання стін, стелі, скла, вентиляційних шахт і т.ін. (див. стетоскоп).

МІКРОФОТОКОПІЮВАННЯ /микрофотокопирование/ — те ж, що мікрофільмування.

МІРА /мера/ [measure] — те, що є основою для оцінки, вимірювання або порівняння чого-небудь.

М. інформаційної агресивності /м. информационной агрессивности/ — обсяг інформації, що цілеспрямовано передається від однієї системи інформаційної до іншої.

М. хаосу в прийнятті рішень /м. хаоса в принятии решений/ — надлишок зв'язків, потенційно здатних ускладнити процес прийняття рішення, в першу чергу за рахунок збільшення часу оброблення вхідних даних.

МІСТ /мост/ [bridge] — пристрій рівня канального моделі ISO/OSI, який дозволяє з'єднувати між собою пристрої в різних мережах обчислювальних локальних. М. не залежать від типу протоколу, але визначаються використовуваним обладнанням. Вони можуть з'єднувати мережі з різними протоколами і різними типами обладнання. Прикладом м. є пристрій, що з'єднує мережі Ethernet і TokenRing. Присутність м. для користувачів невидима (на відміну від шлюзів). М. бувають двох типів: мости локальні і мости віддалені. М. працює аналогічно як маршрутизатор, різниця тільки в тому, що м. встановлює з'єднання на канальному рівні, а маршрутизатор — на мережному.

М. віддалений /м. удаленный/ [remote b.] — міст, що з'єднує два локальні сегменти мереж обчислювальних локальних.

М. локальний /м. локальный/ [local b.] — міст, що з'єднує два сегменти мереж обчислювальних локальних через глобальну мережу.

МІСЦЕ /место/ [place] — простір, який може бути зайнятий ким-, чим-небудь, на якому будь-що відбувається, знаходиться або де можна розташуватися.

М. робоче автоматизоване (АРМ) /место рабочее автоматизированное (АРМ)/ [automatized working p., workstation] — індивідуальний комплекс технічних і програмних засобів, призначених для автоматизації професіональної праці фахівця — керівника, проектувальника, дослідника, випробувача, технолога і т.ін. АРМ забезпечує підготовку, редагування, друк графічної, цифрової і текстової інформації та виконання різноманітних інформаційно-розрахункових функцій для підвищення продуктивності роботи фахівця. До

його складу, як правило, входять: ЕОМ, дисплей графічний і (або) алфавітно-цифровий, графопобудовник та інші пристрої.

МІТКА /метка/ [label] — 1) Знак, зроблений на кому-, чому-небудь. 2) Атрибут доступу, що відображає категорію доступу об'єкта комп'ютерної системи.

М. грифа /м. грифа/ [security l.] — покажчик грифа секретності, безпосередньо пов'язаний з тією інформацією, до якої він відноситься.

М. цілісності об'єкта /м. целостности объекта/ — сукупність атрибутів об'єкта доступу, що забезпечує його цілісність.

МІФ /миф/ (від грец. *μῦθος* — слово, сказання) — 1) Стародавня народна оповідь про явища природи, історичні події тощо або фантастичні оповідання про богів, обожнених героїв, уявних істот; легенда. 2) Інформація, яка пояснює походження і подальше перетворення цих чи інших явищ виключно на основі вигаданих подій. Осмислення людиною навколишньої дійсності через м. ґрунтується не на наукових основах, а на вірі й переконаннях представників конкретної культури, етносу, соціальної групи. Виховання на прикладах дій міфічних персонажів формує у свідомості людей систему морально-етичних цінностей, притаманних даному угрупованню (етносу, клану, професійній групі і т. ін.), почуття співпричетності до її історії. Основний принцип побудови сюжету традиційного м. — сполучення знайомих реалій життя з фантастичними вчинками героїв. З давніх часів правителі усіх рангів широко використовували міфотворчість для своїх цілей. Це сприяло появі спеціального способу впливу на суспільну свідомість, прийнятому на озброєння фахівцями війни психологічної (див. міфи соціальні).

М. приховані /м. скрытые/ — міфи, що описують специфічну частину суб'єктивних уявлень суспільства про навколишній світ та інші угруповання. М. п. існують в формі ідеологічних, релігійних, політичних, побутових установок, забобонів, переконань представників конкретних соціальних угруповань.

М. соціальні /м. социальные/ — міфи, що подають спотворені уявлення про дійсність, які свідомо впроваджуються у свідомість людей з метою формування необхідних соціальних реакцій. Особливістю м.

с. є те, що велика частина суспільства сприймає їх не як вимисел, а як природний стан речей. Під впливом с. м. історія виникнення держав і етносів, як правило, спотворюється настільки, що її об'єктивний аналіз можна здійснювати тільки шляхом критичного зіставлення різноманітних джерел. Проте на практиці у багатьох випадках такий аналіз є надто важким із-за упередженості авторів або замовленого (тобто наперед фальшивого) характеру більшості джерел інформації. По суті справи, вся письмова світова історія із самого початку є об'єктом постійного маніпулювання. Фахівці війни психологічної вважають, що можливості для виникнення й розповсюдження масових с. м., а також для зловживання ними за допомогою засобів масової інформації у сучасному суспільстві не зменшилися, а в дечому багатократно збільшилися. Вони вважають, що с. м. здатні: здійснювати вплив одночасно на інтелектуальну й емоційну сфери людської свідомості, що дозволяє їм вірити в реальність змісту міфу; представляти гіперболічний опис часткового випадку ідеальною моделлю бажаної поведінки, із-за чого зміст міфу впливає на поведінку людей; спиратися на конкретну традицію, що існує у суспільстві. Неможливо впровадити в масову свідомість такі цінності, які протистоять традиційним. Нові міфи завжди виростають зі старих коренів. Зміст інформаційно-пропагандистських матеріалів, створених у відповідності до існуючої у конкретному соціальному угрупованні міфологічної системи, діє на людей не ззовні, а якби із середини їхнього світогляду, що полегшує процес сприйняття цього змісту. При цьому слід враховувати те, що міфи, не зважаючи на широкі можливості для імпровізації, діють все ж в обмежених рамках, так як мають певні характеристики. Міфи бувають явні, приховані і станові.

М. станові /м. сословные/ — міфи, які обслуговують уявлення про близькість або, навпаки, віддаленість певних груп людей один від одного за соціальною, професійною, національною, релігійною ознакою. Вони діють за простою схемою "свій-чужий" і мають достатню ефективність в умовах бойової діяльності.

М. явні /м. явные/ — міфи, до змісту яких входять фольклорні історії і персонажі, популярні сюжети й герої літературних творів. Успіх застосування такого міфу визначається правильною інтерпретацією подій, що описані в ньому. Для цього необхідно дуже добре знати історію й культуру конкретної країни або етносу, чітко розуміти, в яких умовах його можна застосувати, а в яких він принесе лише шкоду.

МІШЕНЬ /мишень/ [target] — об'єкт для стрільби, влучання.

М. інформаційна /м. информационная/ [information t.] — множина елементів інформаційної системи, що належать або здатні належати сфері управління, і мають високі потенційні властивості для перепрограмування на досягнення цілей, неприйнятних для даної системи.

МККТТ /МККТТ/ [CCITT (Comite Consultatif International Telegraphique et Telephonique)] — Міжнародний консультативний комітет з телеграфії та телефонії — організація, резиденція якої знаходиться в Женеві (Швейцарія). Була заснована як частина Міжнародної спілки електрозв'язку (МСЕ) [International Telecommunication Union (ITU)] при ООН. МККТТ рекомендував застосовувати стандарти зв'язку, поширені в усьому світі. З 1993 року рекомендації МККТТ називаються рекомендаціями МСЕ [ITU-T Recommendations]. Рекомендації публікуються регулярно через чотири роки. Кожне видання відрізняється кольором обкладинок. Так, пізніше видання було назване Голубою книгою; видання 1992 року має білі обкладинки.

МОВА /язык/ [language] — 1) Сукупність, погоджень і правил, які використовуються для спілкування, відображення і передавання інформації. 2) В техніці обчислювальній — засіб опису даних і алгоритмів вирішення задач.

М. SGML /я. SGML/ [Standard Generalized Markup L.] — стандарт опису офісних документів, який затверджений ISO.

М. асемблера /я. ассемблера/ [assembly l.] — мова програмування, структура команд якої визначається форматами команд і даними машинної мови, а також архітектурою ЕОМ. М. а. — універсальна мова програмування.

М. високого рівня /я. высокого уровня/ [high-level l.] — мова програмування, яка характеризується високим рівнем узагальнення понять, які відповідають деякій галузі застосування і дозволяють лаконічно і змістовно визначати завдання для ЕОМ в термінах, які близькі до термінів, що використовуються в

професійній діяльності людей.

М. моделювання /я. моделирования/ [simulation l.] — мова програмування, призначена для розроблення програм моделювання.

m6405**М. природна** /я. естественный/ [human l., natural l.] — мова, правила якої засновуються на поточному застосуванні без точного попереднього опису.

М. природно-ділова /я. естественно-деловой/ — підмножина мови природної, яка є внутрішньо формалізованою і розширеною спеціальними термінами і той же час залишається для людини природним засобом спілкування.

М. програмування /я. программирования/ [programming l.] — формалізована мова, призначена для опису алгоритмів вирішення задач на ЕОМ.

М. розмічування гіпертексту HTML /я. разметки гипертекста HTML/ [HyperText Markup L. (HTML)] — мова опису (формат) гіпертекстових документів що містять: посилання на інші документи (файли), текст оформлений різними шрифтами, статичні і динамічні графічні зображення, звук і деяке функціональне наповнення. HTML є спрощеною версією більш узагальненої мови SGML (Standard Generalized Markup Language), яка формально визначає структуру документів. Мова HTML проста, але достатньо потужна для подання більшості документів загального призначення. В полях, що описують тип вмісту, формат HTML позначається типом *text/html*. Базову основу Web складають HTML-документи з гіперпосиланнями (у вигляді адреси мережного ресурсу — покажчика URL), що передаються за протоколом HTTP.

М. штучна /я. искусственный/ [artificial l.] — мова, правила якої точно встановлені перед її використанням.

МОВЛЕННЯ /вещание/ — 1) Спілкування людей за допомогою мови; мовна діяльність. 2) Передавання повідомлень по радіо, телебаченню.

М. телевізійне /в. телевизионное/ — одна з найбільш ефективних форм впливу психологічного. Йо-

го роль безперервно зростає з розширенням мережі супутникового телебачення, цифрового телебачення, приєднання телебачення до Інтернету. Психологічний вплив за допомогою м. т. має цілий ряд переваг у порівнянні з іншими формами ведення психологічної війни: м. т. має найсильніший вплив на формування суспільної думки — ефект присутності, синхронності, причетності глядача до подій, що відбуваються на екрані телевізора, заставляє його вірити у правдивість поданого йому матеріалу; за допомогою м. т. можна показати конкретні епізоди бойових дій, фотодокументи, що пропагують міць і силу своєї зброї або демонструють звірячість противника; телебачення дозволяє передавати факсимільним способом різноманітні друковані видання, в тому числі листівки, в інші країни світу; при неможливості прямої передачі на телевізійні приймачі (або ретрансляції передач) населення й військовополонені можуть дивитися їхні записи за допомогою відеомагнітофонів.

М. усне (звукове) /в. устное (звуковое)/ — вплив інформаційно-психологічний, який здійснюється шляхом передавання через звукомовні станції різноманітних повідомлень і програм (див. також програма усного мовлення), які безпосередньо сприймають військовослужбовці противника, його цивільне населення, полонені. Переваги м. у.: високий ступінь оперативності; високий ступінь конкретності; сприйняття передач м. у. не потребує використання спеціальних технічних засобів; при м. у. можливий "зворотній зв'язок" з об'єктом впливу (сприйняття його реакції на передачу); м. у. передбачає використання музики, шумів та інших звукових ефектів, що підвищує емоційний вплив на слухачів. Недоліки, що знижують ефективність м. у.: вплив бойових і природних шумів, погодних і кліматичних умов, а також завад, які може створювати спеціально противник; радіус дії м. у. обмежений відносно невеликим простором; велика можливість виявлення й придушення противником звукомовного засобу.

МОДЕЛЬ /модель/ [model] (франц. modéle, від лат. modulus — міра) — матеріальний об'єкт, система математичних залежностей або програма, що імітують структуру або функціонування досліджуваного

об'єкта. Основна вимога до моделі — її адекватність об'єкту.

М. ISO/OSI /м. ISO/OSI/ — див. модель взаємодії відкритих систем.

М. безпеки /м. безопасности/ [security m.] — формальне подання політики безпеки, що розроблена для системи. М. б. містить формальний опис факторів та правил, що визначають управління, розподіл і захист інформації критичної.

М. Белла-Лападула /м. Белла-Лападула/ [Bell-LaPadula m.] — формальна автоматна модель політики безпеки, що описує множину правил керування доступом. В цій моделі компоненти системи розподіляються на об'єкти і суб'єкти доступу. Вводиться поняття безпечного стану і доводиться, що коли кожний перехід зберігає безпечний стан (тобто переводить систему з безпечного стану в безпечний), то згідно з принципом індукції система є безпечною.

М. вербальна /м. вербальная/ [verbal m.] (лат. verbalis, від verbum — слово) — словесний опис моделі на мові природній або професійно-орієнтованій.

М. взаємодії відкритих систем (МВВС) /м. взаимодействия открытых систем (МВОС)/ [Open Systems Interconnection (OSI) m.] — запропонована Міжнародною організацією по стандартизації (ISO) модель мережі із семи рівнів, для кожного з яких створені свої стандарти і загальні моделі.

М. інформаційна /м. информационная/ [information m.] — 1) Формалізований опис інформаційних структур і операцій над ними. 2) Параметричне подання процесу циркуляції інформації, яке підлягає автоматизованій обробці в системі керування.

М. загроз для інформації /м. загроз для информации/ [m. of threats to information] — формалізований опис методів та засобів здійснення загроз для інформації.

М. захисту /м. защиты/ [protection m.] — абстрактний (формалізований або неформалізований) опис комплексу програмно-технічних засобів і (або) організаційних заходів захисту від несанкціонованого доступу.

М. зловмисника /м. злоумышленника/ — модель (опис) можливостей, поведінки та способів фізично-

го проникнення потенційного зловмисника до джерел інформації, що захищається. В умовах відсутності інформації про зловмисника, його кваліфікації, технічної оснащеності для запобігання грубих помилок найкраще переоцінити загрозу, ніж недооцінити, хоча такий підхід може призвести до збільшення витрат на захист.

М. каналу витоку інформації інформаційна /м. информационная канала утечки информации/ — модель, що містить характеристики інформації, витік яких можливий каналом витоку інформації: кількість і цінність інформації, пропускна здатність каналу, прогнозована якість інформації, що приймається зловмисником.

М. каналу витоку інформації комплексна /м. комплексная канала утечки информации/ — модель, що об'єднує і ув'язує між собою статичні і динамічні моделі каналу витоку інформації. В ній вказуються інтегральні параметри каналу витоку інформації: джерело інформації і його вигляд, середовище розповсюдження і його протяжність, місце розташування приймача сигналу, інформативність каналу і показники загрози безпеці інформації.

М. каналу витоку інформації просторова /пространственная м. канала утечки информации/ — модель, що містить опис положення каналу витоку інформації у просторі: місця розташування джерела і приймача сигналів, їхня відстань від меж території організації, орієнтація вектора розповсюдження носія інформації в каналі витоку інформації і його протяжність. Таку модель доцільно подавати у вигляді графа на плані приміщення, будівлі, території організації, прилеглих зовнішніх ділянок середовища.

М. каналу витоку інформації структурна /м. канала утечки информации структурная/ — модель, що описує структуру (склад і зв'язки) каналу витоку інформації. Таку модель доцільно подавати в табличній формі.

М. каналу витоку інформації функціональна /м. канала утечки информации функциональная/ — модель, що характеризує режими функціонування каналу витоку інформації, інтервали часу, протягом

якого можливий витік інформації.

М. математична /м. математическая/ [mathematical m.] — система математичних залежностей, яка описує структуру або функціонування об'єкта.

М. механізму захисту /м. механизма защиты/ [security m.] — формальне визначення внутрішніх характеристик захисту, що забезпечуються певним механізмом захисту. Як правило, містить докладну специфікацію дозволених і заборонених відносин між суб'єктами і об'єктами доступу згідно з відповідними категоріями доступу та грифом секретності, а також визначає події, які повинні фіксуватися у журналі контрольному.

М. навіюючого впливу /м. внушающего воздействия/ — опис процесу навіювання у вигляді замкнутої системи "суб'єкт-об'єкт", яка включає три взаємозв'язаних структурних компонентів: операціональний (вплив об'єкта); процесуальний (прийняття навіюючого змісту об'єктом); результативний (реакції об'єкта у відповідь). Ефективна реалізація усіх компонентів м. н. в. залежить від правильного застосування його конкретних способів і прийомів.

М. об'єкта захисту /м. объекта защиты/ — опис об'єкта захисту, що включає: визначення джерел інформації, що належить захисту; опис просторового розташування основних місць розміщення джерел інформації, що підлягають захисту; визначення шляхів розповсюдження носіїв з інформацією, що підлягає захисту, за межі контрольованих зон (приміщень, будівель, території, організації); опис існуючих перепон (перешкод) на шляхах розповсюдження носіїв з інформацією за межі контрольованих зон.

М. політики безпеки /м. политики безопасности/ [security policy m.] — формальне подання політики безпеки, що розроблена для системи. М. п. б. містить формальний опис факторів та правил, що визначають керування, розподіл і захист критичної інформації.

М. порушника /м. нарушителя/ [violator's m.] — абстрактний (формалізований або неформалізований) опис порушника правил розмежування доступу.

М. порушника правил розмежування доступу /м. нарушителя правил разграничения доступа/

[security policy violater's m.] — абстрактний (формалізований або неформалізований) опис порушника правил розмежування доступу.

М. технічної розвідки /м. технической разведки/ [technical intelligence m.] — формалізований опис методів, засобів та можливостей розвідки технічної.

М. чорного ящика /м. черного ящика/ [black-box-m.] — модель, що описує лише входи та виходи системи, але не внутрішнє влаштування системи. Наприклад, модель математична "чорного ящика" — це просто сукупність множин X і Y (X відповідає входам, Y виходам); якщо оператор F, що їх зв'язує (Y=F (X)) припускається існуючим, то він вважається невідомим.

М. фізична /м. физическая/ [physical m.] — матеріальний аналог реального об'єкта.

МОДЕЛЮВАННЯ /моделирование/ [model(l)ing] (від франц. modeler — ліпити, формувати) — метод дослідження явищ і процесів, що ґрунтується на заміні конкретного об'єкта досліджень (оригіналу) іншим, подібним до нього (моделлю). Розрізняють моделі вербальні, фізичні і математичні і відповідне м. В галузі інформаційної безпеки м. здійснюється як з метою розробки методів вдосконалення системи захисту, так і з метою розробки методів подолання системи захисту та маніпуляції даними і управляючими командами.

М. загроз безпеці інформації /м. угроз безопасности информации/ — опис і аналіз способів викрадення, модифікації і знищення інформації з метою оцінки шкоди (збитків), які можуть бути нанесені цими способами. Моделювання загроз включає: моделювання способів фізичного проникнення зловмисника до джерел інформації (див. модель зловмисника); моделювання каналів витоку інформації.

М. інформаційне /м. информационное/ [information m.] — моделювання, зв'язане із створенням і перетворенням різноманітних форм інформації, наприклад, графічної або текстової, у вигляд, який задається користувачем. В сучасних системах інформаційних воно здійснюється шляхом створення підсистеми документального забезпечення.

М. каналів витоку інформації /м. каналов утечки информации/ — метод повного дослідження можливостей каналів витоку інформації з метою наступного розроблення способів і засобів захисту інформації.

В основному застосовуються моделі вербальні і математичні. Доцільно мати моделі, що описують канали в статиці і динаміці. Статичний стан каналу описують моделі структурна і просторова, що взаємно доповнюють одна одну. Динаміку каналу витоку інформації описують моделі функціональна і інформаційна. Всі моделі об'єднуються і ув'язуються між собою в одній моделі каналу витоку інформації комплексній.

М. об'єкта захисту /м. объектов защиты/ — опис і аналіз джерел конфіденційної інформації та існуючої системи її захисту. М. о. з. включає структурування інформації, що потребує захисту та розроблення і аналіз моделей об'єктів захисту. В результаті моделювання визначається стан безпеки інформації та слабкі місця, наявні в існуючій системі її захисту.

МОДЕМ /модем/ [modem] — 1) Функціональний пристрій (модулятор-демодулятор), який забезпечує модуляцію і демодуляцію сигналів. 2) Пристрій, який перетворює цифрові сигнали в аналогову форму й навпаки для передавання їх лініями зв'язку аналогового типу (найчастіше телефонними лініями). Для забезпечення сумісності протоколи роботи м., види перетворень сигналів, швидкості передавання даних стандартизуються рекомендаціями МСЕ (див. також МККТТ) серії V. Ускладнені м., окрім операцій передавання та прийому, здатні автоматично телефонувати, повторювати виклик або відповідати на нього. Для функціонування м. необхідне програмне забезпечення зв'язку.

МОДИФІКАЦІЯ /модификація/ [modification] (лат. modificatio від modifoco — установлюю міру) — 1) Видозміна, перетворення, поява нових ознак, властивостей; якісно відмінні стани чого-небудь. 2) Зміна користувачем або процесом інформації, що міститься в об'єкті.

МОДУЛЯЦІЯ /модуляция/ [modulation] (лат. modulatio — розмірність, гармонійність, ритм, від modulor — розмінюю) — термін, що відображає в широкому розумінні змінювання за заданим законом величин, що характеризують фізичний процес. У радіотехніці м. називають змінювання параметрів високочастотних коливань радіопередавача згідно з інформацією, що передається. В залежності від змінюваного параметра (наприклад, амплітуди, частоти, фази або параметрів імпульсної послідовності) розрізняють відповідно основні види м.: амплітудну, кутову (частотну, фазову) та імпульсну. Частота модулюючого сигналу повин-

на бути малою порівняно з несучою.

М. амплітудна (АМ) /м. амплитудная (АМ)/ [Amplitude M. (AM)] — модуляція несучої, при якій параметром, що змінюється, є амплітуда коливань.

М. амплітудно-імпульсна (АІМ) /м. амплитудно-импульсная (АИМ)/ [pulse amplitude m.] — модуляція імпульсна, при якій параметром, що змінюється, є амплітуда імпульсів.

М. імпульсна /м. импульсная/ [pulse m.] — модуляція несучої послідовністю імпульсів.

М. кутова /м. угловая/ [angle m.] — модуляція несучої, при якій параметром, що змінюється, є частота і фаза коливань.

М. несучої /м. несущей)/ [carrier m.] — див. модуляція.

М. фазова (ФМ) /м. фазовая (ФМ)/ [Phase M. (PM)] — кутова модуляція, при якій фаза несучої змінюється пропорційно миттєвим значенням сигналу модулюючого.

М. фазово-імпульсна (ФІМ) /м. фазоимпульсная (ФИМ)/ [displacement-position m., pulse-position m.] — імпульсна модуляція, при якій параметром, що змінюється, є фаза імпульсів.

М. частотна (ЧМ) /м. частотная (ЧМ)/ [Frequency M. (FM)] — модуляція кутова, при якій відхилення частоти модульованого сигналу змінюється пропорційно миттєвим значенням сигналу модулюючого.

М. частотна вузькосмугова /м. частотная узкополосная/ — модуляція частотна, при якій девіація (найбільше відхилення) частоти менша, ніж максимальна частота сигналу модулюючого.

М. частотна широкосмугова /м. частотная широкополосная/ — модуляція частотна несучої, при якій девіація (найбільше відхилення) частоти коливань в декілька разів перевищує максимальну частоту сигналу модулюючого.

М. частотно-імпульсна (ЧІМ) /м. частотно-импульсная (ЧИМ)/ [pulse-frequency m.] — модуляція імпульсна, при якій параметром, що змінюється, є частота слідування імпульсів.

М. широтно-імпульсна (ШІМ) /м. широтно-импульсная (ШИМ)/ [pulse duration m.] — модуляція імпульсна, при якій параметром, що змінюється, є тривалість імпульсів.

МОНІТОР /монитор/ [monitor] (від лат. monitor — остерігаючий) — 1) Машинна програма, яка спостерігає, регулює, контролює або перевіряє операції в системі оброблення даних. 2) Прилад, для контролю за параметрами, які мають залишатися в заданих межах. 3) Дисплей, що використовується для контролю процесів і управління системою.

М. системи відеоконтролю /м. системы видеоконтроля/ — пристрій, призначений для перетворення сигналу телевізійного в зображення. Може приєднуватися до камери телевізійної безпосередньо за допомогою кабелю. М. поділяються також на чорно-білі і кольорові. Вони можуть мати розмір екрана 7, 9, 12, 14, 15, 17, 21 дюйм (1 дюйм дорівнює 2,54 см) і роздільну здатність до 1000 ліній у центрі екрана. Для зменшення кількості моніторів в системі відеоконтролю між телевізійними камерами і моніторами вмикають комутатори, квадратори і мультиплексори.

МОНІТОРИНГ /мониторинг/ [monitoring] (від лат. monitor — остерігаючий) — безперервне слідкування за станом навколишнього середовища і управління ним, своєчасне інформуванням людей про можливе настання несприятливих, критичних або недопустимих ситуацій. Прикладом використання моніторингу є експертні системи, в яких порівнюються результати спостережень за поведінкою об'єкта з критичними точками, критичними властивостями й слабкими місцями.

М. інформаційної безпеки /м. информационной безопасности/ [information security m.] — безперервне і послідовне слідкування за станом загроз, зв'язаних з можливим розв'язанням війни інформаційної, з постійною і тверезою оцінкою можливості протидії, нейтралізації і запобіганню цих загроз. М. і. б. повинен охоплювати: динаміку зовнішньополітичної ситуації, глобальні і локальні протиріччя і конфлікти; науково-технічний прогрес в галузі розробки засобів і методів проникнення в ресурси інформаційні і впливи на інфраструктуру інформаційну, а також в галузі захисту інформації; стан внутрішнього і міжнародного законодавчо-правового забезпечення безпеки інформаційної; стан і ефективність систем забезпечення інформаційної безпеки.

М. політичних подій /м. политических событий/ [political m.] — система відслідковування політичних

подій, виявлення, раннього попередження і випередження небажаних подій.

МОТИВАЦІЇ (СПОНУКАННЯ) /мотивации (побуждения)/ [motivation] — активні стани мозкових структур, що спонукають вищих тварин та людину здійснювати дії, що спадково закріплені або набуті внаслідок досвіду, спрямовані на задоволення індивідуальних (голод, спрага і т. ін.) або групових (турбота за потомство і т. ін.) потреб.

МОТИВИ /мотивы/ [motive] — те, що спонукає діяльність людини, із-за чого вона здійснюється. В широкому розумінні до м. відносять потреби й інстинкти, потяги й емоції, установки й ідеали. Див. також мотивації.

МУЛЬТИМЕДІА /мультимедиа/[multimedia] (від лат. multum — багато і медіа) — 1) Складні поліфункціональні системи для збирання, оброблення, передавання і перетворення інформації з одних форм в інші із широкими можливостями їхнього інтерактивного сприйняття й використання в різноманітних цілях. 2) Сполучення рухомих і нерухомих образів, звуку і даних у цифровій формі, що допомагає їхньому зберіганню, копіюванню й передаванню без втрати якості.

МУЛЬТИМЕДІАТИЗАЦІЯ /мультимедиатизация/ [multimediatization] — упровадження мультимедіа в різноманітні сфери інформаційної діяльності.

МУЛЬТИПЛЕКСОР /мультиплексор/ [multiplexer] (від лат. multiplex — складний, численний) — функціональний пристрій, який дозволяє двом або більше каналам спільно використовувати один загальний засіб передавання даних.

М. оптичний /м. оптический/ [optical m. (demultiplexer)] — пристрій для поєднання (розділення) сигналів оптичних різної довжини хвиль.

М. передавання даних (МПД) /м. передачи данных (МПД)/ [telecommunication control unit, telecommunication m.] — 1) Приферійний пристрій, призначений для дистанційного приєднання до ЕОМ декількох пунктів абонентських і забезпечення роботи з ними під керуванням системи обчислювальної.

2) Пристрій, який забезпечує ущільнення декількох каналів передавання даних в одному каналі зв'язку.

М. передавання даних віддалений /м. передачи данных отдаленный/ [renome communication m.] — пристрій, який забезпечує сполучення декількох низькошвидкісних каналів передавання даних з одним надшвидкісним каналом.

М. передавання даних програмований /м. передачи данных программированный/ — мультиплексор передавання даних, в якому передбачене програмоване оброблення даних, в тому числі контроль, перетворення, адресацію і розпізнавання повідомлень.

М. системи відеоконтролю /м. системы видеоконтроля/ — мультиплексор, призначений для забезпечення запису на ідеомагнітофон сигналів від приєднаних камер телевізійних, спостереження на екрані монітора зображень камер і відеомагнітофона в будь-якій комбінації як за розмірами зображень, так і по їхній кількості. М. с. в. також можуть обладнуватися детекторами руху, які сповіщають операторів або вмикають відеомагнітофони при зміні картинки на одній або декількох камерах.

МУЛЬТИПЛЕКСУВАННЯ /мультиплексирование/ [multiplexing] — ущільнення сигналів при передаванні даних для декількох пристроїв по одному каналу. Мультиплексні канали і мультиплексори відіграють велику роль в розвитку сучасних супермагістралей інформаційних.

Н

НАВАНТАЖЕННЯ /нагрузка/ [load] — в мережах інформаційно-обчислювальних — кількість пакетів даних, що генеруються за одиницю часу усіма джерелами даних і вводяться в мережу для передавання.

НАВЕДЕННЯ /наводка/ [aiming] — установлення зв'язку, контакту.

Н. паразитне /н. паразитная/ [spurious a.] — передача електричних сигналів з одного елемента радіопристрою в інший, не передбачена його схемою і конструкцією. Н. п. виникають із-за зв'язків паразитних індуктивних і ємнісних. Н. п. створюють загрозу безпеці інформації у випадку наведень на кола, що мають вихід сигналів з інформацією, що належить захисту, за межі зони контрольованої. Найбільшу загрозу ство-

рюють наведення в проводах кабелів телефонної мережі, радіотрансляції, електроживлення від сигналів розташованих поряд кабелів, по яких передається конфіденційна інформація. Крім того, наведення дуже малого рівня можуть модулювати високочастотний сигнал, що розповсюджується за межі контрольованої зони.

НАВІДНИК /наводчик/ [gunner] — особа, що вказує співробітникові розвідки на людину як на потенційного агента. Після цього співробітник розвідки здійснює оперативне розроблення кандидата і приступає до вербування.

НАВІЮВАНІСТЬ /внушаемость/ [suggestibility] — властивість психіки, що виявляється в її піддатливості до впливу психологічного. Н. зв'язана з віковими (діти більш піддаються навіюванню ніж дорослі), статевими (жінки більш піддаються навіюванню ніж чоловіки), індивідуальними психологічними особливостями людей, з їхньою силою волі, життєвим досвідом, а також з широтою кругозору, компетентністю і рядом інших факторів. З нагромадженням життєвого досвіду, наукових і професійних знань схильність людини до н. знижується, проте і в зрілому віці люди в цій чи іншій мірі схильні до неї. Розрізняють навіюваність загальну, навіюваність ситуативну, а також навіюваність індивідуальну і групову. Н. підсилює: особливості психічного розвитку конкретної особистості (звичку скорятися, безвідповідальність, боязкість, незручність, соромливість, довірливість, підвищену емоційність, вразливість, мрійливість, бентежність, слабкість логічного мислення, схильність до наслідування, схильність до фантазування, забобонність, релігійність); ситуативні фактори (тілесне розслаблення, сонливість, втому [загальну, органів чуття, мислення], біль, сильне емоційне збудження, стурбованість, почуття безвихідності стану, нудьги, симпатії до об'єкта, слабку волю, низьку критичність мислення, слабкі монотонні подразники, некомпетентність у питаннях і видах діяльності, малу ступінь їхньої значущості для людей, відсутність досвіду дій у складній або незнайомій обстановці, дефіцит часу для прийняття рішень, несподіваність навіювання); деякі захворювання (або певного стану) об'єкта (розумова відсталість, фізичне виснаження, нервово-психічна астенія

[підвищена втомлюваність, нестійкість настрою, порушення сну], наркоманія, алкоголізм, імпотенція).

Н. групова /в. групповая/ — навіюваність, що забезпечується взаємонавіюванням (зараженням) між членами групи.

Н. загальна /в. общая/ — навіюваність, зумовлена особливостями психічного розвитку конкретної особистості, вона властива усім людям, хоча в різній мірі.

Н. індивідуальна /в. индивидуальная/ — навіюваність однієї конкретної людини.

Н. ситуативна /в. ситуативная/ — навіюваність, що виникає як наслідок анормальних станів психіки, дефіциту інформації і т. ін.

НАВІЮВАННЯ /внушение/ [suggestion] — вплив на особистість, що призводить або до появи у людини всупереч його волі й свідомості певного стану, почуття, відношення, або до здійснення людиною поступку, що безпосередньо не витікає з прийнятих ним норм і принципів діяльності. Об'єктом н. може бути як окрема людина, так і групи, колективи, соціальні верстви населення. Н. є одним з базових методів психологічного впливу (див. метод навіювання). В цьому випадку н. повинні бути властиві наступні характеристики: цілеспрямованість і плановість н.; конкретність об'єкта н.; некритичність сприйняття інформації об'єктом н.; визначеність поведінки, що ініціюється. Ефективність впливу н., звичайно, залежить від: здатності суб'єкта до н., зв'язаної з такими його якостями як інтелект і кмітливість, воля й упевненість у собі, кругозір і компетентність, доброзичливість до об'єкта, власна переконаність у тому, що навіюється; змісту н., що залежить від характеру інформації, що навіюється, та її місця в інформаційному потоці (якщо інформація, що навіюється, розташована на початку потоку, то сприйнятливість до н. умовно можна оцінити в 50%, в середині — в 30%, в кінці — 70%); навіюваності об'єкта впливу, зв'язаної з відношенням об'єкта до суб'єкта. Тактичні принципи використання н. у війні психологічній полягають у наступному: необхідно використати такі способи й прийоми н., які здатні викликати специфічний інтерес конкретних груп військовослужбовців і населення противника; треба використати такі способи й прийоми н., які здатні нейтралізувати небажані ідеї і настрої у більшості представників цих груп; потрібно використати такі способи й прийоми н., які не

будуть нехтувати до тих пір, поки не буде досягнута мета психологічної операції. Н. можна класифікувати за способом навіюючого впливу — навіювання відкрите, навіювання закрите; за засобами впливу — навіювання контактне, навіювання дистантне; за інтервалом часу між впливом і зворотною реакцією — навіювання безпосереднє, навіювання відстрочене; за тривалістю ефекту впливу — навіювання короткочасне, навіювання довготривале; за змістом впливу — навіювання специфічне, навіювання неспецифічне.

Н. безпосереднє /в. непосредственное/ — навіювання, при кому зворотна реакція об'єкта виникає відразу після сприйняття навіюючого впливу.

Н. відкрите (пряме) /в. открытое (прямое)/ — навіювання з конкретною, чітко визначеною метою. Наприклад, людей закликають до виконання певних дій. В. н. відрізняється прямою спрямованістю на певний об'єкт.

Н. відстрочене /в. отстроченное/ — навіювання, при якому між впливом і зворотною реакцією існує той чи інший розрив у часі (створюється установка на спрацьовування навіювання у майбутньому).

Н. дистантне /в. дистантное/ — навіювання, що здійснюється за допомогою засобів усної та друкованої пропаганди, радіо й телебачення. В цьому випадку зворотній зв'язок між суб'єктом і об'єктом навіюючого впливу відсутній.

Н. довготривале /в. длительное/ — навіювання, що характеризується збереженням впливу протягом достатньо тривалого проміжку часу.

Н. закрите (непряме) /в. закрытое (косвенное)/ — навіювання, що характеризується замаскованістю мети, або не має прямої спрямованості на того, хто є істинним об'єктом впливу.

Н. контактне /в. контактное/ — навіювання, що здійснюється в умовах безпосереднього спілкування з об'єктом, головним чином, в населених пунктах, що зайняті своїми військами, і серед військовополонених. З цією метою фахівці психологічної війни проводять індивідуальні бесіди, мітинги, збори, інформування, різноманітні культурно-розважальні заходи. К. н. найбільш ефективне, оскільки має місце зворотній зв'язок

з аудиторією, але в бойовій обстановці воно застосовується дуже рідко.

Н. короткочасне /в. кратковременное/ — навіювання, що характеризується невеликим періодом ефективності впливу. Наприклад, військовослужбовець на полі бою може відчувати протягом нетривалого часу почуття страху, яке ініціюється навіюючим впливом.

Н. неспецифічне /в. неспецифическое/ — провокування у об'єкта негативних психічних станів, щоб викликають певну поведінку. У процесі здійснення н. н. мовні (вербальні) фактори сполучають з немовними (невербальними). Основна мета н. н. — формування у об'єкта впливу астенічних станів, в основі яких лежить феномен фрустрації. Н. н. саме через акцентування фрустрації провокує у об'єкта астенічні психологічні стани (неспокій, депресію, страх, паніку і т. ін.). Основними способами н. н. є: спосіб залякування; спосіб емоційного придушення; спосіб ініціювання агресивних емоційних станів.

Н. специфічне /в. специфическое/ — навіювання об'єктові певних, дуже конкретних ідей, установок, мотивів з метою заміщення ними існуючих і провокування у нього певної реакції у зміні поведінки. При н. с. використовують тільки вербальні (мовні) засоби впливу і воно, як складова частина навіювання, значно підсилює його ефективність. Розрізняють і застосовують наступні основні способи н. с.: спосіб приклеювання ярликів, спосіб сяючого узагальнення, спосіб перенесення, спосіб свідчення, спосіб гри в простонародність, спосіб перетасовки фактів, спосіб загальної платформи. Способи й прийоми н. с. та навіювання неспецифічного складають основний зміст впливів психологічних на основі навіювання.

НАГРОМАДЖЕННЯ (НАКОПИЧЕННЯ) /накопление/ [accumulation, cumulation] — поступове збирання, накопленння в будь-якій кількості.

Н. інформації /н. информации/ [a. of information] — один з основних видів роботи інформаційної. Розрізняють нагромадження інформації активне і нагромадження інформації пасивне. Розвиток інформатики постійно пересуває межу можливостей добування знань при н. і. із застосуванням ЕОМ. Одна з первинних завдань н. і. — перетворення нагромаджуваної інформації з форми у вигляді фізичних сигналів у символьну форму, а також стиснення інформації, тобто зменшення надмірності в її поданні. При цьому

часто доводиться вирішувати задачу розпізнавання образів, наприклад, розпізнавання мови, оброблення зображень.

Н. інформації активне /н. информации активное/ — нагромадження інформації, при якому здійснюється певне оброблення інформації, що поступає, спрямоване на збагачення знань одержувача інформації.

Н. інформації пасивне /н. информации пассивное/ — нагромадження інформації, при якому інформація, що поступає, просто "складується", при чому приймаються заходи до забезпечення її збереження і повторного зчитування.

НАГРОМАДЖУВАЧ /накопитель/ [drive, storage, accumulator] — 1) пристрій запам'ятовуючий зовнішній. 2) У СКБД — основна частина бази даних, призначена для розташування і зберігання даних.

Н. активний /н. активный/ [active disk unit] — нагромаджувач на дискові магнітному, доступний в даний момент системі і користувачу.

Н. на гнучких магнітних дисках (НГМД) /н. на гибких магнитный дисках (НГМД)/ [floppy-disk d.] — нагромаджувач, в якому носіями інформації є змінні диски магнітні гнучкі.

Н. на магнітних дисках (НМД) /н. на магнитных дисках (НМД)/ [magnetic disk storage] — нагромаджувач, носієм інформації в якому є магнітні диски, об'єднані в пакет.

Н. на магнітних картах /н. на магнитных картах/ [magnetic card s.] — нагромаджувач, носієм інформації в якому є магнітні карти.

Н. на магнітній стрічці (НМС) /н. на магнитной ленте (НМЛ)/ [magnetic tape s.] — нагромаджувач, в якому носієм інформації є магнітна стрічка. Відрізняється великою ємністю, але малою швидкодією.

Н. на магнітному барабані (НМБ) /н. на магнитном барабане (НМБ)/ [magnetic drum s.] — нагромаджувач, носієм інформації в якому служить магнітний барабан. Відрізняється високою швидкодією, але малою ємністю.

Н. на магнітооптичних дисках /н. на магнитооптических дисках/ [magneto-optic disk s.] — нагро-

маджувач, носієм інформації в якому є диск магнітооптичний.

Н. на оптичних дисках /накопитель на оптических дисках/ [optical disk s.] — нагромаджувач, носієм інформації в якому є диск оптичний. Відрізняється високою швидкодією і дуже великою ємністю.

Н. на фіксованому диску /н. на фиксированном диске/ [fixed d.] — нагромаджувач на диску, що має носій інформації, який не знімається.

НАДІЙНІСТЬ /надежность/ [reliability] — властивість системи зберігати величини вихідних параметрів у межах установлених норм при заданих умовах (забезпечити нормальну роботу системи). Для н. систем автоматизованих можна виділити окремо надійність апаратури і надійність програмного забезпечення комплексу засобів автоматизації. Проблема надійності для таких систем вирішується наступними шляхами: підвищенням надійності деталей і вузлів; побудовою надійних систем з менш надійних елементів за рахунок структурної надмірності (дублювання, потроєння елементів, пристроїв, підсистем і т. ін.); застосуванням контролю функціонального з діагностикою відмови, що збільшує надійність функціонування системи шляхом скорочення часу відновлення апаратури, що відмовила.

НАДМІРНІСТЬ /избыточность/ [redundancy] — перевершеність міри, звичайної норми чого-небудь; зайвинність, надлишковість.

Н. мови /и. речи/ [r. of language] — надмірність, зумовлена різними значеннями частоти використання у мові букв, а також суттєво меншою кількістю дозволених граматикою складів, слів і фраз по відношенню до можливих комбінацій складів, слів і фраз, які теоретично можна скласти з букв алфавіту. У природних мовах наступні одне за другим слова, зв'язані між собою смислом і синтаксисом граматики, а послідовно розташовані букви в межах одного слова — правилами орфографії. Чим більше букв в алфавіті, менше словниковий склад мови і суворіші правила граматики, тим вища н. м.

НАЛЕЖНІСТЬ /принадлежность/ — у значенні входити до складу чого-небудь, відноситися до розряду кого-, чого-небудь.

Н. групова /п. групповая/ — характеристика об'єктів психологічної війни, що визначає належність

об'єктів психологічної війни (операції) до певної групи соціальної. Н. г. необхідно постійно уточнювати в інтересах правильної й ефективної організації операцій психологічних. Зокрема, найкращими об'єктами впливу психологічного є: військовослужбовці недавно сформованих і резервних частин; військовослужбовці підрозділів, що знаходяться в оточенні; особовий склад підрозділів, що понесли великі втрати в ході бойових дій; групи військовослужбовців, що незадоволені курсом уряду й утягненням країни у війну; військовослужбовці частин, що знаходяться в гіршому матеріально-побутовому становищі ніж інші; підрозділи, в яких відмічаються прояви соціальних, національних, релігійних та інших конфліктів; групи солдат і офіцерів противника з числа національних меншин; прошарки, групи клани та інші угруповання цивільного населення, що незадоволені своїм правовим, економічним, соціальним положенням; пацифістські, дисидентські і деякі релігійні групи.

НАПАД /нападение/ [attack] — у значенні накидатися на кого-, що-небудь з ворожими намірами, а також взагалі почати діяти проти кого-небудь з ворожими цілями.

Н. інформаційний /н. информационное/ [information a.] — атака на мережу обміну інформацією віддалена, яка полягає у раптовому застосування зброї інформаційної для здійснення впливів на мережу противника. Ефективність н. і. досягається у тому випадку, якщо забезпечені його широкомасштабність, довгостороковість та скритність.

НАУКА /наука/ [science] — 1) Динамічна система знань, які розкривають нові явища у суспільстві і природі з метою їхнього використання у практичній діяльності людей. 2) Сфера дослідницької діяльності, спрямованої на вироблення знань про природу, суспільство та мислення, яка включає в себе всі умови та моменти цього виробництва: учених з їхніми знаннями та здібностями, кваліфікацією та досвідом, з розподілом та кооперацією наукової праці; наукові заклади, експериментальне й лабораторне обладнання; методи науково-дослідної роботи, апарат понять та категорій, систему інформації наукової, а також усю суму наявних знань, що виступає як передумова або засіб, або результат наукового виробництва. Безпосередні функції науки — опис, пояснення та передбачення процесів і явищ, які складають предмет її вивчення, на

основі законів, що відкриваються нею. Система науки умовно ділиться на природничі, суспільні та науки про мислення.

НАЦІЯ /нация/ [nation] (від лат. natio — народ, плем'я) — стійка історична спільність людей, що визначається соціальними зв'язками певної формації і характеризується специфічними етнічними рисами, зумовленими особливостями економічного і культурного розвитку, спільністю території, мови, побуту, традицій і звичаїв, а також відображенням цих факторів в суспільній свідомості і суспільній психології.

НЕБЕЗПЕКА /опасность/ [danger, hazard] — 1) Здатність викликати будь-яку шкоду. 2) Можливість, загроза виникнення будь-чого дуже поганого, будь-якого нещастя.

Н. інформаційна /о. информационная/ [information d.] — можливість, загроза заподіяти будь-яку шкоду, приносити нещастя при впровадженні і використанні технологій інформаційних нових. Джерела н. і. можуть бути природними (об'єктивними) і навмисними. Перші виникають в результаті ненавмисних помилок та несправностей, випадкових факторів, стихійних бід і т.ін. Навмисні інформаційні впливи здійснюються свідомо і цілеспрямовано. Виділяють наступні найбільш суттєві групи навмисних н. і.: застосування зброї інформаційної; злочини комп'ютерні; електронний контроль за приватним життям та суспільно-політичними відносинами; використання нових інформаційних технологій в політичних цілях.

НЕВИЗНАЧЕНІСТЬ /неопределенность/ [uncertainty] — ситуація, при якій не все точно встановлене. В теорії інформації мірою н. є ентропія.

Н. апостеріорна /н. апостериорная/ [posterior u.] (від лат. a posteriori — з наступного) — невизначеність, набута з досвіду.

Н. апріорна /н. априорная/ [prior u.] (від лат. a priori — з попереднього) — невизначеність, що передує досвіду.

НЕВІДСЛІДКОВАНІСТЬ /неотслеживаемость/ [untraceability] — властивість транзакції, коли абонент є не тільки анонімним, але і дві транзакції, які створені одним і тим абонентом, не можуть бути ув'язані між собою при будь-яких обставинах. Така властивість досить часто застосовується в системах електронних

грошей та електронної торгівлі.

НЕЛЕГАЛ /нелегал/ [illegal] (від не... і лат. legalis, від lex — закон) — співробітник розвідки, що знаходиться на оперативній роботі за кордоном і видає себе за громадянина країни перебування або за іноземця. Основна робота н. — вербування агентів, що мають доступ до секретної інформації або до об'єктів, закладів, що цікавлять розвідку. Н., який роз'їжджає із країни в країну, називають "гастролером".

НЕСУЧА /несущая/ [carrier (frequency)] — електромагнітне коливання, призначене для утворення сигналу радіочастотного шляхом змінювання одного або декількох параметрів цього коливання.

НОВИНИ /новости/ [news] — нові відомості, вісті, звістки, повідомлення, але насамперед про найважливіші події в країні й світі.

Н. м'які /н. мягкие/ [soft n.] — інформація, яка на відміну від новин твердих може нести на собі відбиток авторської індивідуальності як у виборі подій, так і у формі їх викладення.

Н. тверді /н. твердые/ [hard n.] — інформація про важливі події і незаперечні факти в стилі, що не допускає (на відміну від новин м'яких) думок або суб'єктивних оцінок журналістів і канони суворих лапідарних (стислих, коротких, виразних) повідомлень, які за мовою й тоном повинні носити об'єктивно-відповідальний характер.

НОМЕР /номер/ [number] (від лат. numerus — число) — порядкове число предмета в ряді інших однорідних.

Н. ідентифікаційний персональний (ПІН) /н. идентификационный персональный (ПИН)/ [Personal Identification N. (PIN)] — вид паролю, що, звичайно, складається тільки з цифр, і який, як правило, має бути пред'явлений нарівні з ідентифікатором, що носиться.

НОНКОМУНІКАЦІЯ /нонкоммуникация/ [noncommunication] — термін для характеристики негативних комунікативних можливостей сучасних ЗМІ. Вважається, що вони можуть занурювати аудиторію у міражі тотальної знаковості, робити її інертною й безвольною, перетворювати її в об'єкт для маніпулювання в інтересах не виявлення, а містифікації істин, що призводить до відмови від волевиявлення й відновлення

в суспільному житті й комунікаціях, які стають засобами не загальнолюдських зв'язків, а засобами їхнього руйнування.

НОНКОНТРАКТ /нонконтракт/ [noncontract] (ам. — скорочення від англ. non contractor — крім підрядчиків) — термін, прийнятий для позначення інформації і матеріалів, які заборонено показувати або передавати в руки представників комерційних фірм, що співробітничають з державними структурами, незалежно від того, чи є в них допуск до секретної інформації та який.

НОНФОРН /нонформ/ [nonforn] (ам. — скорочення від англ. non foreign — крім іноземців) — термін, прийнятий для позначення секретної інформації і матеріалів, які заборонено показувати або передавати в руки громадян іноземних держав незалежно від того, чи є у них допуск до секретної інформації і який.

НОРМА /норма/ [norm, standard] (від лат. norma — правило, взірець) — звичайний, узаконений, загальноприйнятий, обов'язковий порядок, стан і т. ін.; правило, стандарти.

Н. ефективності захисту інформації /н. эффективности защиты информации/ — значення показників ефективності захисту інформації, встановлені документами нормативними.

Н. законів про інформаційні ресурси, продукцію, послуги /н. законов о информационных ресурсах, продукции, услугах/ — норми інформаційно-правові, що регулюють відносини в галузі ресурсів інформаційних, інформаційної продукції, послуг інформаційних. Такими нормами захищаються: інформаційні ресурси і продукція від доступу несанкціонованого; інформаційні ресурси як національне надбання; інформаційні ресурси як твори, засновані на підборі і розташуванні матеріалу; інформаційні ресурси і продукція як речова власність і т. ін.

Н. законів про інформаційні технології /н. законов о информационных технологиях/ — норми інформаційно-правові, що регулюють відносини у зв'язку з виробництвом і застосуванням технологій інформаційних і засобів їхнього забезпечення. Такими нормами захищаються: системи інформаційні, банки і бази даних, їхні мережі як інтелектуальна і речова власність; інформаційні системи, банки і бази даних, їхні мережі від доступу несанкціонованого; носії машинні з інформацією, наприклад, засобами підпису ци-

фрового електронного; бази даних (знань) в складі систем інформаційних автоматизованих і їхніх мереж; програмні засоби в складі ЕОМ, їхніх мереж як інтелектуальна власність і т. ін.

Н. законів про право на інформацію /н. законов о праве на информацию/ — норми інформаційно-правові, що регулюють відносини з приводу права на інформацію, захищаючи право на пошук, одержання, споживання і розповсюдження інформації.

Н. законів про створення і розповсюдженням інформації /н. законов о создании и распространении информации/ — норми інформаційно-правові, що регулюють відносини у зв'язку із створенням і розповсюдженням інформації. Таким нормами захищаються: інформація як результат творчої діяльності; інформація документована як власність інтелектуальна і речова; громадянин, суспільство, держава від впливу недостовірної, неправдивої інформації; честь і достоїнство громадянина у зв'язку із створенням і розповсюдженням недостовірної інформації або несанкціонованим розповсюдженням інформації про нього; інформація як таємниця комерційна; дані персональні як інформація конфіденційна про особистості і т. ін.

Н. інформаційно-правова /н. информационно-правовая/ — норма права, що регулює будь-які відносини у сфері інформаційній. Типові н. і.-п. повинні забезпечувати регулювання відносин з приводу прав, обов'язків і відповідальності суб'єктів у зв'язку: з створенням і розповсюдженням інформації; з формуванням і використанням інформаційних ресурсів; з реалізацією права на пошук, одержання, передачу і споживання інформації; з створенням і застосуванням інформаційних систем, інформаційних технологій і засобів їхнього забезпечення; з створенням і застосуванням засобів і механізмів інформаційної безпеки.

Н. права /н. права/ [n. of law, legal n.] — форма вираження права, санкціоноване державою, обов'язкове правило загального характеру (закон, указ, постанова) в цій чи іншій галузі суспільних відносин. Н. п. можуть бути прямої дії або системостворюючими. Сукупність н. п., що регулюють однорідні відносини, створюють галузі права (державне, цивільне, кримінальне, право інформаційне і т. ін.).

Н. права системостворюючі /н. права системообразующие/ — норми права, призначені для створе-

ння умов для комплексного регулювання відповідного виду відносин за допомогою актів підзаконних.

Н. про відповідальність за правопорушення в інформаційній сфері /н. об ответственности за правонарушения в информационной сфере/ — норми інформаційно-правові про відповідальність за правопорушення при формуванні і використанні ресурсів інформаційних, при споживанні інформації, при створенні і застосуванні технологій інформаційних і засобів їхнього забезпечення, а також створення і застосування засобів і механізмів інформаційної безпеки. До складу вказаних норм можуть входити наступні види відповідальності: за порушення прав інтелектуальної власності на інформацію; за недостовірну і неправдиву інформацію, що створюється і розповсюджується засобами масової інформації; за приховування і навмисне викривлення інформації про джерела загроз; за неподання інформації про формування інформаційних ресурсів; за псування або втрату документів; за недостовірність, неповноту і несвоєчасність подання обов'язкової інформації; за порушення процесів і правил формування інформаційних ресурсів; за порушення процесів і правил підготовки і надання інформаційних продуктів і послуг інформаційних, за несвоєчасне надання інформації, за необґрунтовану відмову в наданні інформації, за надання неякісної і недостовірної інформації; за невстановлення правил надання інформації; за порушення правил одержання і споживання інформації; за незаконне одержання і використання інформації з обмеженим доступом; за створення неякісних інформаційних технологій і засобів їхнього забезпечення; за порушення прав і свобод особистості, зв'язаних з інформацією; за незаконне використання персональних даних; за порушення інституту таємниці — державної, особистої, виробничої, комерційної; за злочини комп'ютерні; за порушення заборони віднесення відкритої інформації до інформації з обмеженим доступом; за порушення правил ліцензування і сертифікації в інформаційній сфері; за незаконний доступ до інформаційних систем, засобів зв'язку і передавання інформації; за порушення правил охорони ліній і споруд зв'язку.

НОСІЙ /носитель/ [carrier, medium] — пристрій, що несе, переміщає будь-що, а також взагалі те, що охоплює, несе в собі будь-що.

Н. відомостей, що складають державну таємницю /н. ведомостей, содержащих государствен-

ную тайну/ — матеріальні об'єкти, в тому числі фізичні поля, в яких відомості, що складають таємницю державну, знаходять своє відображення у вигляді символів, образів, сигналів, технічних рішень і процесів.

Н. інформації (даних) /н. информации (данных)/ [data m.] — матеріальні об'єкти, що забезпечують запис, зберігання і передавання інформації у просторі і часі. Н. і. можуть бути: люди; матеріальні тіла (макрочастки); поля (випромінювання); елементарні частки (мікрочастки).

Н. інформації через державний кордон /н. информации через государственную границу/ — носії інформації, які можуть легально або нелегально перетинати державний кордон. Основними носіями такого виду є: люди, що зберігають інформацію у своїй пам'яті; матеріальні тіла з інформацією, які перевозяться або переносяться людьми; електромагнітні випромінювання у світловому (оптичному) та радіодіапазонах.

Н. кодів паролів /н. кодов паролей/ — носії, призначені для запису на них і зчитування кодів паролів. Такими носіями можуть бути перепустки в контрольно-пропускних системах, різного виду картки для ідентифікації особи або оригіналів документів, кредитні картки, пристрої типу Touch Memory і т.ін. Вибір того чи іншого носія визначається вимогами до автоматизованої системи, її призначення, ступеня захисту інформації, кількості користувачів, вартості і т. ін.

Н. машинний (Н. машиночитаний) /н. машинный (н. машиночитаемый)/ [machine m. (machine-readable m.)] — носій, інформація з якого може бути введена в ЕОМ без додаткового проміжного перетворення.

Н., що розповсюджуються за межі контрольованої зони /н., распространяемые за границы контролированной зоны/ — носії інформації, для яких є можливим вихід за межі зони контрольованої. До таких носіїв можна віднести: людей; паперові і машинні носії з документами і публікаціями; продукцію, матеріали, сировину, обладнання, газоподібні, рідинні і тверді відходи, частки радіоактивного випромінювання; акустичні, електричні, магнітні і електромагнітні сигнали і випромінювання, електричний струм, що розповсюджуються проводами електроживлення, телефонної мережі, охоронної і пожежної сигналізації і т.ін. Ці носії можуть містити інформацію семантичну і ознакову, а також речовини демаскуючі.

За дальністю розповсюдження вказані носії поділяють на три групи: носії без обмеження відстані (люди, документи, які перевозять або переносять, продукція, відходи та інші матеріальні носії); носії, що розповсюджуються за межі прямої видимості (акустичні хвилі великої потужності, радіохвилі в діапазонах довгих, середніх та коротких хвиль, електричний струм з інформацією в кабелях, світло (через світловоди), рідинні та газоподібні відходи; носії, що розповсюджуються в межах прямої видимості (світло, мова, радіохвилі в ультракороткохвильовому діапазоні, слабкострумові електричні сигнали, радіоактивні промені.

НОУ-ХАУ /ноу-хау/ [know-how] (ам. — знання справи, букв. знаю, як) — 1) Технічні знання, досвід, секрети виробництва, методи, алгоритми, програмне забезпечення, технології, необхідні для вирішення технічних або інших задач. Термін застосовується до технічної і іншої інформації. Роль н.-х. росте в умовах ринку. В міжнародній практиці під н.-х. розуміють договір про передачу технічних знань, досвіду, навичок в формі документації. Як правило, він супроводжується направленням фахівців для налагодження виробничого процесу. 2) Науково-технічна інформація про останні досягнення та спеціалізовані видання, що містять якісну інформацію про суспільно-економічне та культурно-політичне життя окремих країн і світу у цілому. Вважається, що така інформація є важливою умовою розвитку суспільства інформаційного, яка забезпечує його головні сфери інтелектуальними ресурсами когнітаріату.

О

ОБ'ЄКТ /объект/ [object] (від лат. objectus — предмет) — 1) Певна частина реальної дійсності, що оточує нас (предмет, процес, явище). 2) В мережах обчислювальних — комплекс взаємопов'язаних спільною метою функцій одного рівня; елемент проблемної структури обчислювальної мережі. 3) В теорії захисту інформації — пасивна сутність, яка підлягає захисту.

О. авторського права /о. авторского права/ — первинні твори, в тому числі літературні (включаючи програми для ЕОМ), і так звані вторинні, тобто похідні твори (переклади, обробки, анотації, реферати, резюме, огляди, інші переробки творів науки, літератури і мистецтва), а також збірники та інші складені

твори, що являють собою за підбором і розташуванням матеріалу результати творчої праці (енциклопедії, антології, бази даних). Не є об'єктами авторського права офіційні документи, їхні офіційні переклади; повідомлення про події і факти, що мають інформаційний характер.

О. атаки /о. атаки/ — сторона, що атакується. В мережах обміну інформацією (МОІ) вона може бути представлена окремим комп'ютером (з інформацією, що зберігається й обробляється в ньому), сегментом МОІ або МОІ в цілому.

О. атаки хибний (ХОА) /о. атаки ложный (ЛОА)/ — об'єкт або елемент мережі інформаційно-обчислювальної, що підставляється противникові та імітує процес або результат роботи об'єкта атаки, вибраного противником. О. а. х. призначений для використання в процесі протидії інтелектуальної і сприяє досягненню мети інформаційної боротьби в інформаційно-обчислювальній мережі. У відповідності до принципів побудови хибного об'єкта атаки в загальному випадкові о. а. х. складається з наступних модулів: модуля взаємодії з противником; основного модуля, який відповідає за перетворення даних і композицію усіх інших модулів о. а. х.; модуля взаємодії із суб'єктом інформаційної боротьби; модуля взаємодії з центром безпеки інформаційно-обчислювальної мережі. О. а. х. повинен функціонувати, на основі коректно побудованого алгоритму інтелектуальної протидії, залучаючи, коли це необхідно суб'єкта інформаційної боротьби для вирішення нетривіальних ситуацій взаємодії з противником.

О. віртуальний /о. виртуальный/ [virtual o.] — ідеальний об'єкт, описаний у вигляді діючою програмної моделі. У взаємодії з користувачем проявляє себе як реальний об'єкт.

О. демаскуючий /о. демаскирующий/ — об'єкт, на основі ознак якого можна не тільки виявити об'єкт, що належить захисту, але і визначити його характеристики. Окреслення в об'єкті захисту о. д. дозволяє вирішувати питання захисту про нього шляхом захисту інформації про о. д. Як і демаскуючі ознаки о. д. поділяються за інформативністю на іменні, прямі і непрямі, за часом прояву — постійні, періодичні і епізодичні.

О. доступу /о. доступа/ [access o.] — пасивна сутність (запис, файл, блок пам'яті і т. ін.), що містить

або одержує інформацію. Доступ до о. д. здійснюється суб'єктами доступу за допомогою набору операцій, які надаються о. д.

О. застосування інформаційної зброї /о. применения информационного оружия/ — комп'ютерні й зв'язкові системи, що використовуються державними організаціями при виконанні функцій керівництва; воєнна інфраструктура інформаційна, що вирішує завдання управління військами і бойовими засобами, збором і обробленням інформації в інтересах збройних сил; інформаційні і керуючі структури банків, транспортних і промислових підприємств; засоби масової інформації, в першу чергу електронні (радіо, телебачення і т. ін.).

О. захисту інформації /о. защиты информации/ — система оброблення даних, що містить інформацію, яку належить захищати.

О. інформаційної безпеки /о. информационной безопасности/ — свідомість, психіка людей; системи інформаційні різного масштабу і різного призначення.

О. інформаційної безпеки соціальні /о. информационной безопасности социальные/ — особистість, колектив, суспільство, держава, світове товариство.

О. категорійований /о. категорированный/ [classified o.] — об'єкт, в якому обговорюється, формується, пересилається, приймається, перетворюється, накопичується, обробляється, відображається і зберігається інформація з обмеженим доступом.

О. керування /о. управления/ [control o.] — 1) Система, в якій відбуваються процеси, що підлягають керуванню. Як о. к. можуть виступати не тільки фізичні (технічні) системи, але і біологічні, екологічні, економічні, організаційні, інформаційні і т.ін. 2) Пасивний діяч інформаційний.

О. комп'ютерної системи /о. компьютерной системы/ [product o., system o.] — елемент ресурсу системи комп'ютерної, що знаходиться під керуванням комплексу засобів захисту і характеризується певними атрибутами й положенням. При розгляді взаємодії двох о. к. с., що виступають як приймачі або джерела інформації, виділяють об'єкт пасивний, над яким виконується операція, і активний об'єкт, який виконує

або ініціює цю операцію. Розглядаються такі типи о. к. с.: об'єкти-користувачі, об'єкти-процеси і пасивні об'єкти. Поняттю "суб'єкт" часто відповідає суперпозиція об'єкта-користувача й об'єкта-процесу. Об'єкти-користувачі і об'єкти-процеси є такими тільки всередині конкретного домену. В інших доменах об'єкти залишаються в пасивному стані. Це дозволяє одному об'єкту-процесу керувати іншим об'єктом-процесом або навіть об'єктом-користувачем, оскільки останній залишається "пасивним" з точки зору керуючого об'єкта. Пасивний об'єкт переходить в стан об'єкта-користувача, коли індивід (фізична особа) "входить" в систему. Цей об'єкт-користувач виступає для комплексу засобів захисту як образ фізичного користувача. За цим процесом іде активізація об'єкта-процесу за ініціативою користувача. Цей об'єкт-процес є керуючим для пасивних об'єктів усередині домену користувача. Взаємодія двох о. к. с. (звернення активного об'єкта до пасивного з метою одержання певного виду доступу) приводить до появи потоку інформації між об'єктами і (або) зміни стану системи.

О. пасивний /о. пассивный/ [passive o.] — об'єкт комп'ютерної системи, над яким виконується дія і (або) який служить джерелом чи приймальником інформації.

О. поділюваний /о. разделяемый/ [shared o.] — об'єкт комп'ютерної системи, який одночасно або почергово використовується різними користувачами і (або) процесами.

О. правових відносин в інформаційній сфері /о. правовых отношений в информационной сфере/ — інформація документована, ресурси інформаційні, інформаційна продукція, послуги інформаційні, системи інформаційні і їхні мережі, технології інформаційні і засоби їхнього забезпечення.

О. прикриття /о. прикрытия/ – споруди і конструкції, що створюють ознаки фальшивого об'єкта для дезінформування противника. Фальшиві споруди можуть бути плоскими і об'ємними, функціональними і нефункціональними. Об'ємні і функціональні споруди повинні відтворювати повний набір демаскуючих ознак о. п. протягом усього періоду захисту.

О. психологічних операцій /о. психологических операций/ — об'єкти психологічної війни у вузькому розумінні цього поняття. Це конкретні люди: особовий склад цих чи інших військових підрозділів против-

ника; персонал органів управління й забезпечення; службовці об'єктів соціально-економічної інфраструктури (залізничних, дорожніх, авіаційних, портових вузлів і споруд); напевно, визначені категорії населення (наприклад, національні, релігійні та інші меншини). В залежності від характеру воєнної, політичної, економічної ситуації о. п. о. можуть мінятися й уточнюватися. Так, в оборонній операції ними можуть бути: частини (підрозділи) першого ешелону військ, що ведуть наступ; особовий склад підрозділів, оточених в результаті проведення контратак; особовий склад тактичних десантів, що діють в смузі оборони з'єднання.

О. психологічної війни /о. психологической войны/ — особовий склад і все цивільне населення противника, а також союзних йому держав.

О. розвідки /о. разведки/ — особа, організація, об'єкт, місцевість або держава, проти яких проводиться операція розвідувальна.

О.-користувач /о.-пользователь/ [user o.] — подання фізичного користувача в системі комп'ютерній, що створюється в процесі входження користувача в систему і повністю характеризується своїм контекстом (псевдонімом, ідентифікаційним кодом, повноваженнями і т. ін.).

О.-процес /о.-процесс/ [process o.] — програма, що виконується у даний момент часу, яка повністю характеризується своїм контекстом (поточним станом регістрів обчислювальної системи, адресним простором, повноваженнями і т. ін.).

ОБ'ЄКТИВ /объектив/ [objective, object glass, (objective) lens] (від лат. objectivus — предметний) — сукупність лінз чи дзеркал або разом лінз і дзеркал для створення зображення предмета. Об'єктиви знаходять широке застосування в засобах спостереження в оптичному діапазоні. Описуються сукупністю параметрів, необхідних для оцінки засобів спостереження: фокусною відстанню (див. фокус, об'єктив короткофокусний, об'єктив середньофокусний, об'єктив довгофокусний, об'єктив панкратичний), кутом поля зору і зображення (див. об'єктив вузькокутовий, об'єктив середньокутовий, об'єктив ширококутовий, об'єктив із змінним кутом зображення), світлосилою (див. об'єктив надсвітлосильний, об'єктив світлосильний, об'єктив малосвітлосильний), здатністю роздільною, характеристикою частотно-контрастною. Для добування інформації

застосовуються об'єктиви трьох видів: для аерофотозйомки, широкого застосування (фото-, кіно-, відеозйомки і т. ін. з використанням побутових і професійних апаратів) і для прихованого спостереження (зйомки) (телеоб'єктиви, об'єктиви точкові).

О. вузькокутовий /о. узкоугольный/ [narrow-angle o.] — об'єктив, у якого величина кута поля зору не перевищує 30°.

О. довгофокусний /о. длиннофокусный/ [long–(distance/focus) o.] — об'єктив, у якого фокусна відстань є більшою за діагональ кадру поля зображення. Має вузький кут зору. О. д. використовуються для розпізнавання об'єктів спостереження.

О. із змінний кутом поля зору /о. с изменяющимся углом поля зрения/ — об'єктив, у якого реалізована зміна фокусної відстані. Чим більша фокусна відстань об'єктива, тим більше деталей об'єкта можна розглянути на його зображенні, але при цьому менший кут поля зору. Розміри об'єкта h на зображенні визначаються зі співвідношення h = fH/L у залежності від розмірів реального об'єкта H, відстані від нього до об'єктива L і фокусної відстані об'єктива h.

О. із змінною фокусною відстанню /о. с переменным фокусным расстоянием/ [variable focus/zoom(ing) /varifocal l.] — див. об'єктив панкратичний.

О. короткофокусний /о. короткофокусный/ [short-focus o.] — об'єктив, у якого фокусна відстань є меншою за діагональ кадру поля зображення. Має широкий кут зору. О. к. використовуються для виявлення об'єктів спостереження.

О. малосвітлосильний /о. малосветосильный/ — об'єктив, у якого величина геометричного відносного отвору 1:k=1:2 і менше.

О. надсвітлосильний /о. сверхсветосильный/ — об'єктив, у якого величина геометричного відносного отвору 1:k=1:5,6 і більше.

О. панкратичний /о. панкратический/ [pancratic o.] (від грец. $\pi\tilde{\alpha}\nu$ — що у складних словах означає все, всеохоплюючий та $\kappa\rho\acute{\alpha}\tau\o\varsigma$ — сила) — складна оптична система, в якій передбачена можливість

зміщення оптичних компонент, за рахунок чого досягається зміна величини фокусної відстані. Величину фокусної відстані змінюють дискретно або плавно. Дискретна зміна фокусної відстані досягається застосуванням афокальних насадок, що зменшують або збільшують фокусну відстань. Плавна зміна фокусної відстані здійснюється переміщенням окремих компонент уздовж оптичної осі за лінійним або нелінійним законом. В залежності від способу корекції аберацій (нерівномірної різкості на усьому полі зображення або наявності кольорових окантовок) п. о. поділяють на варіооб'єктиви і трансфокатори.

О. світлосильний /о. светосильный/ [high-power o., rapid/fast l.] — об'єктив, у якого величина геометричного відносного отвору 1:k знаходиться в межах 1:2,8 — 1:4. Див. також світлосила.

О. середньокутовий /о. среднеугольный/ — об'єктив, у якого величина кута поля зору знаходиться у межах 30° — 60°.

О. середньофокусний /о. среднефокусный/ — об'єктив, у якого фокусна відстань є приблизно рівною діагоналі кадру поля зображення.

О. точковий /о. точечный/ — об'єктив, що має дуже малі габарити і фокусну відстань та великий кут поля зору. Призначений для потайного спостереження (зйомки) через щілини і отвори з портфеля, годинника, запальнички тощо.

О. ширококутній /о. широкоугольный/ [wide-angle o.] — об'єктив, у якого величина кута поля зору перевищує 60°.

ОБЛІК /учет/ [calculation] — засвідчення, встановлення наявності, з'ясування кількості чого-небудь; обрахунок, обчислення.

О. інформаційних ресурсів /у. информационных ресурсов/ — процес, який разом із реєстрацією інформаційних ресурсів забезпечує реалізацію функцій контролю за станом ресурсів інформаційних та компонентів системи захисту інформації у системі обчислювальній.

ОБМЕЖЕННЯ /ограничение/ [limitation, restriction, constraint] — встановлення певної межі чого-небудь;

зв'язування чогось обмежувальними умовами.

О. доступу /о. доступа/ [access l.] — сукупність заходів, призначених для створення деякої фізичної замкнутої перепони навколо об'єкта захисту з організацією контрольованого доступу осіб, зв'язаних з об'єктом захисту своїми функціональними обов'язками. О. д. до комплексів технічних засобів оброблення інформації здійснюється на основі наступних заходів із застосуванням засобів обмеження доступу: виділення спеціальної території для розташування комплексів технічних засобів оброблення інформації; спорудження по периметру зони спеціальної огорожі із сигналізацією; спорудження спеціальних будівель або інших споруд; виділення спеціальних приміщень у будівлі; створення контрольно-пропускного режиму на території, будівлі і приміщення.

О. доступу до інформації /о. доступа к информации/ — сукупність методів, засобів та заходів, що забезпечують захист даних від доступу несанкціонованого.

О. прав осіб у зв'язку з допуском до державної таємниці /о. прав лиц в связи с допуском к государственной тайне/ — тимчасове обмеження в правах осіб або громадян, допущених або таких, що раніше допускалися, до таємниці державної. Обмеження можуть стосуватися: права виїзду за кордон на термін, зумовлений в трудовому договорі (контракті) при оформленні допуску громадянина до державної таємниці; права на розповсюдження відомостей, що складають державну таємницю, і на використання відкриттів і винаходів, що містять такі відомості; права на недоторканість приватного життя при проведенні перевірочних заходів на період оформлення допуску до державної таємниці.

О. цілісності /о. целостности/ [integrity c.] — правило, що визначає логічні обмеження, які накладаються на дані і використовуються системою керування базами даних для підтримання цілісності даних.

ОБМІН /обмен/ [exchange] — 1) Дія за значенням обмінювати і обмінюватися. 2) Передавання даних між джерелом і приймачем.

О. даними /о. данными/ [data e.] — процедура приймання і передавання даних, включаючи кодування,

декодування, буферизацію і перевірку.

О. шпигунами /о. шпионами/ — передача захопленого і засудженого агента або співробітника ворожої спеціальної служби в руки противника в обмін за свого захопленого агента або розвідника.

ОБРАЗ /образ/ [image] — результат та ідеальна форма відображення предметів і явищ матеріального світу у свідомості людини. О. на чуттєвому ступені пізнання — відчуття, сприйняття, уявлення; на рівні мислення — поняття, судження, умовиводи. Матеріальною основою втілення о. виступають практичні дії, мова, різноманітні знакові моделі. За змістом о. об'єктивний в тій мірі, в якій він адекватно відображає об'єкт.

ОБРОБЛЕННЯ /обработка/ [processing, handling, treatment, working] — піддавання змінам, аналізу, доведення до стану готовності чого-небудь.

О. даних /о. данных/ [data p.] — 1) Широкий спектр операцій і процедур, що використовуються у процесі аналізу первинної інформації і одержання висновків у вигляді гіпотез чи стверджень теоретичного або прикладного характеру. 2) Виконання операцій над даними, здійснюване за допомогою технічних і програмних засобів. Під операціями над даними розуміють такі дії як збирання, введення, записування, перетворення даних за певними правилами, зчитування, виведення, збереження, знищення, реєстрація, а також обмін по каналах передавання даних.

О. даних автоматичне /о. данных автоматическая/ [automatic data p.] — виконання комплексу операцій над даними за допомогою ЕОМ із метою перетворення маси відомостей і фактів в відомості, що мають цінність із певної точки зору.

О. зображень /о. изображений/ [image p.] — перетворення зображень із допомогою спеціальних апаратурних комплексів, до складу яких входить ЕОМ, із метою поліпшення сприйняття цих зображень людиною.

О. інформації /о. информации/ [information p., information h.] — сукупність різноманітних дій, здійснюваних над зібраною інформацією або інформацією, що надходить, які призводять до цієї чи іншої зміни

вигляду або характеру подання інформації. Наприклад, статистичне оброблення і т. ін. На відміну від перетворення, при якому вихідна інформація (текст, документ і т. ін.) зберігає своє самостійне значення, при обробленні вихідна інформація практично втрачає своє значення.

О. інформації безпаперове /о. информации безбумажная/ — спосіб роботи з документами, при якому оригінали документів виникають і зберігаються в пам'яті ЕОМ, а їхній зовнішній вигляд відтворюється у вигляді зображення на екрані дисплея. Документ може передаватися засобами пошти електронної, а в паперовій формі існує лише у вигляді копії. Безпаперове діловодство потребує особливих юридичних, правових і технічних процедур для скріплення безпаперового документа аналогом підпису відповідальної особи.

О. інформації в реальному масштабі часу /о. информации в реальном масштабе времени/ [real-time p.] — організація роботи системи обчислювальної (системи реального часу), при якій обчислення виконуються у темпі, що забезпечує обслуговування деякого зовнішнього процесу, який не залежить від ЕОМ.

ОБСЛУГОВУВАННЯ /обслуживание/ [service] — робота над задоволенням чиїх-небудь поточних або постійних потреб.

О. інформаційне /о. информационное/ [information s.] — галузь професійної діяльності інформаційної, спрямованої на задоволення різноманітних інформаційних потреб. О. і. включає операції збирання, аналітико-синтетичного перероблення, зберігання, пошуку і розповсюдження інформації, що виконуються інформаційними працівниками (інформаторами, бібліотекарями, бібліографами, перекладачами, видавницькими робітниками) з метою підвищення ефективності творчої діяльності фахівців народного господарства.

О. інформаційне вибіркове /о. информационное выборочное/ [selective information s.] — розповсюдження інформації, при якому враховуються індивідуальні особливості та потреби осіб чи організацій, для яких ця інформація призначена.

ОБСТАНОВКА /обстановка/ [situation, conditions, endovironment] — положення, обставини, умови існу-

вання кого- чого-небудь.

О. сигнальна /о. сигнальная/ [signal e.] — структура щільності випромінювання зумовлена наявністю джерел радіосигналів, побічного і ненавмисного випромінювання, рухом (маневруванням) цих випромінювачів, а також, можливо, застосуванням активних радіозавад.

ОДИНОЧКА /одиночка/ [lone person] — операція розвідувальна, що проводиться одним співробітником або агентом розвідки. Це може бути збирання інформації, робота з агентурою, кур'єрська місія і т. ін.

ОЗНАЙОМЛЕННЯ /ознакомление/ [disclosure] — одержання користувачем або процесом інформації, що міститься в об'єкті.

ОЗНАКА /признак/ [sign, indication] — 1) Показник, прикмета, знак, за якими можна упізнати, визначити будь-що. 2) В системах обчислювальних (search word) — значення, що задаються при пошуку даних.

О. властивостей речовини /п. свойств веществ/ — ознаки речовини, що описують її механічні, хімічні, акустичні, теплові, променисті, електричні, магнітні, ядерні властивості. Механічні властивості речовин характеризують їхню міцність на стискування і розтягування, твердість, пористість, пластичність, змочуваність, непроникливість і т.ін. Хімічні властивості речовини визначаються за результатами взаємодії її з іншими речовинами. Акустичні властивості визначають швидкість передавання і поглинання звуку у речовині. Теплові властивості оцінюються за температурою фазових переходів з одного стану в інший, теплопровідністю, теплоємністю і т.ін. Променисті (оптичні, рентгенівські і т. ін.) властивості речовини описуються коефіцієнтами і спектральними характеристиками пропускання, відбивання, переломлення, можливостями дифракції, поляризації та інтерференції променів світла в інфрачервоному, видимому і ультрафіолетовому діапазонах, а також гамма-випромінювань. Електропровідність, величини термо-електрорушійної сили, окислювально-відновні потенціали, потенціали іонізації, діелектрична і магнітна проникність і т.ін. характеризують електричні і магнітні властивості речовини. Ядерні властивості речовини оцінюються за масою ізотопів, масою і періодом напіврозпаду радіоактивних часток і т. ін.

О. діяльності об'єкта /п. деятельности объектов/ — ознаки, що характеризують етапи і режими

функціонування об'єкта, наприклад, етапи створення нової продукції: наукові дослідження, підготовка до виробництва, виготовлення нової продукції, її випробування і т. ін.

О. епізодична /п. эпизодический/ — ознака, що проявляється при певних умовах.

О. іменна /п. именной/ — ознака, що належить тільки одному конкретному об'єктові.

О. інформаційного суспільства /п. информационного общества/ — найбільш характерні ознаки, за якими будь-яке суспільство можна визначити як інформаційне: комп'ютер персональний, приєднаний до мереж інформаційних транскордонних, стає засобом повсякденного використання; виникають нові форми і види діяльності в інформаційних мережах: робота і торгівля в мережах, відпочинок в мережах, творчість і розваги в мережах, виховання і освіта в мережах, медицина в мережах і т. ін.; кожний член суспільства має можливість своєчасно і оперативно одержувати за допомогою транскордонних інформаційних мереж повну і достовірну інформацію будь-якого виду і призначення з будь-якої держави, знаходячись при цьому практично в будь-якій точці географічного простору; надається унікальна можливість оперативної, практично миттєвої, комунікації кожного члена суспільства як з кожним (і кожного із усіма разом), так і певних груп населення з державними і суспільними структурами поза залежністю від місця проживання на Земній кулі; трансформується діяльність засобів масової інформації за формами створення і розповсюдження інформації, розвивається та інтегрується з інформаційними мережами цифрове телебачення; формується нове середовище — мультимедіа, в якому поряд із "комп'ютерною" розповсюджується також інформація з традиційних ЗМІ; зникають географічні і геополітичні кордони держави в межах інформаційних мереж.

О. непряма /п. косвенный/ — ознака, що не належить безпосередньо об'єктові, але відображає властивості і стан об'єкта. Такі ознаки є результатом взаємодії об'єкта з навколишнім середовищем.

О. об'єкта /п. объекта/ — ознаки, властиві конкретному об'єктові, які дозволяють виявляти цей об'єкт серед інших схожих об'єктів та розпізнавати його належність, призначення, функції, властивості, особливості й характеристики. О. о. складають частину його ознак, а їхні значення відрізняються від значень відповідних ознак інших об'єктів. О. о. описують його різноманітні стани, характеристики й властивості.

У найбільш загальному випадку о. о. поділяють на розпізнавальні ознаки і ознаки діяльності об'єктів. О. о. поділяються на видові, ознаки сигналів та ознаки речовин. За інформативністю ознаки поділяються на іменні, прямі та непрямі. За часом прояву ознаки поділяються на постійні, періодичні та епізодичні.

О. об'єкта видові /п. объектов видовые/ — форма об'єкта, його розміри, деталі об'єкта, тон, колір і структура його поверхні і т.ін. О. о. в. описують зовнішній вигляд об'єкта. Вони об'єктивно йому властиві, але виявляються в результаті аналізу зовнішнього вигляду моделі об'єкта — зображення його на екрані оптичного приймача (сітківки ока людини, фотознімкові, екрані телевізійного приймача, приладу нічного бачення і т. д.). Так як модель в загальному випадку відрізняється від оригіналу, то склад і значення видових ознак залежить не тільки від об'єкта, але і від умов спостереження і характеристик оптичного приймача. У зв'язку з цим розрізняють ознаки об'єкта видові у діапазоні випромінювання оптичного (видимого та інфрачервоного) і діапазоні радіовипромінювання.

О. об'єкта демаскуючі /демаскирующие п. объекта/ — див. ознаки об'єкта.

О. об'єктів видові у діапазоні видимого оптичного випромінювання /п. объектов видовые в диапазоне видимого оптического излучения/ — ознаки видові, що добуваються при візуально-оптичному спостереженні у видимому діапазоні оптичного випромінювання. До них відносяться: фотометричні та геометричні характеристики об'єктів (форма, розміри об'єкта, колір, структура, малюнок і деталі його поверхні); тіні, дим, пил, сліди на ґрунті, снігу, воді; взаємне розташування елементів групового (складного) об'єкта; розташування об'єкта відносно інших відомих об'єктів.

О. об'єктів видові у діапазоні інфрачервоного випромінювання /п. объектов видовые в диапазоне инфракрасного излучения/ — ознаки видові, що добуваються за допомогою спеціальних приладів (нічного бачення, тепловізорів). До них належать: геометричні характеристики зовнішнього вигляду об'єкта (форма, розміри, деталі поверхні); температура поверхні.

О. об'єктів видові у діапазоні радіовипромінювання /п. объектов видовые в диапазоне радиоизлучения/ — ознаки видові, що добуваються за допомогою радіолокаційних станцій. До них належать:

ефективна площа розсіювання; геометричні характеристики (форма, розміри, яскравість, деталі); електропровідність поверхні.

О. об'єктів радіолокаційного спостереження /п. объектов радиолокационного наблюдения/ — див. ознаки видові об'єктів у діапазоні радіовипромінювання.

О. періодична /п. периодический/ — ознака, що проявляється через певні рівні проміжки часу.

О. підготовки до збройної боротьби в галузі психологічної війни /п. подготовки к вооруженной борьбе в области психологической войны/ — значне підсилення протиборства між імовірними противниками в сфері інформаційній; бойове розгортання органів психологічної боротьби; початок здійснення операцій психологічних.

О. розпізнавальні /п. опознавательные/ — ознаки, що описують об'єкт в статичному стані: його призначення, належність, параметри.

О. побудови речовини /п. строения вещества/ — ознаки речовини, що описують її побудову на макроскопічному, мікроскопічному і субмікроскопічному рівнях, на останньому — у вигляді кристалічної решітки, макромолекул, молекул, субатомних часток і атомів.

О. постійна /п. постоянный/ — ознака, що не змінюється протягом життєвого циклу об'єкта.

О. пряма /п. прямой/ — ознака, яка належить об'єктові, що розглядається.

О. речовин /п. веществ/ — ознаки, що визначають фізичний і хімічний склад, структуру і властивості речовин матеріального об'єкта. Демаскуючі о. р. містяться не тільки в кінцевому продукті, але і в тих вихідних та проміжних продуктах технологічного процесу одержання цієї речовини (див. речовина демаскуюча). Ознаки речовин можуть поділятися на ознаки складу речовини, ознаки побудови речовини та ознаки властивостей речовини.

О. сигналів / п. сигналов/ — ознаки, що описують параметри полів і сигналів, що генеруються об'єктом: їхні потужність, частота, вид (аналоговий, імпульсний), ширина спектра і т.ін. Зумовлені тим, що будь-яке матеріальне тіло з температурою, вищою абсолютного нуля випромінює електромагнітні поля,

створювані тепловим рухом електронів атомів речовини. Крім того, об'єкт може містити створені штучно джерела полів або електричного струму. У складі об'єкта можуть знаходитися радіоактивні речовини. Радіоелектронні засоби випромінюють функціональні та побічні електромагнітні поля, механічні рухи частин приладів і машин створюють акустичні поля.

О. складу речовини /п. состава вещества/ — ознаки речовини, що характеризують фізичний, хімічний, ізотопний та іонний (для плазми) склад речовини. За фізичним складом речовини можуть бути однорідними твердими (кусковими, порошковими), рідкими, газоподібними і неоднорідними, у вигляді розчинів, емульсій і т.ін. За хімічним складом речовини поділяються на органічні і неорганічні. У свою чергу, органічні речовини — на вуглеводневі, із умістом кисню та із умістом азоту, неорганічні — на оксиди, кислоти, основи і солі. Ізотопний склад характеризує стабільність або нестабільність ядер речовин або, іншими словами, наявність у речовини радіоізотопів. Іонний склад речовини визначається при знаходженні її в іонізованому стані (плазмі), який виникає внаслідок дії високої температури або газового розряду (для газоподібних речовин).

ОКУЛЯР /окуляр/ [eyepiece, ocular] (від лат. ocularius — очний) — система з однієї або кількох лінз для збільшення й розглядання зображення, що створюється об'єктивом оптичного приладу.

ОН-ЛАЙН /он-лайн/ [on-line] (з англ. букв. — на лінії) — назва оперативного інтерактивного режиму телекомп'ютерних зв'язків. Слово on-line входить до складу різноманітних термінів, що позначають, наприклад, базу даних з їхнім безперервним обновленням (on-line database), службу надання поточної інформації (on-line service), спеціалізований вузол інформаційних ресурсів і Інтернеті — "мережний офіс " (on-line office).

ОПЕРАЦІЯ /операция/ [operation] (від лат. operatio — дія) — ряд дій, заходів, пов'язаних з досягнення певної мети.

О. інформаційна /о. информационная/ [information o.] — сукупність узгоджених за метою, завданнями, місцем і часом дій (акцій), ударів, і битв, що проводяться за єдиним замислом і планом для вирішення

завдань боротьби інформаційної (завоювання і утримання переваги інформаційної над противником або зниження його інформаційної переваги) на театрі воєнних дій, стратегічному або оперативному напрямах. О. і. можуть бути наступальними і оборонними. Мета о. і. досягається вирішенням наступних завдань: інформаційним впливом на противника, захистом інформаційним і ефективним використанням ресурсів інформаційних власного угруповання військ (сил). О. і., звичайно, проводиться в межах відповідної загальновійськової, самостійної, спільної або спеціальної операції. О. і. можна класифікувати за масштабами як стратегічні, оперативно-стратегічні, оперативні і оперативно-тактичні і характеризувати наступними основними показниками: просторовим розмахом, тривалістю, а також кількісним і якісним складом сил і засобів.

О. інформаційна наступальна /о. информационная наступательная/ — операція інформаційна, що має за мету завоювання переваги інформаційної над противником. В цій операції головні зусилля спрямовуються на дезорганізацію його систем управління військами і зброєю, а частина сил та засобів забезпечують стійкість власного управління. При цьому всі заходи, що проводяться в межах боротьби інформаційної, повинні забезпечувати сприятливі умови для бойових дій своїх військ (сил).

О. інформаційна оборонна /о. информационная оборонительная/ — операція інформаційна, що проводиться в умовах великої переваги інформаційної противника і має за мету зниження цієї переваги. В такій операції головні зусилля сил і засобів спрямовуються на забезпечення інформаційної безпеки органів управління об'єднань і з'єднань, на захист інформації в системах керування. Частина сил і засобів спрямовуються на дезорганізацію управління військами і зброєю противника.

О. інформаційної війни /информационной войны/ [information war о.] — операції, що проводяться спеціально для впливу на потоки інформаційні противника і досягнення переваги інформаційної над противником. Результат бойових операцій залежить від о. і. в. Війна інформаційна впливає на бойове планування, розгортання збройних сил, припинення бойових дій і перегрупування військових частин. Деякі о. і. в. можуть виходити за межі безпосередніх бойових дій. Це відноситься, наприклад, до формування громад-

ської думки. У проведенні о. і. в. важливу роль відіграє розвідка. Вона не обмежується тільки науковими і технічними аспектами при добуванні і аналізі даних розвідувальних. В багатьох випадках такі дані повинні включати відомості біографічного характеру про державних керівників і командування противника, соціологічні, культурні і економічні фактори, особливо коли війська входять в безпосередній контакт з місцевим населенням в районах їхнього знаходження.

О. психологічна /о. психологическая/ — сукупність узгоджених, скоординованих і взаємозв'язаних за метою, завданнями, місцем і часом, об'єктами і процедурами видів, форм, способів та прийомів психологічного впливу; головний елемент змісту війни психологічної. П. о. складаються з політичних, воєнних, економічних, дипломатичних і власне інформаційно-психологічних заходів, спрямованих на конкретні групи населення й військ противника з метою впровадження їм чужих ідеологічних і соціальних установок, формування хибних стереотипів поведінки, трансформації в необхідному напрямкові їхніх настроїв, почуттів, волі, спонукання їх до відмови від бойових дій, зрадництва, здавання у полон або дезертирства. При правильному плануванні о. п. передують застосуванню воєнної сили, а потім супроводжують або доповнюють повторне її використання. О. п. бувають різних видів, які у свою чергу класифікують за тривалістю (стратегічні , оперативні, тактичні), за умовами та часом здійснення (о. п. мирного часу та загрозливого періоду, о. п. воєнного часу, о. п. в миротворчій діяльності), за спрямованістю (о. п. проти цивільного населення, о. п. проти військ противника, о. п. проти командування противника, о. п. для введення противника в оману, о. п. для сприяння опозиційним силам і дисидентським рухам, о. п. для здійснення культурної експансії й диверсій, консолідуючі о. п.).

О. радіоелектронної боротьби /о. радиоэлектронной борьбы/ — комплекс заходів і дій з радіоелектронного придушення і захисту своїх військ (сил) і систем зброї від радіоелектронного придушення. Складовими частинами операції РЕБ будуть: радіоелектронні удари з метою придушення всієї системи радіоелектронних засобів противника; радіоелектронна оборона (захист) об'єктів і засобів; заходи забезпе-

чення операції РЕБ.

О. розвідувальна /о. разведывательная/ [intelligence o.] — сукупність дій, заходів, що проводяться органами розвідки для добування, оброблення і подання керівництву інформації, необхідної для прийняття рішень.

О. спеціальні /о. специальные/ [special o.] — термін для позначення підривних і диверсійних операцій.

О. таємна /о. тайная/ [secret o.] — сукупність заходів, що проводяться розвідувальною організацією в скритій або замаскованій формі, головним чином, із тим, щоб утрудняти (або зробити неможливим) процес доказу причетності до них їхніх організаторів.

О. тайникова /о. тайниковая/ [hiding-place o.] — дії, спрямовані на закладення матеріалу в таємне місце (тайник) із тим, щоб його міг вилучити агент шпигунської організації. Зв'язок через тайник є однією з форм безособового зв'язку.

ОПИТУВАННЯ /опрос/ [polling, inquiry, questioning] — метод збирання первинної інформації шляхом звернення із запитаннями до певної групи людей. З допомогою о. отримують як фактичну інформацію (інформацію про події), так і відомості про погляди, оцінки і особисті думки опитуваних.

ОПІРНІСТЬ /сопротивляемость/ — властивість чого-небудь протистояти певним впливам, змінам, а також сила, ступінь такого протистояння.

О. групова /с. групповая/ — опірність навіюванню з боку групи як цілого. Цей різновид опірності навіюванню залежить від якісного складу групи: ступеню її згуртованості, єдності мети й мотивів діяльності та інших факторів. Чим менше розвинені міжгрупові зв'язки й відносини, тим слабкіша о. г. Встановлено також, що загальна опірність групи завжди нижча опірності окремих, найбільш стійких її членів.

О. загальна /с. общая/ — опірність навіюванню, яка зумовлена критичністю людей до спроб будь-що навіяти їм. В цілому, вона широка за спектром дії, але слабка за силою (хоча є суттєві відмінності між людьми за цими параметрами).

О. індивідуальна /с. индивидуальная/ — протидія навіюванню зі сторони однієї людини. Встанов-

лена залежність цього різновиду опірності навіюванню від індивідуальних і вікових особливостей психіки (стійкості поглядів і переконань, багатства життєвого досвіду, загальної критичності, співвідношення між раціональними й емоційними сторонами психіки і т. ін.).

О. навіюванню /с. внушению/ — властивість об'єкта протистояти навіюючому впливу (див. навіювання) суб'єкта (контрсугестія). Здатність до о. н. залежить від особливостей інтелектуальної і емоційно-вольової сфери особистості. О. н. поділяють на навмисну і ненавмисну, індивідуальну і групову, загальну і спеціальну. О. н. мінлива. Один і той же об'єкт виявляє різну ступінь о. н. по відношенню до різних суб'єктів і різного змісту інформації, що навіюється. О. н. також характеризується динамізмом. Величина реальної о. н. постійно коливається як у сторону зниження, так і в сторону підвищення. При зростанні вона може привести до такої величини, коли будь-який навіюючий вплив даремний. Так високу о. н. має солдат в атаці. В цей час будь-що йому навіювати не має ні найменшого сенсу.

О. навмисна /с. намеренная/ — опірність навіюванню, що діє на усвідомлюваному рівні психіки: об'єкт впливу свідомо аналізує те, що йому пробують навіяти, зіставляє навіювання зі своїми знаннями, поглядами, переконаннями і т. ін.

О. ненавмисна /с. ненамеренная/ — властива багатьом людям схильність в усьому сумніватися, недовірливість та інші прояви загальної критичності.

О. спеціальна /с. специальная/ — опірність навіюванню, що має більш вузьку сферу дії, аж до відношення до конкретної людини або до конкретної інформації. Наприклад, людина, вихована на певних принципах, не буде сприймати інформацію, що суперечить їм.

ОРГАН /орган/ [agency, bodies] (від грец. *ὀργανøν* — знаряддя, інструмент) — установи, організації, що виконують певні функції.

О. влади /о. власти/ [government b.] — державні і суспільні заклади і організації, що функціонують в даній системі влади. Розрізняють органи державного управління, органи місцевого самоуправління, вищі органи влади, органи законодавчої, виконавчої, судової влади, органи політичного, воєнного, господарського

керівництва і т. ін.

О. державної розвідки /о. государственной разведки/ — органи розвідки, створені державою для забезпечення керівництва країни інформацією, необхідною для прийняття ним політичних, економічних, воєнних, науково-технічних рішень в умовах жорсткої міждержавної конкуренції. Структура органів державної розвідки залежить від цілей держави, її зовнішньої політики та можливостей.

О. добування інформації /о. добывания информации/ — спеціалізовані органи, призначені для добування інформації. Найчастіше є складовою частиною органів розвідки.

О. захисту державної таємниці /о. защиты государственной тайны/ — органи державної влади, підприємства, заклади і організації та їхні структурні підрозділи, які взяли на себе зобов'язання або зобов'язані відповідно до свого статусу виконувати вимоги законодавства держави про державну таємницю.

О. інформаційний /о. информационный/ [information a., information department] — установа або підрозділ, який постійно здійснює роботу інформаційну.

О. інформаційної війни /о. информационной войны/ — органи керування інформаційною війною і люди (фахівці, офіцери, підрозділи) для її ведення. До о. і. в. можуть відноситись: органи планування і координації з питань інформаційної війни, які здійснюють розроблення системи планування діяльності з усіх питань, що зв'язані з інформаційною війною; органи стратегічного рівня з відслідковування ознак початку інформаційної війни, які займаються збиранням і аналізом інформації розвідувальної, визначенням ознак початку атак інформаційних; органи проведення операцій із захисту від зброї інформаційної, що здійснюють попередження про інформаційні атаки тактичного рівня і займаються ліквідацією наслідків нападу інформаційного; підрозділи розроблення конструкцій і архітектури автоматизованих систем керування (АСК), що здійснюють розроблення єдиної архітектури і технічних стандартів в галузі засобів і систем захисту від інформаційної зброї; групи незалежних експертів, що здійснюють аналіз уразливості АСК, у тому числі, через здійснення експериментальних атак на АСК та їхні окремі елементи.

О. керування /о. управления/ — 1) Орган, призначений для спрямовування діяльності кого-, чого-

небудь. 2) Складова частина, деталь різних механізмів, пристроїв і т. ін., що виконує певну керуючу функцію. 3) Активний діяч інформаційний.

О. комерційної розвідки /о. коммерческой разведки/ — органи розвідки, створені комерційною структурою для забезпечення її інформацією, необхідною для успішної діяльності на ринку в умовах гострої конкурентної боротьби. О. к. р. входять до складу служби безпеки комерційної структури.

О. контррозвідки /о. контрразведки/ — див. контррозвідка.

О. психологічної війни /о. психологической войны/ — орган керування війною психологічною і люди (фахівці, офіцери, військові підрозділи) для її ведення. О. п. в. повинен бути здатним до швидкого розгортання, оперативного слідкування за обстановкою в різноманітних регіонах, спроможним до виконання поставлених завдань в будь-яких умовах. На озброєнні о. п. в. знаходяться різноманітні види засобів психологічної війни технічних.

О. розвідки /о. разведки/ — спеціалізовані органи, призначені для добування, оброблення і подання необхідної для прийняття рішень інформації будь-яким державним або комерційним структурам, до складу яких вони входять.

О. сертифікації /о. сертификации/ [Designated Approving Authority (DAA)] — організація, якій довірено рішення про допуск засобів захисту для забезпечення безпеки інформації в системі оброблення даних та яка в змозі нести відповідальність за забезпечення атестаційних затверджень.

О. технічного захисту інформації /о. технической защиты информации/ — спеціалізований підрозділ, призначений для забезпечення захисту інформації технічного в організації. Може входити до складу служби безпеки організації. Основні завдання органу: обслідування виділених будівель (приміщень) з метою встановлення потенційно можливих каналів витоку конфіденційної інформації через технічні засоби, конструкції будівель і обладнання; виявлення і оцінка ступеня небезпеки технічних каналів витоку інформації; розроблення заходів ліквідації (запобігання витоку) потенційних каналів витоку інформації; організація контролю (в тому числі і інструментального) за ефективністю прийняти захисних заходів, аналіз результа-

тів контролю і розроблення пропозицій з підвищення надійності і ефективності заходів захисту; підготовка заявок на придбання технічних засобів захисту, участь у встановленні засобів захисту, їхній експлуатації і контролі стану. Крім того, на о. т. з. і. доцільно покласти також технічні питання охорони носіїв інформації.

О. чуття /о. чувств/ [senses, organs of sense] — органи зору, слуху, гравітації, нюху, смаку, дотику, що складаються з чутливих нервових клітин і допоміжних структур. Сприймають і попередньо аналізують різноманітні подразнення, що одержуються організмом із зовнішнього і внутрішнього середовища; передають інформацію в центральну нервову систему. О. ч. сприяють найбільш досконалому пристосуванню організму до навколишнього світу.

ОРГАНІЗАЦІЯ /организация/ [organization] (франц. organisation) — 1) Створення, засновування чого-небудь, із залученням до цього процесу інших. 2) Об'єднання людей, суспільних груп, держав на базі спільності інтересів, мети, програми дій і т.ін. 3) Особливості будови чого-небудь, структура.

О. вивчення об'єктів психологічної війни /о. изучения объектов психологической войны/ — організація роботи органів психологічної війни, спрямованої на збирання й аналіз відомостей, що характеризують об'єкти психологічного впливу відповідно до процесу вивчення об'єктів психологічної війни. Див. також етапи вивчення об'єктів психологічної війни та документи органів психологічної війни інформаційні.

О. добування інформації /о. добывания информации/ — перший етап технології добування інформації, який передбачає реалізацію наступних заходів: структурування (декомпозицію) завдань, поставлених користувачами інформації; розроблення задуму заходів добування інформації; планування заходів; постановка завдань виконавцям заходів; нормативне і оперативне управління діями виконавців і режимами роботи технічних засобів. О. д. і. займаються підрозділи планування і управління органів розвідки.

О. з розподілу адрес в Інтернеті /о. по распределению адресов в Интернете/ [Internet Assigned Numbers Authority (IANA)] — організація, призначена для контролю розподілу в Інтернеті числових параметрів протоколу IP, гарантуючи, що кожний домен одержує унікальне значення. Крім IP-адресів, IANA є центральним реєстром для інших чисел і даних, що мають відношення до Інтернету.

ОРГАНІЗМ /организм/ [organism] (франц. organisme) — 1) Будь-яка жива істота. 2) Сукупність фізичних і духовних властивостей людини. 3) Складна організована єдність.

О. інформаційний /о. информационный/ [information o.] — відносно короткий набір команд (до 30 команд), що використовується при створенні вірусів комп'ютерних. О. і. передається керування комп'ютером, в результаті чого здійснюється захоплення інформаційно-обчислювальних ресурсів системи керування автоматизованої (оперативної пам'яті, простору на магнітних носіях інформації, процесорного часу).

ОСЕРЕДОК /ячейка/ [cell] — 1) Первинний підрозділ, найменша одиниця в складі будь-якого об'єднання або організації. 2) Найнижча ланка в структурі будь-якої групи агентурної (мережі).

ОСНОВИ /основы/ [base, basic, ground, foundation, fundament, law, principle] — найважливіші вихідні положення чого-небудь (науки, теорії і т. ін.).

О. теорії інформаційної боротьби загальні /о. теории информационной борьбы общие/ — найважливіші спільні вихідні положення теорії інформаційної боротьби. В загальних основах визначаються: апарат понять інформаційної боротьби; напрямки і методи досліджень інформаційної боротьби; тенденції розвитку інформатизації і її роль в різноманітних галузях життя суспільства; роль і місце інформаційної боротьби у мирний і воєнний час; об'єкт, предмет, цілі, завдання і структура теорії інформаційної боротьби. Найважливішими логічними елементами змісту о. т. і. б. з. є категорії, закони, закономірності і принципи інформаційної боротьби.

ОСОБИСТІСТЬ /личность/ [personality] — 1) Людина як суб'єкт відносин і свідомої діяльності. 2) Відносно стійка система поведінки індивіда, побудована насамперед на основі введення в соціальний контекст. Стрижневим формуванням о. є самооцінка, яка будується на оцінках індивіда іншими людьми і його оцінюванні цих інших.

ОСОБЛИВОСТІ /особенности/ — характерна риса, ознака, властивість кого-, чого-небудь.

О. індивідуально-особистістні /о. индивидуально-личностные/ — характеристики різних категорій людей, специфіку яких необхідно враховувати, для досягнення максимального ефекту впливу психологічно-

го. Існує ряд класифікацій, що дозволяють відрізняти одні категорії людей від інших. Так за класифікацією Кречмера-Шелдона, що заснована на взаємозв'язку між статурою й характером, розглядають три основних групи людей: пікніки (ендоморфи), атлетіки (мезоморфи), астеніки (ектоморфи). За темпераментом люди поділяються на сангвініків, флегматиків, холериків, меланхоліків. За акцентуацією характеру (гіпертрофією окремих рис характеру порівняно з іншими рисами) налічується декілька десятків різновидів типів людей: демонстративний (істероїдальний) тип; застряваючий (параноїдальний) тип; збудливий тип; боязливий (сензитивний) тип; екзальтований тип; епілептоїдний тип і т.ін. Акцентуйовані особистості особливо уразливі по відношенню до одних впливів, що травмують психіку, в цей же час мають дуже високу стійкість до інших впливів.

О. морально-психологічного стану /о. морально-психологического состояния/ — характеристика об'єктів психологічної війни, що визначає особливості й ступінь морально-психологічної підготовки об'єктів психологічного впливу.

О. національно-психологічні /о. национально-психологические/ — форма прояву психології національної; одна з основних характеристик об'єктів психологічної війни, специфіку якої необхідно враховувати, для досягнення максимального ефекту впливу психологічного. Об'єкти психологічного впливу (військовослужбовці й населення противника) — це люди, які думають, відчувають, переживають, сприймають сказане у відповідності до закономірностей, притаманних даній етнічній спільності. Якщо способи психологічного впливу на війська й населення противника, зміст і форма подавання агітаційно-пропагандистських матеріалів не відповідають н.-п. о. об'єкта, то сам вплив може бути або даремним, або приведе до протилежного результату.

ОХОРОНА /охрана/ [guarding, protection, guard] — 1) Група (людей, кораблів, машин), що охороняють кого-що-небудь. 2) Термін, що означає слідкування за збереженням кого-, чого-небудь.

ОЦІНКА /оценка/ [estimate, estimation, assessment, evaluation] — 1) Думка (висновок) про цінність, рівень

або значення кого-чого-небудь. 2) Наближене значення певної величини.

О. безпеки інформації /о. безопасности информации/ [information security e.] — процес, метою кого є визначення відповідності стану безпеки інформації в системі комп'ютерній встановленим вимогам. Див. також аналіз кваліфікаційний та кваліфікування рівня безпеки.

О. вартості (цінності) інформації /о. стоимости (ценности) информации/ [value estimation of information] — дані, що визначають цінність інформації. Для одержання цих даних застосовують різноманітні підходи: квазіекономічний — за основу береться інформація як товар, що має свою ринкову ціну; прагматичний — цінність інформації визначається найвирішальнішою ситуацією; це означає, що інформація тим цінніша, чим швидше вона сприяє вирішенню проблеми; праксеологічний — цінність інформації визначається результативністю дій для досягнення наміченої мети; семантичний — цінність інформації визначається мірою, в якій вона служить для збагачення знань споживача.

О. величини загрози безпеці інформації /о. величины угрозы безопасности информации/ — для елемента інформації величина загрози може бути визначена у вигляді добутку потенційних збитків від реалізації загрози на ймовірність її реалізації. Так як одержати точні і об'єктивні кількісні значення величини загрози важко, то можлива наближена оцінка при наступних обмеженнях і умовах: максимальні збитки від викрадення інформації відповідають її ціні; в умовах повної невизначеності про наміри зловмисника щодо добування інформації помилка прогнозу мінімальна, якщо прийняти величину ймовірності реалізації загрози протягом певного періоду часу рівною 0,5. Якщо взяти середнє значення з усіх елементів інформації, то верхня межа загрози становить половину ціни інформації, що підлягає захисту. Очевидно, що з підвищенням ціни інформації стає більшою загроза її безпеці, а це потребує більше ресурсів для захисту цієї інформації.

О. вірогідності інформації /о. достоверности информации/ [correctness estimation of information] — дані, що враховують вірогідність джерела інформації, оцінка автора та методів, що використовуються в

роботі інформаційній.

О. достовірності повідомлення за схемою Канта /о. достоверности сообщения по схеме Канта/ — якісно-кількісний спосіб кількісної оцінки достовірності повідомлення. У відповідності з ним діапазон можливих імовірностей розбивається на 7 інтервалів і достовірність конкретної інформації оцінюється в шансах: достовірна інформації (ймовірність відсутності неправдивої інформації є близькою до 1); майже визначено, що інформація достовірна (9 шансів проти одного); є багато шансів, що інформація достовірна (3 шанси проти одного); шанси приблизно однакові (1 за, 1 проти); є багато шансів, що інформація недостовірна (3 шанси проти одного); майже визначено, що інформація недостовірна (за 9 шансів проти одного); недостовірна інформація (ймовірність неправдивої інформації є близькою до 1).

О. експертні /о. экспертные/ [expert evaluation] — дані, які одержує висококваліфікований фахівець в даній галузі — експерт при аналізі об'єкта і прогнозуванні його подальшого розвитку.

О. ефективності інформаційної боротьби /о. эффективности информационной борьбы/ — визначення ступеня відповідності результатів боротьби інформаційної її меті (цілі). Стосовно до боротьби збройної можна виділити два рівні о. е. і. б. — о. е. і. б. у війнах і збройних конфліктах в цілому і о. е. і. б. в операціях (бойових діях) та розділити її (на кожному рівні) на дві частини: загальну оцінку ефективності власне інформаційної боротьби (як самостійного виду боротьби) і спеціальну оцінку дій, в інтересах яких ведеться інформаційна боротьба. Методологія оцінки ефективності інформаційної боротьби відіграє важливу роль в розвитку теорії інформаційної боротьби.

О. інформаційна /о. информационная/ — документ, в якому аналізується існуюче на даний момент положення, або робиться прогноз про розвиток подій на майбутнє; будь-яке передбачення, яке міститься в інформаційному документі.

О. захисту /о. защиты/ [security e.] — визначення ступеня відповідності системи захисту встановленій моделі механізму захисту, стандарту забезпечення захисту і технічним умовам. О. з. може бути зроблена шляхом: спостереження за поведінкою системи при виконанні її функцій; спроб упровадитися до системи

з використанням методів зловмисника; аналізу подробиць побудови системи, особливо програмного забезпечення, який часто проводиться з використанням верифікації і атестації.

О. надійності джерела інформації /о. надежности источника информации/ — показник достовірності інформації, що характеризує відсутність в ній елементів дезінформації. В першому наближенні джерело інформації оцінюється за багаторівневою шкалою, наприклад: цілком надійне; звичайно надійне; доволі надійне; не завжди надійне; ненадійне; надійність не може бути визначена.

О. розбірливості мовної інформації (мови) /о. разборчивости речевой информации (речи)/ — відношення кількості прийнятих без спотворення одиниць мови (фраз, слів, букв, звуків) до загальної кількості переданих. Зниження вимог до розбірливості може знижувати надмірність письмової або усної мови.

О. уразливості /о. уязвимости/ [vulnerability a.] — дослідження об'єкта оцінки з метою визначення можливості реалізації загроз.

ОЧИЩЕННЯ /очистка/ [clearing] — звільнення будь-якого простору, поверхні чогось.

О. пам'яті /о. памяти/ [memory c.] — знищення даних у пам'яті шляхом установлення полів цих даних в заданий або випадковий стан.

П

ПАБЛІК РІЛЕЙШНЗ /паблик рилейшнз/ [Public Relations (PR)] (з англ. — зв'язок із громадськістю)— 1) Сприяння встановленню взаєморозуміння і доброзичливих відносин між особистістю, організацією та іншими людьми, групами людей або суспільством у цілому через розповсюдження роз'яснювального матеріалу, розвитку обміну інформацією та оцінки суспільної реакції. До п. р. відноситься спеціалізована діяльність промислових корпорацій, різноманітних закладів і торговельних об'єднань із створення за допомогою засобів масової інформації і рекламного бізнесу сприятливих вражень про ці організації й привернення до них уваги потенційних клієнтів і авторитетних представників впливових суспільних сил. З цією метою

ЗМІ забезпечуються відповідною інформацією. 2) Відділ інформації комерційного підприємства. 3) Служба зв'язку з громадськістю.

ПАВУТИНА /паутина/ [cobweb, spider's web, web] — легка сітка з тонких волокон, утворених із клейкої рідини, яку виділяють павуки та деякі інші членистоногі тварини, а також окрема нитка такої сітки; павутиння.

П. всесвітня /п. всемирная/ [World Wide Web (WWW)] — гіпертекстова інформаційно-пошукова система в Інтернеті. Блоки даних WWW (сторінки) розташовуються на окремих комп'ютерах, що називаються WWW-*серверами* і належать окремим організаціям або приватним особам. За допомогою гіпертекстових посилань, вбудованих у документи WWW, користувач може переходити від одного документа до іншого. В основі WWW лежить протокол передавання гіпертекстових повідомлень HTTP, а самі сторінки форматуються за допомогою спеціальної мови розмічування гіпертексту HTML.

ПАКЕТ /пакет/ [packet] — в протоколах TCP/IP — дані, що передаються між рівнями мережним і канальним. Також узагальнений термін для даних, що передаються в Інтернеті.

ПАМ'ЯТЬ /память/ [memory] — 1) Здатність до відтворення минулого досвіду, одна з основних властивостей людини, що виражається в здатності довго зберігати інформації про події зовнішнього світу, реакціях організму і багаторазово вводити її у сферу свідомості і поведінки. Виділяють процеси запам'ятовування, зберігання і відтворення, що включають узнавання і спомин, тобто пригадування. 2) Функціональна частина ЕОМ, призначена для приймання, зберігання і видавання даних. Розрізняють пам'ять внутрішню (основну, оперативну) і зовнішню.

П. віртуальна /п. виртуальная/ [virtual m.] — безперервний простір пам'яті, який надається окремому споживачеві безвідносно до реальних обсягів пам'яті основної. Забезпечується засобами пам'яті зовнішньої і обміну сторінками між зовнішньою і основною пам'яттю.

П. внутрішня (власна) /п. внутренняя (собственная)/ [internal (private) s.] — пам'ять, яка вбудована

в обчислювальний пристрій і безпосередньо керується цим пристроєм.

П. зовнішня /п. внешняя/ [external (backing) s.] — пристрій запам'ятовуючий на магнітних дисках, магнітних стрічках або дисках оптичних, призначений для довготривалого зберігання інформації.

П. людини /п. человека/ — сукупність процесів організації й зберігання минулого досвіду, що робить можливим його повторне використання в діяльності, в тому числі і в інтересах війни психологічної. Розрізняють наступні види пам'яті: моторну, емоційну, словесно-логічну. Всі вони зв'язані з процесами запам'ятовування, які, крім того, містять процеси мислення (у складній і суперечній єдності з мовою), прояву інтересів і потреб, емоцій і чуття.

П. оперативна (основна, головна) /п. оперативная (основная, главная)/ [main s.] — програмно адресна пам'ять, швидкодія якої сумірна з швидкодією центрального процесора, призначена для тимчасового зберігання програм і даних. Дані в п. о. доступні машинним командам для безпосередніх посилань за адресою або для оброблення.

П. основна /п. основная/ [main s.] — пам'ять оперативна в аспекті її основного призначення: зберігання виконуваних на даний момент програм і оперативно необхідних для цього даних.

П. постійна /п. постоянная/ [permanent s.] — частина пам'яті оперативної комп'ютера персонального, яка розташована в пристрої запам'ятовуючому постійному і містить програми базової системи вводу-виводу.

П. постійна програмована /п. постоянная программируемая/ — див. пристрій запам'ятовуючий постійний програмований (ППЗП).

ПАНІКА /паника/ [panic, scare] (від грец. *πανικόν* — несвідомий жах) — психологічний стан, який викликаний загрозливим впливом зовнішніх умов та виражений у почутті дошкульного страху, що охоплює людину або багатьох людей, нестримного неконтрольованого намагання уникнути небезпечної ситуації.

ПАРАПСИХОЛОГІЯ /парапсихология/ [parapsycology] (від грец. *παρα...* — префікса, що означає відступ, відхилення, зміну, і психологія) — позначення галузі досліджень, що ставить за мету вивчення форм сприйняття, що здійснюється без участі органів чуття, а також форм впливу живої істоти на фізичні яви-

ща поза організмом без зусилля м'язів (бажанням, думкою і т. ін.). П. використовується для пояснення психічних явищ, що не мають чіткого наукового обґрунтування: екстрасенсорного сприйняття, телепатії, телекінезу і т.ін. Інша назва п. — психотроніка.

ПАРОЛЬ /пароль/ [password] (від франц. parole — слово, промова) — ідентифікатор суб'єкта доступу (найчастіше рядок символів), що є його (суб'єкта) секретом і використовується в процедурі автентифікації.

П. головний /п. главный/ [master p.] — 1) Кореневе слово, що є спільним для певного набору паролів; 2) Пароль, призначений для захисту каталогу паролів.

ПАРОСТОК /побег/ [sprout] — в криптології — випадкова послідовність x, що подається на вхід генератора псевдовипадкового. Під "випадковістю" розуміється, що x є реалізацією випадкової величини X рівномірно розподіленої на множині $/0,1/^{\infty}$. Звичайно, паросток — це теоретичне поняття. За добре наближення до нього можна вважати послідовність x, отриману з фізичного генератора випадкової послідовності, який задовольняє певним вимогам. Інша назва зерно.

ПАСТКА /ловушка/ — хитрий маневр, прийом для заманювання противника в невигідне, небезпечне становище.

П. програмна /л. программная/ — закладка програмна, що використовує помилки або неоднозначність у програмному забезпеченні.

ПАТРОНАТ /патронат/ [patronage] (лат. patronatys від patronys — захисник) — заступництво, покровительство, опіка.

П. інформаційний /п. информационный/ [information p.] — форма забезпечення інформаційної безпеки фізичних і юридичних осіб із боку держави. П. і. припускає забезпечення органів управління системи інформаційної безпеки держави відомостями про фактори дестабілізуючі і загрози стану інформованості фізичних і юридичних осіб (забезпечення інформаційної безпеки інформаційне) і власне захист інтересів життєво важливих цих осіб від загроз інформаційних (захист інформаційний).

ПЕЛЕНГ /пеленг/ [bearing] (гол. peiling) — напрям від спостерігача до будь-якого об'єкта. П. визначають

кутом між площиною меридіана і вертикальною площиною, яка проходить через точку спостерігання та об'єкт. На основі двох або більше пеленгів із різних точок або за одним пеленгом і дальністю від пеленгатора до об'єкта розраховуються координати об'єкта.

ПЕЛЕНГАТОР /пеленгатор/ [direction finder] — технічний пристрій для визначення пеленга на об'єкт. Розрізняють такі п.: візуальні (із використанням оптичних приладів), акустичні, гідроакустичні, теплові, радіопеленгатори, які є елементами відповідно звукометричних, гідроакустичних, тепло- і радіопеленгаторних станцій.

ПЕЛЕНГАЦІЯ /пеленгация/ [location finding, position measurement] — прикладна галузь науки, що вивчає питання визначення напрямку (пеленга) на будь-які об'єкти (джерела). Термін п. застосовується також у значенні пеленгування, наприклад, радіопеленгація.

ПЕЛЕНГУВАННЯ /пеленгование/ [direction finding] — визначення пеленга на будь-який об'єкт (джерело). Можна виділити чотири види п., які знайшли практичне застосування: акустична (звукова) пеленгація; оптична (візуальна) пеленгація; теплова пеленгація; радіопеленгація.

ПЕРЕБІЖЧИК /перебежчик/ [deserter] — особа, що відрікається від своєї країни (і, як правило, покидає її), та яка може бути використаною іншою країною як джерело цінної інформації.

П. прихований /п. скрытый/ — перебіжчик, який таємно відрікся від своєї країни, але не виїхав за її межі. Звичайно, такі перебіжчики стають агентами-"кротами", залишившись на попередньому місці роботи, де вони мають доступ до секретної інформації і передають її іншій державі.

ПЕРЕВАГА /преимущество/ [advantage] — зверхність над ким-чим-небудь у якому-небудь відношенні.

П. інформаційна /п. информационное/ [information a.] — ситуація, при якій є можливість змінити уявлення противника про дійсну обстановку і позбавити його здатності прогнозувати подальші події та впливати на них. Основою здобуття і. п. є більш швидке одержання і використання оперативної інформації, ніж це може зробити противник.

ПЕРЕВАНТАЖЕННЯ /перенагрузка/ [overload] — забезпечення надмірною кількістю чого-небудь.

П. інформаційне /п. информационная/ [information o.] — надлишкова, кумулятивно зростаюча інформація, що поступає різними каналами засобів масової інформації і здатна чинити негативний вплив на стан здоров'я, психіки і менталітету людей.

П. комунікаційне /п. коммуникационная/ [communication o.] — фізичний стан одержувача інформації (настільки насиченого нею), що він уже не може сприймати її значення. Див. також шуми інформаційні.

ПЕРЕВЕРБУВАННЯ /перевербовка/ — процес перетворення ворожого агента у подвійного. Див. також вербування.

ПЕРЕДАВАЧ /передатчик/ [transmitter, sender] — технічний пристрій, призначений для перетворення сигналу джерела інформації, в форму, яка забезпечує його запис на носій інформації, що відповідає середовищу розповсюдження. В найбільш загальному випадку п. виконує наступні функції: створює (генерує) поля (акустичне, електромагнітне) або електричний струм, які переносять інформацію; здійснює запис інформації на носій (модуляцію інформаційних параметрів носія), підсилює потужність сигналу (носія з інформацією); забезпечує передавання (випромінювання) сигналу в середовище розповсюдження в заданому секторі простору. Див. також радіопередавач.

ПЕРЕКОНАНІСТЬ /убежденность/ [conviction, persuasion] — глибока упевненість в істинності засвоєних ідей, уявлень, понять, образів. Вона дозволяє приймати однозначні рішення і здійснювати їх без вагань, займати тверду позицію в оцінках цих чи інших фактів і явищ. На основі упевненості формуються установки людей, які визначають їхню поведінку в конкретних ситуаціях. Важлива характеристика п. — її глибина. Вона зв'язана з попереднім вихованням людей, їхньою інформованістю, життєвим досвідом, здатністю аналізувати явища навколишнього світу. Глибока упевненість характеризується великою стійкістю, щоб її похитнути недостатньо тільки логічних висновків.

ПЕРЕКОНАННЯ /убеждения/ [views] — свідомі, стійкі мотиви діяльності людей, що мають за звичай ідеологічну основу, і виявляються в їхніх діях, вчинках і поведінці.

ПЕРЕКОНЛИВІСТЬ /убедительность/ [convincingness, persuasiveness] — характеристика змісту інформації доводити що-небудь комусь, змушувати кого-небудь повірити у щось, погодитися з ким- чим-небудь (див. вплив змісту інформації). П. залежить у значній мірі від урахування притаманних об'єкту впливу установок, переконань, інтересів, потреб, його напряму думок, національно-психологічних особливостей і своєрідності мови. П. не входить до доказовості автоматично. Її може забезпечити тільки правильна пропорція між логічною і емоційною компонентами інформаційного повідомлення. При розробці впливу змістом інформації виходять із того, що: зміст інформаційно-пропагандистських матеріалів повинен бути добре обдуманим і відповідати законам формальної логіки; конкретне у змісті інформаційного повідомлення є переконливішим за абстрактне; чим більш динамічніший текст, тим яскравіші і різноманітніші в ньому факти, тим більше він привертає увагу; краще сприймається те, що є ближчим до інтересів і потреб об'єкта впливу; краще осмислюється те, що подається невеликими смисловими частинами (блоками); краще засвоюється те, що викликає відгук у об'єкта впливу; краще сприймається, осмислюється й засвоюється матеріал (інформація), який подається у відповідності до національних традицій сприйняття об'єкта.

ПЕРЕТВОРЕННЯ /преобразование/ [transformation] — переведення будь-чого з одного виду в інший, з однієї форми в іншу.

П. афінне /п. афинное/ [affine t., linear t.] — перетворення, що приводить до системи лінійних рівнянь, яка має однозначно означене рішення. Прикладом афінного перетворення є $y = (ax + s) mod n$.

П. криптографічне /п. криптографическое/ [cryptographical t.] — 1) Метод захисту інформації, що полягає в перетворенні (шифруванні) її складових частин (слів, букв, складів, цифр) за допомогою спеціальних алгоритмів або апаратних засобів і кодів ключів, тобто приведення інформації до неявного виду. Для ознайомлення із шифрованою інформацією застосовується зворотний процес: декодування (дешифрування). Використання п. к. є одним із розповсюджених методів, що значно підвищує безпеку передавання даних у мережах ЕОМ, даних, що зберігаються у віддалених пристроях пам'яті, і при обміні інформацією між віддаленими об'єктами (терміналами). 2) Перетворення даних, яке полягає в їхньому шифруванні,

виробленні імітовставки або підпису цифрового.

ПЕРЕТВОРЮВАЧ /преобразователь/ [converter, changer, transducer, transformer] — пристрій для перетворення сигналів або його модель математична.

П. акустоелектричні /п. акустоэлектрические/ [asoustoelectric t.] — фізичні пристрої, елементи, деталі і матеріали, здатні під дією змінного тиску хвилі акустичної створювати еквівалентні сигнали електричні. Властивості п. а. використовуються за своїм функціональним призначенням для створення мікрофонів різноманітних типів. Проте існують різноманітні радіоелектронні і електричні елементи та пристрої, яким властивий так званий "мікрофонний ефект", тобто здатність перетворювати акустичні сигнали в електричні. Це обумовлює появу в радіоелектронних засобах і системах, що містять п. а., небезпечних сигналів (див. джерело небезпечного сигналу), які створюють передумови для витоку інформації. Небезпечні сигнали на виході а. п. можуть розповсюджуватися проводами, що виходять за межі контрольованих зон або модулювати (див. модуляція) інші, більш потужні електричні сигнали, до яких можливий доступ зловмисників. П. а., здатні створювати небезпечні сигнали, поділяються на індуктивні, ємнісні та п'єзоелектричні.

П. акустоелектричні електродинамічні /п. акустоэлектрические электродинамические/ [electrodynamic asoustoelectric t.] — перетворювачі акустоелектричні індуктивні, в яких електричні сигнали, модульовані акустичними сигналами, виникають при переміщеннях під дією акустичних хвиль індуктивностей (котушок із металевим проводом) у магнітних і електричних полях. п. а .е., здатним створювати небезпечні сигнали, є, наприклад, динамічна головка гучномовця. Непрацюючі, але безпосередньо приєднані до радіотрансляційної мережі гучномовці, можуть виконувати функцію мікрофона і передавати інформацію розмов у приміщенні на достатньо великі відстані.

П. акустоелектричні електромагнітні /п. акустоэлектрические электромагнитные/ [electromagnetic asoustoelectric t.] — перетворювачі акустоелектричні індуктивні, в яких електричні сигнали, модульовані акустичними сигналами, виникають в індуктивностях внаслідок змін напруженості полів (магнітних і електричних) під дією акустичних хвиль. До п. а. е., здатних створювати небезпечні сигнали, відносяться

електромагніти електромеханічних дзвінків та капсулів телефонних апаратів.

П. акустоелектричні ємнісні /п. акустоэлектрические емкостные/ [capacitive asoustoelectric t.] — перетворювачі акустоелектричні, в яких небезпечні сигнали, модульовані акустичними сигналами, виникають внаслідок механічної зміни під тиском хвилі акустичної зазорів між пластинами конденсаторів і проводами, що приводить до еквівалентної зміни значень зосереджених і розподілених ємностей схем радіотехнічних засобів.

П. акустоелектричні індуктивні /п. акустоэлектрические индуктивные/ [inductive asoustoelectric t.] — перетворювачі акустоелектричні, в яких сигнали електричні, модульовані акустичними сигналами, виникають при переміщеннях під дією хвиль акустичних індуктивностей (котушок із металевим проводом) у магнітних і електричних полях або при змінах геометричних розмірів котушок або їхніх осердь. П. а. і. поділяються на електродинамічні, електромагнітні, магнітострикційні.

П. акустоелектричні магнітострикційні /п. акустоэлектрические магнитострикционные/ [magnetostrictive asoustoelectric t.] — перетворювачі акустоелектричні індуктивні, в яких електричні сигнали, модульовані акустичними сигналами, виникають в індуктивностях унаслідок зміни властивостей феромагнітних речовин осердь внаслідок деформації, викликаної дією акустичних хвиль. До п. а. м., здатних створювати небезпечні сигнали, відносяться контури з феромагнітними осердями, дроселі, трансформатори тощо (див. матеріали магнітострикційні).

П. акустоелектричні п'єзоелектричні /п. акустоэлектрические пьезоэлектрические/ [piezoelectric asoustoelectric t.] — перетворювачі акустоелектричні, в яких використовуються властивості деяких кристалічних речовин (кварцу, сегнетової солі, титаніту і ніобіту барія і т. ін.) створювати заряди на своїх поверхнях при їхній деформації, в тому числі під дією хвилі акустичної. Ці речовини застосовуються для створення функціональних акустоелектричних перетворювачів, наприклад, п'єзоелектричних мікрофонів. Небезпечні сигнали створюють матеріали п'єзоелектричні, в основному кварци, що застосовуються в генераторах для

стабілізації частоти, а також п'єзоелементи вібраторів і датчиків технічних засобів охорони.

П. аналого-цифровий /п. аналого-цифровой/ [analog-to-digital c.] — пристрій, призначений для перетворення аналогових величин у дискретні цифрові величини.

П. електроакустичний /п. электроакустический/ [electroacoustic t.] — пристрій, що перетворює електромагнітну енергію в енергію акустичних хвиль і навпаки. В залежності від напрямку перетворення розрізняють п. е.: випромінювачі (передавачі) і приймачі. п. е. широко застосовуються для випромінювання і прийому хвиль акустичних діапазону звукового в техніці зв'язку і звуковідтворення, для вимірювання і прийому акустичних коливань в ультразвуковій техніці, гідроакустиці, і в акустоелектроніці.

П. світлоелектричні /п. светоэлектрические/ [photoelectric t.] — фізичні пристрої, елементи, деталі і матеріали, здатні під дією видимої частини випромінювання електромагнітного оптичного діапазону створювати еквівалентні сигнали електричні. П. с. використовуються при створенні камер телевізійних різноманітних типів, основу яких складають вакуумні передавальні трубки або мішені твердотільних перетворювачів (див. прилад із зарядовим зв'язком.

П. цифро-аналоговий /п. цифро-аналоговый/ [digital-to-analog c.] — пристрій, призначений для перетворення дискретних величин в аналогові.

П. частоти /п. частоты/ [frequency c.] — в радіотехніці — електронний пристрій, що змінює частоту радіосигналу, яка подається на його вхід, унаслідок впливу допоміжних коливань іншої частоти на елементи цього пристрою. З одержаного спектра коливань із комбінаційними частотами фільтр, приєднаний до виходу п. ч. виділяє коливання з частотою, яка найчастіше дорівнює різниці частот радіосигналу і допоміжних коливань. П. ч. використовується в супергетеродинних радіоприймачах, у каскаді перетворення частоти в так звану частоту проміжну, а також в синтезаторах частот і радіопередавачах.

ПЕРЕХОПЛЕННЯ /перехват/ [intercept(ion), wiretapping] — 1) Захоплення, схоплення кого-чого-небудь на шляху слідування. 2) Несанкціоноване приймання радіосигналів та сигналів електричних і добування з них інформації семантичної, ознак демаскуючих сигналів і формування зображень об'єктів при пере-

хопленні сигналів телевізійних або факсимільних. 3) Складова частина назви способів підслухування і спостереження (див. аудіоперехоплення, відеоперехоплення).

П. безпосереднє (активне) /п. непосредственный (активный)/ — перехоплення інформації, яке здійснюється за допомогою безпосереднього приєднання до телекомунікаційного обладнання комп'ютера, комп'ютерної системи або мережі, наприклад, лінії принтера або телефонного проводу каналу зв'язку, що використовується для передавання даних і управляючих сигналів, або безпосередньо через відповідний порт персонального комп'ютера. У зв'язку з цим розрізняють: форсоване перехоплення, перехоплення символів, перехоплення повідомлень.

П. електромагнітне (пасивне) /п. электромагнитный (пассивный)/ — перехоплення інформації за допомогою пристроїв, що не потребують безпосереднього приєднання до інформаційної системи. Дія таких пристроїв заснована на прийманні, закріпленні на фізичному носії та аналізі електромагнітного випромінювання, що виникає при функціонуванні багатьох засобів комп'ютерної техніки, включаючи і засоби комунікації. Прикладом п. е. є перехоплення інформації з дисплея комп'ютера дистанційне.

П. інформації /п. информации/ — в системах інформаційних — навмисні дії, спрямовані на несанкціоноване одержання даних і інформації машинної.

П. інформації з дисплея дистанційне /п. информации с дисплея дистанционный/ — одержання відеозображення екрана дисплея функціонуючої ЕОМ методом перехоплення електромагнітного. Для відтворення відеозображення можуть використовуватися телевізори, інші дисплеї тощо.

П. повідомлень /п. сообщений/ [message wiretapping] — перехоплення безпосереднє за допомогою спеціального термінала, несанкціоновано приєднаного до лінії зв'язку; приймання і використання повідомлень, що циркулюють між пунктами абонентськими і ЕОМ.

П. символів /п. символов/ [character seize] — виділення з тексту, що набирається користувачем на клавіатурі термінала, знаків, не передбачених стандартним кодом даної ЕОМ. Вид перехоплення безпосе-

реднього.

П. форсоване /п. форсированный/ [willful i.] (франц. forcé, від force — сила) — перехоплення безпосереднє, що являє собою перехоплення повідомлень, що направляються станціям робочим (ЕОМ), які мають неполадки в обладнанні або каналах зв'язку.

ПЕРЕШКОДИ /помехи/ — те ж, що завади.

ПЕРІОД /период/ [period] (від грец. *περίδøδøς* — кружний шлях, обертання, чергування) — проміжок часу, протягом якого відбувається якийсь процес.

ПЕРСОНАЛІЗАЦІЯ /персонализация/ [personalization] — процес занесення на пластикову картку даних, які дозволяють ідентифікувати саму карту, її власника, а також перевірити платежеспроможність картки при її прийманні до оплати або видачі готівки.

ПЕРЦЕПЦІЯ /перцепция/ (від лат. perceptio — сприймання, пізнавання) — чуттєве сприйняття зовнішніх предметів.

П. соціальна /п. социальная/ — див. сприйняття соціальне.

ПІДГОТОВКА /подготовка/ [preparation, processing, training] — здійснення чого-небудь попередньо для облаштування, організації чого-небудь.

П. морально-психологічна /п. морально-психологическая/ — підготовка військовослужбовців, спрямована на формування у них такого душевного настрою, який дозволяє переборювати страх, розгубленість, втомленість, допомагає в будь-якій ситуації зберігати упевненість в своїх силах, спонукає бути хоробрим і завзятим; складова частина бойової підготовки. П. м.-п. дозволяє вирішувати наступні завдання: виховувати фізично витривалих і психологічно стійких воїнів, здатних успішно переборювати труднощі бойового й похідного життя; вироблювати в них стійкі професійні бойові навички, які дозволяють успішно діяти в екстремальних умовах на полі бою; формувати психологічну готовність до боротьби із сильним противником, який здатний домагатися успіху в ході бойових дій; забезпечити соціально-психологічну згуртованість частин, підрозділів, бойових екіпажів і обслуг. Важливими елементами п. м.-п. є психотерапія, психости-

мулювання, а також ідейно-політичне виховання. Сучасна концепція п. м.-п. передбачає цілеспрямоване загартовування психіки військовослужбовців в умовах, що максимально наближені до бойових: це, що військовослужбовець успішно витримує в ході навчання, він спокійно витримає і в умовах справжньої війни; в першу чергу з усіх психологічних якостей потрібно формувати почуття упевненості; методи й прийоми психотерапії і психостимулювання повинні бути різноманітними.

ПІДКЛАДАННЯ /подкладывание/ — процес кладення, поміщення під кого, що-небудь або в середину чогось.

П. свині /п. свиньи/ — вид атаки, коли порушник підключається до лінії зв'язку і імітує роботу системи з метою одержання інформації про ідентифікацію користувача.

ПІДКЛАДКА /подкладка/ [bug] — предмет, який під що-небудь підкладають. Див. також закладка.

П. програмна /п. программная/ [program b.] — потай впроваджена програма, що являє загрозу для інформації.

ПІДКЛЮЧ /подключ/ [subkey] — ключ, утворений з основного ключа, який використовується в деякій частині алгоритму криптографічного. Див. також ключ цикловий.

ПІДПИС /подпись/ [signature] — 1) Напис на будь-чому. 2) Власноручно написане прізвище.

П. безперечний /п. бесспорная/ — схема цифрового підпису, що використовує протокол заперечення.

П. груповий /п. групповая/ — схема підпису цифрового, яка дозволяє будь-якому членові групи підписати повідомлення таким чином, щоб при перевірці можна було встановити, що повідомлення підписане одним із членів групи, без конкретизації його особи.

П. електронний (цифровий) (ЕЦП) /п. электронная (цифровая) (ЭЦП)/ [electronic (digital) s.] — цифрова послідовність, що додається до повідомлення (даних) для забезпечення цілісності та підтвердження авторства і формується із застосуванням криптосистем асиметричних.

П. коду /п. кода/ — механізм, що дозволяє підписувати програмне забезпечення, що розповсюджується мережами загального користування. П. к. дозволяє автентифікувати автора програмного забезпечення і

гарантувати, що у процесі передавання код не модифікувався.

П. цифровий /п. цифровая/ [digital s.] — дані, одержані в результаті перетворення криптографічного блоку даних і (або) його параметрів (хеш-функції, довжини, дати утворення, ідентифікатора відправника і т. ін.), що дозволяють приймальникові даних впевнитися в цілісності блоку і справжньості джерела даних і забезпечити захист від підробки та підлогу.

П. цифровий сліпий /п. цифровая слепая/ [blind digital s.] — підпис цифровий, при якому абонент, що підписує, не може встановити тотожність між підписаними даними та будь-якими характеристиками процесу підпису цих даних (наприклад, часом, коли цей процес підпису відбувався). На час підпису абонент, що підписує, не має доступу до змісту даних, які він підписує.

ПІДРОБКА /подделка/ [falsification] — фальшива річ, імітація.

П. інформації /п. информации/ [information f.] — навмисні дії, що призводять до зміни інформації, яка повинна оброблятися або зберігатися в системі обчислювальній.

ПІДСВІДОМІСТЬ /подсознание/ [subconsciousness] — галузь активних психічних процесів, які, не будучи в певний момент центром смислової діяльності свідомості, здійснюють вплив на хід свідомих процесів.

ПІДСИСТЕМА /подсистема/ [subsystem] — частина системи, яка є сукупністю деяких відносно автономних елементів і разом з тим характеризується підпорядкованістю функціонування всієї системи.

П. багатофункціонального захисного шолома /п. многофункционального защитного шлема/ — центральний елемент комплекту спорядження, який доставляє солдатові візуальну і аудіоінформацію. В ньому максимально використовуються передові технології для досягнення функціональної ефективності і комфорту для солдата. Шолом має плоский нашоломний дисплей з високою чіткістю зображення, прилад нічного бачення і блок електронних схем управління, підсилення яскравості зображення і захвату цілей. Маса шолома складає близько 1,27 кг. Він виготовлений з матеріалу “кевлар” на основі скловолокна і захищає солдата від ураження лазерною зброєю або балістичною зброєю .

П. індивідуального захисту комплекту спорядження /п. индивидуальной защиты комплекта

снаряжения/ — підсистема, що має бронежилет або бронекомбінезон для захисту тіла з матеріалу "кевлар", додаткові пластини з того ж матеріалу для захисту області серця та спини, спеціальний фартух для захисту нижньої частини тіла та ніг. При конструюванні всіх цих захисних засобів зверталася увага на зменшення їхньої маси, зняття обмежень для рухів солдата і підвищення мобільності.

П. інженерного захисту /п. инженерной защиты/ — частина системи охорони об'єктів, призначена для механічного запобігання проникненню зловмисника до об'єктів захисту. Вона включає конструкції інженерні, що створюють механічні перепони на шляху зловмисника, і засоби (комплекси) керування доступом людей і транспорту на територію, що охороняється.

П. інтерфейсу із системами зброї комплекту спорядження /п. интерфейса с системами оружия комплекта снаряжения/ — підсистема, що забезпечує взаємодію з різноманітними системами прицілювання зброї з усіма підсистемами комплекту спорядження.

П. керування /п. управления/ [control segment] — частина системи охорони об'єктів, що забезпечує функціонування системи і керування її елементами в різноманітних ситуаціях (див. засоби керування системою охорони об'єктів).

П. комп'ютер-радіо комплекту спорядження /п. компьютер-радио комплекта снаряжения/ — підсистема, що є "мозком" всього комплекту спорядження. Вона включає в себе засоби апаратні і програмні комп'ютера, радіостанцію, сумісну з станцією супутникового зв'язку, спеціальну радіостанцію для зв'язку всередині всього підрозділу, пристрій розпізнавання по голосу, приймач відеозображення та інші компоненти. Для вводу даних в комп'ютер призначена проста клавіатура, яка носиться на зап'ясті.

П. мікроклімату і кондиціювання комплекту спорядження /п. микроклимата и кондиционирования комплекта снаряжения/ — підсистема, що має пристрої примусового обдування і терморегулювання, які створюють нормальний мікроклімат для солдата, сприяють його ефективним діям на полі бою.

П. нейтралізації загроз /п. нейтрализации угроз/ (від лат. neutralis — не належний ні тому, ні іншому) — частина системи охорони об'єктів, що має у своєму складі функціонально об'єднаних людей і засоби для

фізичного і психологічного впливу на зловмисників, що проникли на територію, що охороняється, а також засоби гасіння пожежі (див. засоби нейтралізації загроз об'єктові охорони).

П. сповіщення /п. оповещенния/ — частина системи охорони об'єктів, яка повинна сповіщати співробітників служби безпеки, насамперед, охоронців, органи охорони, пожежну охорону тощо про проникнення зловмисників на територію, що охороняється, про пожежу або інші стихійні лиха, захист від яких передбачений завданнями системи. Основу цієї підсистеми складають технічні засоби охорони.

П. спостереження /п. наблюдения/ — частина системи охорони об'єктів, що забезпечує можливість дистанційного візуального контролю за територією, що охороняється, та діями зловмисників. Основу п. с. найчастіше складають телевізійні засоби спостереження. До неї входять також засоби освітлення, що забезпечують необхідний рівень освітленості території в нічний час.

ПІДСЛУХУВАННЯ /подслушивания/ [listening] — спосіб добування інформації дистанційного від джерел сигналів акустичних. П. буває безпосереднє і за допомогою технічних засобів. Цим способом добувається в основному інформація семантична (мовна) , а також ознаки демаскуючі сигналів від працюючих механізмів, машин та інших джерел звуку.

П. безпосереднє /п. непосредственное/ — підслухування тільки за допомогою слухового апарату людини. При п. б. зловмисником приймаються сигнали акустичні, що розповсюджуються від джерела звуку прямолінійно, по повітроводах або через різноманітні загородки (двері, стіни, вікна і т. ін.) і екрани. Для полегшення сприйняття структурних звуків, що розповсюджуються у твердому середовищі використовують пристрої — стетоскопи, які передають коливання поверхні твердого середовища розповсюдження в слухові проходи вух людини.

П. за допомогою технічних засобів /п. с помощью технических средств/ — технічна реалізація різноманітних способів підслухування: приймання і прослуховування акустичних сигналів, що розповсюджуються у повітрі, воді і твердих тілах; прослуховування мови, що виділяється з перехоплених радіо- і електричних сигналів функціональних каналів зв'язку та із сигналів побічного випромінювання і наведень;

застосування лазерних систем підслухування; використання закладних пристроїв; засобів високочастотного нав'язування. Підслухування здійснюється на основі застосування наступних технічних засобів: приймачів акустичних, в тому числі з мікрофонами спрямованими; приймачів небезпечних сигналів; пристроїв закладних; засобів лазерного підслухування; засобів високочастотного нав'язування.

ПІДСТРАХУВАННЯ /подстраховка/ [safety net] — заходи підтвердження і підтримки прикриття або легенди агента розвідки. Проводяться превентивно на той випадок, коли це прикриття підлягає перевірці з боку іноземної спеціальної служби.

ПІДХІД /подход/ [approach] — сукупність прийомів, способів впливу на кого-що-небудь, вивчення будь-чого, ведення справи.

П. системний /п. системный/ [system a.] — методологічний напрям в науці, основне завдання якого складає розроблення методів дослідження і конструювання складноорганізованих об'єктів — систем різних типів і класів (найчастіше таких, що слабо формалізуються). П. с. являє собою певний етап в розвитку методів пізнання, методів дослідницької і конструкторської діяльності, способів опису і пояснення природи об'єктів, що аналізуються або створюються штучно. П. с. реалізується на основі принципів системного підходу та потребує від фахівців системного мислення. З позиції п. с. сукупність взаємозв'язаних елементів, функціонування яких спрямоване на забезпечення безпеки інформації, створює систему захисту інформації.

П. системний до інформаційної безпеки /п. системный к информационной безопасности/ — розгляд безпеки інформаційної з позицій підходу системного. Дозволяє підвищити ефективність наукового осмислення проблеми інформаційної безпеки від загрози нових небезпек інформаційних (інформаційно-технічних), зумовлених досягненнями науково-технічного прогресу. Системний підхід потребує визначення і розгляду суб'єктів інформаційної безпеки, засобів і об'єктів інформаційної безпеки, принципів забезпечення інформаційної безпеки, джерел небезпеки інформаційної, напрямків небезпечних інформаційних потоків.

ПІЗНАННЯ /познание/ [perception, cognition] — процес відображення й відтворення дійсності в мисленні, зумовлений суспільно-історичним розвитком; взаємодія суб'єкта і об'єкта, результатом якої є нове знання

про світ.

ПІКНІК /пикник/ [pyknic] (від грец. *πυκνός* — міцний, кремезний) — людина, для якої характерна певна будова тіла: кремезна фігура, коротка шия і великий живіт.

ПЛАН /план/ [plan] (від лат. planum — рівне місце, площина) — 1) Система взаємопов'язаних об'єднаних загальної метою завдань, що визначають строки, порядок і послідовність виконання робіт, операцій тощо. 2) Порядок, послідовність викладання будь-якого матеріалу.

П. забезпечення безупинної роботи й відновлення /п. обеспечения непрерывной работы и восстановления/ — план реагування на небезпечні ситуації, резервного копіювання і наступних відновлювальних процедур, який є частиною програми захисту і забезпечує доступність основних ресурсів системи й безперервність оброблення в кризових ситуаціях.

П. захисту /п. защиты/ — необхідний в повсякденній роботі документ, який визначає реалізацію системи захисту.

ПЛАНУВАННЯ /планирование/ [planning, scheduling] — практика складання планів, проведення діяльності в раніше наміченому порядку.

П. інформаційних систем стратегічне /п. информационных систем стратегическое/ — див. система інформаційна стратегічна.

ПЛАТФОРМА /платформа/ [platform] (франц. plate-form — букв. плоска форма) — рівний підвищений майданчик.

П. комп'ютерна /п. компьютерная/ [computer p.] — тип комп'ютера персонального (PC, Macintosh, Atary, Sincler і т. ін.), на якому може бути встановлений даний програмний продукт.

ПОВЕДІНКА /поведение/ [behaviour] — система взаємозв'язаних реакцій, що здійснюється живими організмами для пристосування до середовища. П. тварин і людини вивчається етологією, психологією, соціологією.

ПОВЕРХНЯ /поверхность/ [surface] — зовнішня сторона чого-небудь.

П. розсіювання ефективна (ЕПР) /п. рассеивания эффективная (ЭПР)/ [reflection s.] — характеристика відбивної здатності цілі (об'єкта), що опромінюється хвилями електромагнітними. Значення ЕПР визначається як відношення потоку (потужності) електромагнітної енергії, відбитої об'єктом в напрямку точки приймання, до поверхневої щільності потоку енергії, що падає на ціль. ЕПР об'єкта залежить в основному від розмірів та конфігурації цілі, властивостей її матеріалу, довжини і поляризації хвилі та напрямку опромінювання.

ПОВІДОМЛЕННЯ /сообщение/ [message] — 1) Те, що повідомляється, звістка, інформація. 2) Впорядкована послідовність символів, призначена для передавання інформації. 3) Довільна кількість інформації, початок і закінчення якої визначені, призначена для передавання від одного абонента іншому в будь-якій формі, що відповідає виду зв'язку.

П. двостороннє /с. двухстороннее/ — спосіб подання аргументів у вигляді повідомлення, що містить як аргументи джерела інформації, так і контраргументи противника, які доведеться викривати. Така побудова повідомлення служить спонукальним мотивом до активної розумової діяльності об'єкта, в результаті того здійснюється перегляд суджень, що складалися у нього раніше. П. д. спрямовується переважно на людей з високим рівнем освіти, що відчувають потребу в зіставленні різних поглядів, точок зору, думок, оцінок. В цей же час п. д. як би випереджає аргументацію противника і створює передумови для утворення певного імунітету проти його офіційної пропаганди.

П. інформаційне /с. информационное/ [data m., information m.] — вид програми радіомовлення, яка містить оперативну інформацію про найбільш важливу подію, факт або явище, що представляють значний інтерес для більшості цих слухачів противника, на яких ведеться мовлення. П. і. повинно відповісти на питання: що відбулося, де, коли, хто діяв, як, чому, які наслідки того, що трапилося. Вважають, що тривалість кожного повідомлення не повинна складати більше однієї хвилини. Повідомлення можна передавати

в ефір у вигляді тематичної добірки, наприклад: “Останні вісті”, “Положення на фронті” і т. ін.

П. одностороннє /с. одностороннее/ — спосіб подання аргументів у вигляді повідомлення, що містить аргументи тільки джерела інформації. Такі повідомлення більш ефективні тоді, коли об’єкт психологічного впливу не відчуває ворожих почуттів по відношенню до джерела інформації і, до того ж, має низький рівень освіти. Об’єкт у цьому випадку здатний відносно легко прийняти точку зору джерела інформації. П. о. можна також використовувати для впливу переконуючого на людей, що мають різний освітній рівень.

ПОВНОВАЖЕННЯ /полномочия/ [privilege] — право суб’єкта доступу (користувача або процесу) на виконання певних дій, зокрема на одержання певного типу доступу до об’єктів.

ПОВНОТА /полнота/ [completeness] — наявність чого-небудь у достатній мірі, вища ступінь насиченості чим-небудь.

П. добутої інформації /п. добытой информации/ — повнота інформації, що поступає від органів добування інформації, яка повинна забезпечувати знання проблеми, необхідне для обґрунтованого прийняття рішення керівництвом. Характеризується наступними показниками: відповідністю обсягу добутих відомостей, даних обсягу всієї добутої інформації; відношенням розкритих проблем (питань) до загального числа поставлених проблем (питань).

П. інформації /п. информации/ [information c.] — характеристика, яка визначає кількість інформації, необхідної для прийняття рішення.

ПОВТОРЮВАЧ /повторитель/ [repeater] — пристрій рівня фізичного моделі ISO/OSI, призначений для підсилення сигналу з одного сегмента кабелю на інший сегмент без зміни змісту. Дозволяє збільшувати довжину магістралі мережі і кількість абонентів. Застосовується в мережах обчислювальних локальних.

ПОГОДЖЕННЯ /соглашение/ [agreement] — 1) Взаємна згода, домовленість. 2) Договір, що встановлює які-небудь умови, взаємовідносини, права й обов’язки сторін.

П. ключів (формування ключів) /с. ключей/ [key a.] — методи встановлення ключа, при яких спільний ключ генерується за деякою процедурою, в якої беруть участь два (або більше) абонентів. Значення

ключа залежить від інформації всіх (або принаймні більше одного) абонентів. Властивістю цих методів є неможливість визначення значення ключа одним з абонентів до початку процедури формування спільного ключа.

ПОДОЛАННЯ /преодоление/ [mounting, overcoming, surmounting] — переборення різних перешкод.

П. використанням механізму установки (зняття) програмних засобів захисту інформації /п. использованием механизма установки (снятия) программных средств защиты информации/ — спосіб подолання програмних засобів захисту, заснований на знаннях особливостей установки (зняття) захисту. Здійснюється на основі наступного алгоритму дій: одержують санкціонований або несанкціонований доступ до захищеного програмного засобу, що розташований у пристрої пам'яті; аналізують структуру розташування й зміст усіх файлів (у тому числі і прихованих), створених у пристрої пам'яті програмою установки; виконується копіювання захищеної програми з пристрою пам'яті (при цьому відновлюється вихідний лічильник установок); відновлюється збережений стан системи і її вміст. В результаті одержують ключову дискету з вихідним лічильником установок і нелегальну копію програмного продукту. Спосіб потребує глибокого знання структури файлової системи.

П. зняттям системи захисту з пам'яті ЕОМ /п. снятием системы защиты из памяти ЭВМ/ — спосіб подолання програмних засобів захисту, який полягає у визначенні часу, коли при зашифровуванні (розшифровуванні) в пам'яті ЕОМ знаходиться повністю розшифрована програма, і її копіювання за допомогою перехоплення відповідного переривання.

П. копією ключової дискети /п. копией ключевой дискеты/ — спосіб подолання програмних засобів захисту, що здійснюється шляхом електромагнітного перенесення всієї структури і інформації, розташованої на ключовій дискеті-оригіналі, захищеній від копіювання програмними засобами, на дискету-копію, в результаті чого автентифікаційна частина системи захисту сприймає копію ключової дискети як оригінал.

П. моделюванням звернень до ключової дискети /п. моделированием обращений к ключевой дискете/ — спосіб подолання програмних засобів захисту, який полягає у програмному моделюванні ре-

зультатів звернень ЕОМ до ключової дискети шляхом перехоплення відповідних переривань.

П. модифікацією коду системи захисту /п. модификацией кода системы защиты/ — спосіб подолання програмних засобів захисту, який полягає в модифікації (зміні) коду модуля системи захисту, що виконує наступні функції: перевірку ключової дискети; коригування лічильника установок на жорсткий магнітний диск (вінчестер), захищеного від копіювання програмного засобу з ключової дискети; перевірку санкціонованості запуску захищеного інформаційного ресурсу.

П. програмних засобів захисту /п. программных средств защиты/ — дії злочинця (зловмисника), спрямовані на навмисне подолання програмних засобів захисту комп'ютерної техніки і має декілька різновидів: подолання копією ключової дискети; подолання модифікацією коду системи захисту; подолання моделюванням звернень до ключової дискети; подолання використанням механізму установки (зняття) програмних засобів захисту інформації; подолання зняттям системи захисту з пам'яті ЕОМ і т. ін.

ПОКАЖЧИК URL /указатель URL/ [Uniform Resource Locator (уніфікований покажчик на ресурс)(URL)] — адреса ресурсу Інтернету (Web-сервера, сайта, сторінки). URL схожий до імені файла, але додатково містить ім'я сервера і інформацію про мережний протокол, що використовується даним ресурсом. В деяких випадках URL включає відомості про ім'я користувача, а також спеціальні аргументи і параметри протоколу.

ПОКАЗНИК /показатель/ [criterion, measure] — дані, за якими можна робити висновок про розвиток, хід, стан будь-чого.

П. ефективності системи захисту інформації /п. эффективности системы защиты информации/ [protection c.] — див. критерій ефективності системи захисту інформації.

П. ефективності системи захисту інформації часткові /п. эффективности системы защиты информации частные/ — показники, що характеризують ефективність захисту інформації з окремих сторін. Такими показниками можуть бути: ймовірність виявлення і розпізнавання органами розвідки об'єктів захисту; похибки вимірювання ознак об'єктів захисту; якість розбірливості мови на виході приймача злов-

мисника; достовірність (ймовірність помилки) дискретного елемента інформації (букви, цифри, елемента зображення). На основі різноманітних композицій часткових показників, найчастіше їхньої "зваженої" суми формується критерій ефективності системи захисту інформації глобальний.

П. загрози безпеці інформації /п. угрозы безопасности информации/ — показник, що характеризує розмір шкоди в результаті проникнення зловмисника до джерела інформації, що підлягає захисту, або її витоку по технічному каналу і визначається для кожного шляху і каналу витоку у вигляді добутку ймовірності реалізації даного шляху або каналу на ціну відповідного елемента інформації.

П. звукоізоляції /п. звукоизоляции/ — показник, що характеризує величину ослаблення R в дБ акустичної хвилі засобами звукоізоляції акустичного сигналу:

$$R = 10 \cdot \lg(P_1/P_2),$$

де P_1 — потужність падаючої на засіб звукоізоляції акустичної хвилі, P_2 — потужність акустичної хвилі, що пройшла через цей засіб.

П. інформованості /п. информированности/ — інтегральний показник, що відображає повноту і достовірність всієї інформації, необхідної для оцінки обстановки. Таким показником може бути показник правильної інформованості органу керування:

$$K = \frac{\sum_{i=1}^{D} \sum_{j=1}^{R} P_{ij}}{DR},$$

де D — кількість характеристик тематичного розділу кадастру інформаційного; R — кількість тематичних розділів інформаційного кадастру; P_{ij} — показник правильної інформованості органу управління про i-ту характеристику j-того розділу інформаційного кадастру ($0 \le P_{ij} \le 1$). Згідно формули, інформованість органу керування може змінюватися від 0 до 1. Причому нижнє значення показника відповідає повній дезінформованості органу керування, а верхнє — стану вичерпно достовірного знання обстановки.

П. якості і кількості добутої інформації /п. качества и количества добытой информации/ — пока-

зники, призначені для визначення ефективності органів добування інформації. До них відносяться: повнота добутої інформації; своєчасність добутої інформації; достовірність добутої інформації; точність вимірювання ознак; сумарні витрати на одержання інформації.

ПОЛЕ /поле/ [field] — простір, в межах якого проявляються дії будь-яких сил.

П. бою електронне /п. боя электронное/ — сукупність електронних озброєнь, призначених для бойових дій у галузі командування й керування військами.

П. електричне /п. электрическое/ [electric f.] — часткова форма прояву (поряд із полем магнітним) поля електромагнітного, яка визначає дію на електричний заряд (із боку поля) сили, що не залежить від швидкості руху заряду. Кожний нерухомий заряд створює у навколишньому просторі п. е. Поле одного заряду діє на інший заряд і навпаки. Основна кількісна характеристика п. е. — напруженість п. е., яка в даній точці простору визначає відношення сили, що діє на заряд, розташований в даній точці, до величини заряду. Розподілення п. е. у просторі зображуються за допомогою силових ліній напруженості п. е. Силові лінії потенціального п. е., що породжується електричними зарядами, починаються на позитивних зарядах і закінчуються на негативних (або виходять на безкінечність). Силові лінії вихрового п. е., що породжуються змінним магнітним полем, замкнуті.

П. електромагнітне /п. электромагнитное/ [electromagnetic f.] — особлива форма матерії, через яку здійснюється взаємодія між електрично зарядженими частками. П. е. у вакуумі характеризується вектором напруженості електричного поля і магнітного поля. В середовищі п. е. характеризується додатково двома допоміжними величинами: напруженістю магнітного поля і електричною індукцією. П. е. заряджених часток, які нерухомі або рівномірно рухаються, нерозривно зв'язано з цими частками. Якщо частки рухаються прискорено, то п. е. "відривається" від них і існує незалежно у формі електромагнітних хвиль. П. е. виникає при протіканні провідниками джерела радіосигналу електричного струму змінної частоти і розповсюджується з кінцевою швидкістю у навколишньому просторі. Вектори напруженості електричного і магнітного полів взаємно перпендикулярні і перпендикулярні напрямку розповсюдження електромагнітної

хвилі. Потужність випромінювання е. п. тим більша, чим ближча частота коливань в розподіленому контурі, створеному індуктивністю провідників і розподіленою ємністю між ними і землею, до частоти сигналу. Ефективне перетворення енергії електричних сигналів в електромагнітну хвилю здійснюється антенами.

П. звукове /п. звуковое/ [sound f.] — частина простору, в якому розповсюджуються хвилі звукові.

П. магнітне /п. магнитное/ [magnetic f.] — силове поле, що діє на рухомі електричні заряди і на тіла, що мають магнітний момент. П. м. характеризується вектором магнітної індукції, значення якого визначає силу, що діє в даній точці поля на рухомий електричний заряд і на тіла, що мають магнітний момент. П. м. виникає в результаті руху заряджених мікрочасток (електронів, протонів, іонів), а також із-за наявності у мікрочасток власного (спінового) магнітного моменту. Змінне магнітне поле виникає також при зміні у часі поля електричного. У свою чергу, при зміні у часі п. м. виникає електричне поле. Повний опис електричного і магнітного полів і їхнього взаємозв'язку дають рівняння Максвелла. Для характеристики п. м. часто вводять силові лінії поля (лінії магнітного індукції).

П. фізичні /п. физические/ [physical f.] — особлива форма матерії. П. ф. здійснюють взаємодію між частками речовини. Прикладами п. ф. можуть бути поле ядерних сил, поле тяжіння (гравітаційне поле). П. ф. можуть існувати і незалежно від часток, що їх породжують (наприклад, поле електромагнітне).

ПОЛІГРАМА /полиграмма/ (від грец. $\pi\text{ø}\lambda\acute{\upsilon}\varsigma$... — численний і ...$\gamma\rho\acute{\alpha}\mu\mu\alpha$ — літера, написання) — послідовність кількох символів алфавіту. Послідовність із l символів алфавіту називають також l-грамою.

ПОЛІГРАФ /полиграф/ [polygraph] (від грец. $\pi\text{ø}\lambda\acute{\upsilon}\varsigma$... — численний і ...$\gamma\rho\acute{\alpha}\varphi\omega$ — пишу, креслю, зображую) — детектор брехні, дія якого заснована на хімічних змінах в організмі людини, що відчуває психологічний стрес. При стресі підвищується вміст адреналіну в крові, збільшується потреба організму в кисні, що, у свою чергу, викликає збільшення частоти пульсу, підвищення кров'яного тиску, частоти і глибини дихання. Коли джерело стресу зникає, організм випрацьовує норадреналін, який нейтралізує дію надлишкового адреналіну. Для відображення даних в п. використовують не менш двох самописців: кардіографічний і пневмографічний.

ПОЛІСЕМІЯ /полисемия/ [polycemy] (від грец. $\pi\text{ø}\lambda\acute{\upsilon}\varsigma$ — численний і $\sigma\tilde{\eta}\mu\alpha$ — знак) — наявність різних лексичних значень в одного й того самого слова.

ПОЛІТИК /политик/ [politician] (від політика) — активний учасник політики, політичного життя; політичний діяч, особа, яка професійно займається питаннями політика.

ПОЛІТИКА /политика/ [policy] (від грец. $\pi\text{ø}\lambda\iota\tau\iota\kappa\acute{\alpha}$ — державна діяльність) — 1) Цілі і завдання, що їх ставлять суспільні класи в боротьбі за свої інтереси; методи і засоби досягнення цих цілей і завдань. 2) Лінія поведінки у чому-небудь, певне ставлення до кого-, чого-небудь.

П. безпеки /п. безопасности/ [security p.] — сукупність законів, правил та практичного досвіду, на основі яких будується керування, захист і розподіл інформації конфіденційної.

П. безпеки інформації /п. безопасности информации/ [information security p.] — сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок оброблення інформації і спрямовані на захист інформації від певних загроз. В системах автоматизованих п. б. і. є частиною загальної політики безпеки організації і може включати, зокрема, положення державної політики у галузі захисту інформації (див. концепція інформаційної безпеки держави). Для кожної автоматизованої системи п. б. і. може бути індивідуальною і може залежати від технології оброблення інформації, що реалізується, особливостей системи обчислювальної, середовища фізичного і від багатьох інших факторів. П. б. і. повинна визначати ресурси автоматизованої системи, що потребують захисту, зокрема встановлювати категорії інформації, що оброблюється в системі. Мають бути сформульовані основні загрози для обчислювальної системи, персоналу, інформації різних категорій і вимоги до захисту від цих загроз. Складовими частинами загальної п. б. і. в автоматизованій системі мають бути політики забезпечення конфіденційності, цілісності і доступності інформації, що оброблюється. Відповідальність персоналу за виконання положень п. б. і. має бути персоніфікована. Частина п. б. і., яка регламентує правила доступу користувачів і процесів системи комп'ютерної, складає правила розмежування доступу.

П. безпеки послуги /п. безопасности услуги/ [service security p.] — правила, згідно якими функціо-

нують механізми, що реалізують послугу безпеки.

П. інформаційна /п. информационная/ [infopolicy] — головні напрямки і предмет діяльності держави в галузі інформації. Основною метою п. і. є створення умов для ефективного і якісного інформаційного забезпечення стратегічних і оперативних завдань соціального і економічного розвитку держави. Основними напрямками такої політики є: забезпечення умов для розвитку і захисту всіх форм власності на ресурси інформаційні; формування і захист державних інформаційних ресурсів; створення і розвиток центральних і регіональних мереж інформаційних і систем інформаційних, забезпечення їхньої сумісності і взаємодії в єдиному просторі інформаційному держави; створення умов для якісного і ефективного інформаційного забезпечення громадян, установ державної влади, органів місцевого самоуправління, організацій і суспільних об'єднань на основі державних інформаційних ресурсів; забезпечення безпеки національної в сфері інформатизації, а також забезпечення прав громадян, організацій в умовах інформатизації; сприяння формуванню ринку інформаційних ресурсів, послуг, інформаційних систем і технологій, засобів їхнього забезпечення; формування і здійснення єдиної науково-технічної промислової політики у сфері інформатизації з урахуванням сучасного світового рівня розвитку інформаційних технологій; підтримка проектів і програм інформатизації; створення і удосконалення системи інвестування і механізму стимулювання розробки і реалізації проектів інформатизації; розвиток законодавства у сфері процесів інформаційних, інформатизації і захисту інформації.

ПОЛІФАГ /полифаг/ (від грец. *πøλύς*... — численний ...*φάγøς* — пожирач) — антивірусна програма (див. антивірус, фаг), що розпізнає відомі їй віруси за характерними ділянками їхнього коду.

ПОНЯТТЯ /понятие/ [idea, notion, concept] — 1) Одна з форм мислення, результат узагальнення суттєвих ознак об'єкта дійсності. 2) Розуміння кимсь чого-небудь, що склалося на основі якихось відомостей, власного досвіду.

ПОРТРЕТ /портрет/ [portrait] (франц. portrait) — загальна характеристика, сукупність характерних рис

кого-, чого-небудь.

П. інформаційний /п. информационный/ [information p.] — сукупність елементів і зв'язків між ними, що відображають суть повідомлення (мовного або даних), ознаки об'єкта або сигналу. Елементами дискретного семантичного повідомлення, наприклад, є букви, цифри або інші знаки, а зв'язки між ними визначають їхню послідовність. П. і. об'єктів спостереження, сигналів або речовин є їхні структури ознакові еталонні.

ПОРУШЕННЯ /нарушение/ [violation] — 1) Дія, спрямована на заважання нормальному стану, розвитку будь-чого, переривання будь-якого процесу. 2) Невиконання, недотримування будь-чого.

П. роботи диктофона /н. работы диктофона/ — виключення запису мови на диктофон за допомогою активних засобів порушення його роботи. Внаслідок дії створюваних цими засобами полів змінюються режими роботи підсилювачів запису диктофона, в результаті чого різко погіршується розбірливість мови і стає неможливим її відновлення при відтворенні.

П. цілісності інформації /н. целостности информации/ [information integrity v.] — спотворення інформації, її руйнування або знищення.

ПОРУШНИК /нарушитель/ [infringer, user violator] — 1) Той, хто порушив будь-які правила, закон, звичай. 2) Користувач, який здійснює доступ несанкціонований до інформації. В цьому випадку п. одержує доступ до роботи з включеними до складу системи комп'ютерної засобами. П. класифікуються за рівнем можливостей, що надаються їм штатними засобами системи. Виділяють чотири рівні цих можливостей. Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього: перший рівень визначає найнижчий рівень можливостей проведення діалогу з комп'ютерною системою — можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції оброблення інформації; другий рівень визначається можливістю створення й запуску власних програм із новими функціями оброблення інформації; третій рівень визначається можливістю керування функціонуванням комп'ютерної системи, тобто впливом на базове програмне забезпечення системи

і на склад і конфігурацію обладнання; четвертий рівень визначається всім обсягом можливостей осіб, що здійснюють проектування, реалізацію й ремонт апаратних компонентів системи, аж до включення до її складу власних засобів з новими функціями оброблення інформації. Припускається, що в своєму рівні п. — це фахівець вищої кваліфікації, який має повну інформацію про комп'ютерну систему і комплекс засобів захисту.

П. правил розмежування доступу /н. правил разграничения доступа/ [security policy violator] — суб'єкт доступу, що здійснює доступ несанкціонований до інформації.

ПОСЛІДОВНІСТЬ /последовательность/ [sequence, series] — певна черговість подій, явищ, етапів роботи, порядок розташування чогось.

П. ключова /п. ключевая/ [keystream] — див. гамма.

П. кодова /п. кодовая/ [code s.] — послідовність кодованих символів, одержана за певними правилами. Може бути скінченною або нескінченною. Див. також комбінація кодова.

ПОСЛУГИ /услуги/ [service] — робота, що виконується для задоволення чиїх-небудь потреб; обслуговування.

П. безпеки /у. безопасности/ [security s.] — сукупність функцій, що забезпечують захист від певної загрози або від множини загроз.

П. інформаційні /у. информационные/ [information s.] — дії суб'єктів (власників), спрямовані на забезпечення користувачів інформаційною продукцією. До п. і. відносяться: послуги інформаційного обслуговування (пошук інформації, оброблення інформації, видавання даних або документів, зберігання інформації); послуги надання користування автоматизованими інформаційними системами, банками даних, їхніми мережами; консультативні послуги; послуги передавання інформації.

П. інформаційно-аналітичні /у. информационно-аналитические/ — дії служб інформаційно-аналітичних (органів, фірм), спрямовані на забезпечення користувачів продукцією діяльності інформаційно-аналітичної.

ПОТІК /поток/ [flow] — сукупність чого-небудь, що рухається.

П. інформації /п. информации/ [information f.] — передавання інформації від одного до іншого об'єкта комп'ютерної системи.

П. інформаційний /п. информационный/ [information f., traffic] — інформація, що знаходиться в упорядкованому русі по заданих напрямках із фіксованими початковими, проміжними та кінцевими точками.

П. інформаційний документальний /п. информационный документальный/ [f. of documentary information] — сукупність документів, що утворюють документальний масив. При отриманні п. і. д. виконуються наступні види аналізу: кількісний (статистичний або наукометричний), аналіз структури документального потоку, інформаційних зв'язків, якісний (змістовний) аналіз публікацій в п. і. д.

П. цифровий /п. цифровой/ [digital f.] — послідовність сигналів цифрових, що передаються каналом зв'язку.

ПОШТА /почта/ [mail] (нім. Post, з італ. posta — зупинка, станція, від лат. postus — поставлений) — 1) Один із видів зв'язку загального користування, що провадить пересилання листів, газет, журналів, посилок, грошових переказів. 2) Державна установа для пересилання кореспонденції. 3) Те, що доставляється цим засобом зв'язку.

П. електронна /п. электронная/ [electronic m.] — 1) Система зберігання і пересилання повідомлень між користувачами мережі ЕОМ; передавання ділової кореспонденції з допомогою електрозв'язку; прикладна служба передавання повідомлень між користувачами мережею. 1) Система зберігання і пересилання повідомлень між клієнтами Інтернету. Електронне повідомлення створює людина або комп'ютерна програма. Людина це робить за допомогою інтерфейсу користувача, працюючи на персональному комп'ютері, термінальному фреймі або міні-ЕОМ. Інтерфейс користувача взаємодіє з іншим програмним забезпеченням (у вигляді динамічної або іншої бібліотеки), яке забезпечує взаємодію з сервером поштовим. Саму бібліотеку або її сполучення з інтерфейсом користувача називають агентом користувача. Агент користувача приєднується до поштового сервера через локальну мережу або через (телефонну) лінію, що комутується.

Поштовий сервер, із яким зв'язується користувач називають домашнім сервером — через нього користувач відправляє свої електронні повідомлення. Також домашній сервер пересилає пошту іншим серверам за допомогою програмного модуля — агента пересилки пошти.

П. електронна клієнт-серверна /п. электронная клиент-серверная/ — пошта електронна, що описується трьома видами моделей: автономною(offline), інтерактивною (online) і вимкненою (disconnected).

П. електронна клієнт-серверна автономна /п. электронная клиент-серверная автономная/ — пошта електронна, у якої клієнт періодично приєднується до сервера і приймає накопичену пошту. Після того як повідомлення передані користувачеві, сервер їх вилучає. Все подальше оброблення виконується клієнтом. Така модель реалізована в протоколі POP. Протокол IMAP також підтримує цю модель, але її краще використовувати в поштах електронних клієнт-серверних інтерактивній і вимкненій.

П. електронна клієнт-серверна вимкнена /п. электронная клиент-серверная отключенная/ — пошта електронна, що являє собою дещо середнє між автономною і інтерактивною моделями. Клієнт приєднується до сервера, приймає вибрані повідомлення і оброблює їх в автономному режимі. Пізніше клієнт знову встановлює зв'язок із сервером і передає зміни (правку повідомлення або адресної книги, вилучення повідомлень, відповіді і т.ін. В цьому випадку сервер — головне сховище повідомлень, а клієнт тимчасове. Дану модель підтримує протокол IMAR.

П. електронна клієнт-серверна інтерактивна /п. электронная клиент-серверная интерактивная/ — пошта електронна, у якої клієнт встановлює сеанс зв'язку з сервером, і вся пошта оброблюється під час сеансу на сервері, а клієнт керує цим процесом. Цю модель підтримують протоколи IMAR, NFS і CIFS.

ПОШТАМТ /почтамт/ [head post-office] (нім. Postamt) — установа, яка обслуговує населення всіма видами поштового, телеграфного і телефонного зв'язку.

П. електронний /п. электронный/ — апаратно-програмний комплекс, призначений для керування приєднаними до нього пунктами абонентськими, комутації і передавання повідомлень між сусідніми п. е., власними абонентами, користувачами телеграфного і телефонного зв'язку, абонентами обчислювальної

мережі і власниками факсимільних апаратів.

ПОШУК /поиск/ [search(ing), retrieval] — 1) Дії шукаючого, розшукування кого-, чого-небудь. 2) Спосіб розвідки.

П. об'єктів розвідки /п. объектов разведки/ — цілеспрямовані дії сил та засобів органів розвідки, спрямовані на виявлення об'єктів розвідки (джерел і носіїв інформації, джерел сигналів) для одержання від них даних і відомостей. П. о. р. здійснюється у просторі і часі, а для об'єктів (джерел), що мають носії інформації у вигляді випромінювання і електричного струму, тільки за частотою сигналу.

ПРАВИЛО /правило/ [rule] — 1) Положення, яким передається якась закономірність, стале співвідношення певних явищ; припис, норма. 2) Зібрання якихось положень, що визначають порядок ведення або дотримання чого-небудь.

П. IPSec /п. IPSec/ [IPSec] — базова концепція забезпечення захисту даних, що передаються на "IP-рівні" мережі Інтернет. Складається з визначення протоколів, які реалізують визначені функції захисту інформації, так званих AH-протоколу та ESP-протоколу, правил їхнього використання, протоколів керування ключами (IKE-протокол), алгоритмів для автентифікації та шифрування. Специфікації IPSec викладені в групі стандартів RFC. Історично IPSec розроблявся для IP-протоколу, який відповідає IPv6, але зараз може застосовуватися і для IPv4. RFC 2401 визначає загальні вимоги до базової архітектури захисту даних на IP-рівні. Визначається такий набір функцій захисту інформації: контроль доступу до даних, цілісність, автентифікація джерела даних, контроль повторного використання пакетів, конфіденційність, контроль трафіка. Для протоколів AH та ESP визначаються два способи застосування до IP-пакета: транспорту та тунелювання. В режимі транспорту захисту підлягають тільки сегмент IP-дейтаграми, що відноситься до транспортного рівня, а в режимі тунелювання — весь IP-пакет.

П. доступу /п. доступа/ [access r.] — сукупність правил, які регламентують порядок і умови доступу до інформації, що захищається, і до її носіїв.

П. розмежування доступу (ПРД) /п. разграничения доступа (ПРД)/ [access mediation r-s] — частина

політики безпеки, що регламентує правила доступу користувачів і процесів до пасивних об'єктів.

ПРАВО /право/ [law, right, science of law, jurisprudence] — 1) Сукупність норм і правил для регулювання відносин людей у суспільстві, які встановлюються і охороняються державою, а також наука, що вивчає ці норми. 2) Можливість діяти, поступати яким-небудь чином.

П. авторське /п. авторское/ [author r., copyright] — сукупність законодавчих норм, що визначають правове положення автора по відношенню до створених ним об'єктів авторського права. П. а. не розповсюджується на ідеї, методи, процеси, системи, способи, концепції, принципи, відкриття, факти. Авторові по відношенню до його творів належать особисті немайнові права (право авторства, право на ім'я, право на обнародування творів, право на захист своєї репутації) і майнові права (виключні права на використання твору в будь-якій формі і будь-яким способом, зокрема право на відтворення, право на розповсюдження, право на публічний показ, право на передачу в ефір, право на переклад, право на перероблення). Власник виключних а. п. для повідомлення про свої права вправі використати знак охорони авторського права, який розташовується на кожному екземплярі твору і складається з трьох елементів: латинської букви "С" в колі — ©; імені (найменування) власника виключних авторських прав; року першого опублікування твору.

П. доступу /п. доступа/ [access r.] — 1) Сукупність правил доступу до інформації, що захищається, встановлених правовими документами або власником інформації. 2) Право, надане користувачеві на санкціоноване використання певної інформації (зокрема, програм та даних), що зберігається в системі. 3) Дозвіл або заборона здійснення певного типу доступу.

П. інформаційне /п. информационное/ [information l.] — система соціальних норм і відносин, що виникають у сфері інформаційній і охороняються силою держави. Відносини, що виникають при здійсненні процесів інформаційних (відносини інформаційні), є основними об'єктами правового регулювання. Нормативну базу п. і. складає законодавство інформаційне. П. і. являє собою правовий фундамент суспільства інформаційного.

ПРИВАТНІСТЬ /приватность (частность)/ [privacy] (лат. privatus) — належність до особистого, неофі-

ційного, домашнього, несуспільного. Див. також конфіденційність.

П. даних /п. данных/ [data p.] — статус даних, що полягає в доступності даних тільки власникові або обмеженій групі користувачів; гарантована доступність даних із боку певної особи або групи осіб.

ПРИДУШЕННЯ /подавление/ [suppression] — заходи і дії спрямовані на те, щоб силою покласти кінець чому-небудь, знищити, заглушити.

П. активне небезпечних електричних сигналів акустоелектричних перетворювачів /активное п. опасных электрических сигналов акустоэлектрических преобразователей/ — придушення небезпечних електричних сигналів акустоелектричних перетворювачів шляхом генерування завад в радіодіапазоні (для просторового зашумлення) і звуковому діапазоні (для лінійного зашумлення).

П. вимиканням джерел небезпечних сигналів пасивне /п. отключением источников опасных сигналов пассивное/ — спосіб захисту інформації шляхом вимикання пристроїв із перетворювачами акустоелектричними в приміщеннях, де ведуться конфіденційні розмови. З цією метою в засобах зв'язку, наприклад, телефонних апаратах, постійно приєднаних до ліній зв'язку, встановлюються вимикачі. Більш зручними в експлуатації є спеціальні засоби захисту, що автоматично вимикають радіоелектронні засоби при відсутності у лінії сигналів. Подібні пристрої захисту вимикають гучномовці ретрансляційної мережі при відсутності сигналів мовлення або приєднують до телефонної лінії постійно від'єднане коло дзвінка телефонного апарата при появі в ній сигналу виклику.

П. небезпечних електричних сигналів акустоелектричних перетворювачів /п. опасных электрических сигналов акустоэлектрических преобразователей/ — вид запобігання витоку інформації через побічні випромінювання і наведення за межі зони контрольованої. Способи придушення можуть бути активними і пасивними. Перші забезпечують зменшення рівня небезпечних сигналів, другі — підвищення рівня завад.

П. пасивне буферними пристроями /п. пассивное буферными устройствами/ — спосіб захисту інформації шляхом застосування буферних підсилювачів, наприклад, між гучномовцем і лінією. Буферний

підсилювач пропускає без ослаблення і спотворення сигнали до гучномовця і на 60–120 дБ зменшує рівні небезпечних сигналів у зворотному напрямку.

П. пасивне небезпечних електричних сигналів акустоелектричних перетворювачів /п. пассивное опасных електрических сигналов акустоэлектрических преобразователей/ — придушення небезпечних електричних сигналів акустоелектричних перетворювачів шляхом зменшення рівня небезпечних сигналів, які можуть розповсюджуватися за межі контрольованої зони. Пасивне придушення здійснюється наступними способами: вимиканням джерел небезпечних сигналів; фільтрацією небезпечних сигналів; обмеженням величини небезпечних сигналів; буферними пристроями.

П. пасивне обмеженням величини небезпечних сигналів /п. ограничением величины опасных сигналов пассивное/ — спосіб захисту інформації, заснований на тому, що при проходженні через напівпровідникові обмежувачі знизу (пристрої, дія яких ґрунтується на нелінійних властивостях напівпровідникових елементів) небезпечні сигнали, що виникають в радіоелектронних засобах, що підлягають захисту, і мають малу амплітуду у порівнянні з корисним сигналом, додатково послаблюються в тисячі разів, а корисні сигнали проходять через обмежувач практично без послаблення. Поєднання обмежувача з фільтром використовується в пристроях комплексного захисту інформації шляхом придушення небезпечних побічних сигналів і сигналів високочастотного нав'язування.

П. пасивне фільтрацією небезпечних сигналів /п. пассивное фильтрацией опасных сигналов/ — спосіб захисту інформації шляхом відфільтровування небезпечних сигналів, якщо частоти небезпечних сигналів суттєво відрізняються від частот корисних сигналів. Найпростішим фільтром є конденсатор, встановлений у колі дзвінка телефонного апарата з електромеханічним дзвінком для шунтування небезпечних сигналів, що виникають в обмотці котушки якоря в результаті впливу на якір акустичних хвиль в звуковому діапазоні частот. Більш складні фільтруючі пристрої придушують більш високі частоти акустоелектричних перетворювачів у порівнянні з корисними сигналами годинників єдиного часу, охоронних і пожежних сигналізаторів та ін., а також забезпечують захист інформації в телефонних апаратах від високочастотного

нав'язування, не пропускаючи до них високочастотні електричні сигнали від генератора, приєднаного зловмисником до телефонної лінії.

П. радіоелектронне (РЕП) /п. радиоэлектронное (РЭП)/ [electronic s., jamming] — комплекс заходів і дій для порушення роботи або зниження ефективності застосування радіоелектронних засобів та систем противника шляхом дії на них завадами радіоелектронними; складова частина боротьби радіоелектронної. Включає радіопридушення, придушення оптико-електронне і придушення гідроакустичне. Об'єктами РЕП є засоби радіолокації, радіозв'язку, радіонавігації, лазерної, інфрачервоної, акустичної техніки та інші РЕЗ, що складають основу сучасних систем управління і розвідки. РЕП досягається створенням активних та пасивних завад, радіоблокадою, використанням фальшивих цілей, пасток і т. ін.

ПРИЙМАЧ /приемник/ [receiver] — апарат для приймання будь-чого (сигналів, мови, музики, зображення) за допомогою електромагнітних, акустичних та інших хвиль. П. виконує функцію, зворотні функції передавача. Він здійснює: вибір (селекцію) носія з необхідною для одержувача інформацією; підсилення прийнятого сигналу до значень, необхідних для знімання інформації; знімання інформації з носія (демодуляція, декодування); перетворення інформації в форму сигналу, доступну користувачу (людині, технічному пристрою).

П. акустичні /п. акустические/ [acouctic r.] — приймачі, які забезпечують селекцію акустичних сигналів, що розповсюджуються в атмосфері, воді, твердих тілах, перетворюють їх в сигнали електричні, підсилюють і обробляють електричні сигнали та перетворюють їх в хвилю акустичну (звукову) для сприйняття інформації системою слуховою людини. Крім того, електричні сигнали з виходу приймача можуть подаватися для реєстрації інформації на аудіомагнітофон. Типова структура п. а. містить мікрофон, селективний підсилювач, перетворювач електроакустичний, а також при необхідності аудіомагнітофон.

П. інфрачервоного випромінювання /п. инфракрасного излучения/ [detector of infrared radiation] — приймач оптичного випромінювання, чутливий до електромагнітного випромінювання в інфрачервоній

частині спектра.

П. інфрачервоного випромінювання тепловий /п. инфракрасного излучения тепловой/ — приймач інфрачервоного випромінювання, принцип дії якого ґрунтується на перетворенні енергії випромінювання інфрачервоного у теплову енергію, а потім в електричну.

П. інфрачервоного випромінювання фотонний /п. инфракрасного излучения фотонный/ — приймач інфрачервоного випромінювання, принцип дії якого ґрунтується на внутрішньому або зовнішньому фотоефекті.

П. небезпечних сигналів /п. опасных сигналов/ — приймачі, призначені для приймання радіо і електричних сигналів, що несуть мовну конфіденційну інформацію. Для приймання радіосигналів найчастіше застосовують скануючі приймачі. Для виділення, приймання, підсилення небезпечних електричних сигналів, що розповсюджуються телефонними, ретрансляційними і іншими лініями, застосовують селективні і спеціальні підсилювачі низької частоти. Спеціальні підсилювачі містять селективні елементи для виділення, наприклад, небезпечних сигналів із сигналів електроживлення, датчики для дистанційного знімання сигналів, а також мають конструкцію, зручну для перенесення і автономної роботи в різноманітних умовах потайного (прихованого) підслухування.

П. оптичний (П. оптичного випромінювання) /п. оптический (п. оптического излучения)/ [radiation r., detector of radiation] — прилад, призначений для використання його реакції на електромагнітне випромінювання оптичного діапазону. П. о. засобу спостереження в оптичному діапазоні включає оптичну систему, світлоелектричний перетворювач, підсилювач та індикатор. Оптична система або об'єктив проектує світловий потік від об'єкта спостереження на екран світлоелектричного перетворювача (сітківку ока, фотоплівку, фотокатод, мішень оптико-електронного перетворювача). На мішені оптичне зображення перетворюється в електронне зображення, кількість "вільних" електронів кожної точки якого є пропорційною яскравості відповідної точки оптичного зображення. Способи візуалізації зображення для різних типів п. о. можуть суттєво відрізнятися. Зображення у вигляді зорового образу формується у мозку людини,

на фотоплівці — в результаті хімічного оброблення світлочутливого шару, на екрані технічного засобу — шляхом послідовного або паралельного знімання електронів із мішені, підсилення електричних сигналів і формування під їхньою дією видимого зображення на екрані з люмінофором.

П. панорамний /п. панорамный/ [panoramic r.] (від грец. *πᾶν*... — все і ...*ὅραμα* — вид, видовище) — радіоприймач, який забезпечує швидке визначення завантаження заданого діапазону радіочастот, виявлення найбільш вільних його ділянок із метою вибору робочих частот, а також визначення деяких параметрів випромінювання радіопередавальних пристроїв (смуги частот, глибини і типу модуляції і т. ін.). Обстеження діапазону проводиться шляхом швидкого автоматичного перестроювання п. п. в межах діапазону за періодичним законом (кілька разів в секунду). Сигнали, що приймаються, сприймаються оператором або реєструються спеціальним записуючим пристроєм. П. п. використовується для радіорозвідки, в радіонавігації — для визначення літаком свого місцезнаходження відносно заданої дорожньої лінії за курсовими радіомаяками, розташованими вздовж траси літака та для інших цілей.

П. прямого підсилення /п. прямого усиления/ [direct amplification r.] — радіоприймач, в якому радіосигнал підсилюється на несучій частоті, тобто частотний спектр сигналу не змінюється при проходженні через усі високочастотні тракти, аж до детектора. П. п. п. складається з вхідного кола, високочастотного підсилювача, детектора і низькочастотного підсилювача (іноді і підсилювача потужності). П. п. п. у порівнянні з радіоприймачами супергетеродинними мають низьку селективність і меншу чутливість. П. п. п. часто застосовуються для пошуку і виявлення потужних сигналів малої тривалості, причому вони можуть бути як одноканальними, так і багатоканальними.

П. скануючий /п. сканирующий/ [scanning r.] — радіоприймач для перехоплення сигналів в широкому діапазоні частот. Особливістю с. п. є можливість дуже швидкого (електронного) перестроювання. Наявність у більшості с. п. пристрою “пам’яті”, який запам’ятовує попередньо введені, а також уведені в процесі пошуку, частоти радіосигналів, що мають інтерес для оператора, дозволяє значно скоротити час перегляду широкого діапазону частот. В с. п. передбачений інтерфейс сполучення з ПЕОМ, що дозволяє

автоматизувати пошук сигналів за заданими ознаками, в тому числі таких, що використовують прості види технічного закриття (див. комплекс радіоконтролю автоматизований та комплекси приймальні спеціальні).

П. спеціальні /п. специальные/ [special r.] — засоби радіоконтролю приміщень, призначені для оперативного пошуку радіозакладок. До них відносяться селективні мікровольтметри, приймачі скануючі, спектроаналізатори та приймачі з випромінювачами акустичних сигналів. Останні крім скануючого приймача містять випромінювач тестового акустичного сигналу і мікропроцесор. Випромінювач акустичного сигналу імітує джерело акустичної інформації. Мікропроцесор виявляє радіосигнали, на які настроюється скануючий приймач, за критерієм "свій-чужий" і швидко виявляє радіосигнал закладки, якщо такий існує.

П. супергетеродинний /п. супергетеродинный/ [superheterodyne r.] — радіоприймач, в якому сигнали, що приймаються, шляхом перетворення частоти несучої на проміжну частоту, на якій і здійснюється основне підсилення сигналу до детектування. П. с. можуть бути як з однократним, так і двократним перетворенням частоти. Як правило п. с. складаються з вхідного кола, гетеродина, змішувача, підсилювача проміжної частоти, детектора і низькочастотного підсилювача потужності. Для підвищення чутливості і селективності по дзеркальному каналу в п. с. високого класу може входити і високочастотний підсилювач з настроювальним коливальним контуром, що включається між вхідним колом і змішувачем.

П. цифровий /п. цифровой/ [digital r.] — радіоприймач, у якого сигнал перетворюється у цифровий вигляд з наступним його обробленням засобами обчислювальної техніки.

ПРИКРИТТЯ /прикрытие/ [cover] — захисне маскування, що застосовується по відношенню до людей, організації або об'єкту з метою приховування їхньої таємної діяльності або призначення, істинних цілей, мотивів, джерел фінансування і тих, хто за ними стоїть.

П. неофіційне /п. неофициальное/ — термін, що використовується по відношенню до співробітників розвідки, які працюють за кордоном без традиційного дипломатичного прикриття. Більшість розвідників знаходяться в країні перебування під захистом свого посольства і мають дипломатичну недоторканість. На випадок викриття такий розвідник, як правило, оголошується "персоною нон грата" і висилається з країни.

Розвідники, що працюють під п. н., не мають такого захисту і тому їхня діяльність зв'язана зі значно більш серйозним ризиком. Вони у більшості випадків не можуть користуватися посольськими каналами зв'язку, не мають можливості заховатися в посольстві у випадку провалу. Звичайно такі розвідники видають себе за бізнесменів, що займаються законною (вдавано законною) діяльністю. Вони тримаються осторонь від представників офіційних органів в країні перебування і "легальних" співробітників розвідки, що видають себе за дипломатів і формально підпорядковуються послові. Розвідники, що працюють під п. н., можуть проводити таємні операції, про які посол нічого не знає.

ПРИЛАДИ /приборы/ [devices] — спеціальні пристрої, пристосування, апарати для виконання якої-небудь роботи, керування, регулювання, контролю, спостереження за чим-небудь. Наприклад: вимірювальні прилади, електронні прилади, прилади оптичні і т. ін.

П. візуально-оптичні /визуально-оптические п./ — прилади для спостереження візуально-оптичного, призначені для збільшення розмірів зображення на сітківці ока. В результаті їхнього застосування підвищується дальність спостереження, ймовірність виявлення і розпізнавання дрібних об'єктів. До п. в.-о. відносяться бінокли, монокуляри, підзорні труби, спеціальні телескопи. П. в.-о. характеризуються коефіцієнтом збільшення (кратності). Проте при достатньо великому збільшенні кут зору приладу стає настільки малим, що важко утримувати зображення об'єкта в полі зору. Для стабілізації зображення п. в.-о. встановлюють на штативі або тринозі. В більш складних приладах застосовують електронну стабілізацію зображення, що забезпечує спостереження з рук або з транспорту, що рухається.

П. з перенесенням заряду /п. с переносом заряда/ — клас багатофункціональних напівпровідникових приладів, що містять сукупність однотипних елементів, розташованих на одній напівпровідниковій підкладці; дія заснована на переміщенні заряду, накопиченого в елементах, послідовно по ланцюжку цих елементів в напівпровіднику. Найбільш розповсюдженим різновидом таких приладів є прилади із зарядовим зв'язком.

П. із зарядовим зв'язком (ПЗЗ) /п. с зарядовой связью (ПЗС/ — основний тип приладу з перене-

сенням заряду, в основі роботи якого лежить принцип зберігання локалізованого заряду в потенціальних ямах, утворених в напівпровідникових кристалах унаслідок дії зовнішнього електричного поля, і передавання зарядових пакетів з однієї потенційної ями в іншу при зміні напруги на зовнішніх електродах. Основним елементом ПЗЗ є структура метал-оксид-напівпровідник або контакт з бар'єром Шотки. Елементи розташовані так близько один від іншого, що потенційні ями, утворені між сусідніми електродами, перекриваються і між ними можливий зарядовий зв'язок. ПЗЗ знаходять застосування у фоточутливих інтегральних схемах, в запам'ятовуючих пристроях і схемах аналогового і цифрового оброблення сигналів. З усіх пристроїв на ПЗЗ найбільше розповсюдження одержали однорядкові і матричні фоточутливі інтегральні схеми. Матричні схеми широко застосовуються в камерах телевізійних і апаратах фотографічних цифрових.

П. інфрачервоні /п. инфракрасные/ [infrared d.] — прилади, дія яких заснована на використанні випромінювання інфрачервоного. Розрізняють активні та пасивні п. і. Активні п. і. функціонують за принципом одержання інформації про об'єкти за відбитим від них промінням штучних джерел (прожекторів, лазерів інфрачервоного діапазону і т. ін.), пасивні — за відбитим промінням природних джерел (Місяць, зірки) або випромінюванням самих об'єктів. П. і. у військовій справі використовуються для спостереження, виявлення, пеленгування, автоматичного супроводження цілей, в головках самонаведення, для фотографування в інфрачервоному діапазоні, в наземному зв'язку та космічному.

П. контролю телефонних ліній /п. контроля телефонных линий/ — засоби контролю проводових ліній, призначені для запобігання підслухування телефонних розмов, в тому числі і за допомогою пристроїв закладних. Способи контролю телефонних ліній засновані на тому, що будь-яке приєднання до них викликає зміну електричних параметрів ліній: напруги і струму в лінії, значень ємності і індуктивності лінії, активного і реактивного опору. Для контролю телефонних ліній застосовуються наступні прилади: пристрої сповіщення світловим і звуковим сигналом про зменшення напруги в телефонній лінії, викликане несанкціонованим приєднанням засобів підслухування до лінії; вимірювачі характеристик телефонних лі-

ній (напруги, струму, ємності, опору і т. ін.), при відхиленні від яких формується сигнал тривоги; кабельні локатори, що дозволяють вимірювати неоднорідності телефонних ліній і визначати відстань до неоднорідності (асиметрії постійному струму в місцях приєднання підслуховуючих пристроїв, обриву, короткого замикання і т. ін.).

П. нічного бачення (ПНБ) /п. ночного видения (ПНВ)/ [night observation (viewing) d.] — прилад візуально-оптичного спостереження в інфрачервоній частині оптичного діапазону електромагнітного випромінювання. Основу п. н. б. складає електронно-оптичний перетворювач, який перетворює невидиме очима зображення об'єкта спостереження у видиме. П. н. б. ефективно працюють в умовах природного нічного освітлення, але не дозволяють здійснювати спостереження в повній темряві (при відсутності зовнішнього джерела світла). П. н. б. поділяють на три групи: прилади малої дальності дії (нічні окуляри), що дозволяють бачити фігуру людини на відстані 100–200 м; прилади (нічні біноклі, труби) середньої дальності (людина спостерігається до 300–400 м), спостереження ведеться з рук; прилади великої дальності дії (до 1000 м), що встановлюються для спостереження на тринозі або рухомому носії. За способом підсвічування п. н. д. поділяються на три типи: об'єкт спостереження підсвічується за допомогою штучного джерела інфрачервоного випромінювання, розташованого на п. н. б.; з підсвічуванням від природного освітлення; такі, що приймають власне теплове випромінювання об'єкта спостереження (див. тепловізор). За призначенням ПНБ поділяються на прилади спостереження і розвідки, приціли, прилади водіння машин. ПНБ мають неперископічну і перископічну конструкцію.

П. оптичні /п. оптические/ [optical d.] — технічні прилади, дія яких ґрунтується на хвильових властивостях світла, що дозволяє одержувати зображення об'єктів за допомогою оптичних систем (лінз, призм, дзеркал і т. ін.). Основними частинами п. о. є об'єктив і окуляр. За призначенням п. о. поділяються: на прилади спостереження; прилади вимірювання дальності; прилади вимірювання кутів, напрямків і перевищень; приціли і прилади для наводки; навігаційні прилади; прилади оптичного зв'язку; фотографічні прилади. Основні характеристики п. о.: збільшення, поле зору, величини вхідної і вихідної зіниць, віддале-

ння вихідної зіниці, світлосила, роздільна здатність, світлопропускання і світлорозсіювання і т. ін.

П. приймально-контрольний /п. приемно-контрольный/ — елемент комплексу технічних засобів охорони, призначений для приймання, оброблення і реєстрації сигналів тривоги, що поступають від сигналізаторів. П. п.-к. забезпечують: одночасне приймання сигналів тривоги від усіх об'єктів, що охороняються, з індикацією номера сигналізатора і поданням звукового сигналу; передавання сигналів тривоги на пульт централізованого спостереження; можливість збільшення ємності за рахунок додавання до базового складу лінійних блоків; автоматичний перехід на резервне автономне живлення на випадок від'єднання основного; формування сигналів оповіщення операторів на випадок обриву або короткого замикання шлейфів. П. п.-к. класифікуються за інформаційною ємністю (кількістю шлейфів, що приєднуються) і інформативністю (кількістю видів сигналізаторів). За інформативної ємністю вони бувають малої ємності (до 5 шлейфів), середньої (6–50 шлейфів і великої ємності (більше 50 шлейфів). П. п.-к. малої інформативності забезпечує роботу до 2-х видів сигналізаторів, середньої — від 3 до 5 видів сигналізаторів. П. п.-к. використовуються переважно для охорони одного об'єкта. Застосування мікропроцесорної техніки дозволяє розширити їхні функціональні можливості стосовно автоматизації контролю за станом сигналізаторів, адаптації до їхніх різноманітних характеристик, удосконалення алгоритмів оброблення сигналів. В п. п.-к. середньої і великої ємності передбачається можливість передавання сигналів на пульти централізованого спостереження каналами зв'язку.

П. радіаційної розвідки /п. радиационной разведки/ — див. засоби добування інформації про радіоактивні речовини.

ПРИНЦИП /принцип/ [approach, concept, principle] (від лат. principium — начало, основа) — першооснова; те, що лежить в основі певної теорії науки.

П. активності захисту інформації /п. активности защиты информации/ — принцип технічного захисту інформації, що визначає загальні вимоги до способів і засобів захисту інформації щодо прогнозування

дій зловмисника, розроблення і реалізації випереджаючих заходів захисту.

П. активності розвідки /п. активности разведки/ — принцип добування інформації, що передбачає активні дії всіх елементів системи розвідки при добуванні інформації, насамперед, пошук оригінальних способів і шляхів вирішення завдань стосовно до конкретних умов.

П. багатозональності захисту інформації /п. многозональности защиты информации/ — принцип технічного захисту інформації, що визначає диференційований доступ санкціонований різноманітних категорій користувачів до джерел інформації і реалізується шляхом розподілу простору, який займає об'єкт захисту, на зони контрольовані.

П. багаторубіжності захисту інформації /п. многорубежности защиты информации/ — принцип технічного захисту інформації, що проявляється у створенні на межах зон контрольованих одного або декількох рубежів захисту з метою запобігання проникнення зловмисника в зону. Особливістю захисту межі зони є вимога рівної міцності рубежів на межі і наявність контрольно-пропускних пунктів або постів, що забезпечують керування доступом в зону людей і транспорту. Рубежі зони створюються і всередині зони на шляху можливого пересування зловмисника або розповсюдження інших носіїв, насамперед, полів електромагнітних і акустичних. Наприклад, для захисту акустичної інформації від підслухування в приміщенні може бути встановлений рубіж захисту у вигляді акустичного екрана.

П. безперервності захисту інформації /п. непрерывности защиты информации/ — принцип технічного захисту інформації, що визначає загальні вимоги до способів і засобів захисту інформації щодо забезпечення готовності системи захисту до відбиття загроз безпеці інформації у будь-який час (безперервно).

П. вибору криптографічних методів /п. вибора криптографических методов/ — принцип формування політики в галузі криптографії, який передбачає для користувачів доступ до таких методів шифрування, які задовольняють їхні запити, в тому числі з безпеки і конфіденційності. Державний контроль над методами криптографії не повинен перевищувати необхідний для виконання своїх зобов'язань рівень.

Держава не повинна обмежувати вибір користувачів.

П. вивчення об'єктів психологічної війни /п. изучения объектов психологической войны/ — принципи, що лежать в основі методики вивчення об'єктів психологічної війни: принцип достатності; принцип діяльністного підходу; принцип соціально-конфесіонального підходу; принцип цілеспрямованості; принцип об'єктивності.

П. відповідності рівня захисту цінності інформації /п. соответствия уровня защиты ценности информации/ — принцип технічного захисту інформації, що визначає економічну доцільність застосування тих чи інших заходів захисту. Він полягає в тому, що витрати на захист не повинні перевищувати ціну інформації, що захищається.

П. гнучкості захисту інформації /п. гибкости защиты информации/ — принцип технічного захисту інформації, що проявляється у можливості зміни ступеня захищеності інформації у відповідності до зміни вимог до безпеки інформації. Ступінь захищеності інформації визначає рівень безпеки інформації.

П. довіри методам криптографії /п. доверия методам криптографии/ — принцип формування політики в галузі криптографії, який передбачає сприяння державних і приватних структур зростанню довіри до криптографічних методів захисту інформації.

П. діяльністного підходу /п. деятельностного подхода/ — принцип вивчення об'єктів психологічної війни, який орієнтує на одержання інформації про об'єкти шляхом аналізу змісту особистістно значимої для них діяльності (воєнної, професійної, життєвої і т. ін.). Тільки на основі аналізу діяльності людей можна зробити обґрунтовані висновки про їхню внутрішню сутність, зрозуміти мотивацію поведінки.

П. добування інформації /п. добывания информации/ — принципи, що лежать в основі добування інформації: цілеспрямованість розвідки; активність розвідки; безперервність розвідки; скритність розвідки; комплексне використання сил і засобів добування інформації.

П. достатності /п. достаточности/ — принцип вивчення об'єктів психологічної війни, що вимагає точного визначення того мінімуму інформації про противника, який необхідний і достатній для проведення

цієї чи іншої операції психологічної. Важливо знати, які конкретні психологічні особливості об'єктів психологічного впливу слід виявляти. Крім того, необхідно правильно визначити які методи і прийоми збирання інформації слід використати для вирішення поставленого завдання.

П. забезпечення інформаційно-психологічної безпеки /п. обеспечения информационно-психологической безопасности/ — окрім загальних принципів забезпечення інформаційної безпеки, чисто специфічними п. з. і.-п. б. є: державний і громадський контроль за створенням і використанням спеціальних засобів впливу на психіку людини; державна монополія на розроблення засобів і методів неусвідомлюваного інформаційного впливу; обов'язкове ліцензування (див. ліцензія) діяльності, зв'язаної з застосуванням засобів і методів неусвідомлюваного інформаційного впливу на психіку людини, а також їхня сертифікація; доступність експертизи психоекологічної.

П. забезпечення інформаційної безпеки /п. обеспечения информационной безопасности/ — законність, дотримання балансу інтересів особистості, суспільства і держави; взаємна відповідальність суб'єктів забезпечення безпеки; інтеграція систем національної і міжнародної безпеки. Чисто специфічними п. з. і. б. є: превентивність проведення заходів інформаційної безпеки по відношенню до заходів інших видів безпеки, а також інформованість об'єктів безпеки адекватна, в тому числі і міжнародних.

П. законності доступу /п. законности доступа/ — принцип формування політики в галузі криптографії, який передбачає наявність законного доступу до ключів шифрування. Процес одержання доступу до цих ключів повинен бути юридично оформленим і передбачати процедури незалежного аудита.

П. захисту таємниці особистого життя і персональних даних /п. защиты тайны личной жизни и персональных данных/ — принцип формування політики в галузі криптографії, який передбачає використання методів криптографії як цінного засобу для захисту таємниці особистого життя, включаючи як конфіденційність даних і повідомлень, так і захист персональних даних.

П. інформаційної боротьби /п. информационной борьбы/ — науково обґрунтовані положення, правила, рекомендації з підготовки і ведення боротьби інформаційної, керівництва її силами і засобами. Ство-

рюються на основі законів і закономірностей, а також досвіду, набутого в результаті практичної діяльності в галузі інформаційної боротьби. П. і. б. не тільки відображають об'єктивну сутність, але і приписують, як слід діяти в конкретних умовах. Зміст і масштаби завдань інформаційної боротьби передбачають наявність цілої множини п. і. б. Воєнна наука керується насамперед принципами, що витікають із законів діалектики, із загальних законів і закономірностей соціального розвитку. Разом з тим вона опрацьовує свої специфічні принципи, що відображають, головним чином, закономірності інформаційної боротьби. До таких принципів відносяться: принцип відповідності (підпорядкованості) цілей і завдань інформаційної боротьби політичним цілям; принцип необхідності зосередження сил та засобів інформаційної боротьби у вирішальному місці у вирішальний момент; принцип завчасної підготовки сил і засобів інформаційної боротьби; принцип постійної готовності сил і засобів інформаційної боротьби до захисту власної інформації і до руйнівного впливу на інформаційне середовище противника; принцип високої активності і рішучості дій; принцип узгодженого спільного застосування всіх сил і засобів інформаційної боротьби; принцип безперервності інформаційної боротьби; принцип ведення інформаційної боротьби з напруженням, необхідним вирішення поставлених завдань; принцип своєчасного маневру силами і засобами інформаційної боротьби; принцип раптовості, застосування несподіваних для противника способів виконання завдань; принцип врахування духовного фактора в інтересах виконання поставлених завдань; принцип усебічного забезпечення, підтримки боєздатності і своєчасності відновлення сил і засобів інформаційної війни; принцип твердості і безперервності управління силами і засобами інформаційної боротьби, непохитності в досягненні поставленої мети, виконанні прийнятих рішень і поставлених завдань.

П. комплексного використання сил і засобів добування інформації /п. комплексного использования сил и средств добывания информации/ — принцип добування інформації, що передбачає комплексне використання способів і засобів її добування, які достатньо ефективні в одних умовах і не завжди призводять до позитивних результатів в інших умовах. Крім того, комплексний підхід забезпечує дублювання

даних, що є основним напрямком підвищення достовірності інформації.

П. комплексного використання способів і засобів захисту інформації /п. комплексного использования способов и средств защиты информации/ — принцип технічного захисту інформації, що визначає загальні вимоги до захисту інформації, спрямовані на використання різноманітних способів і засобів захисту, які дозволяють компенсувати недоліки одних перевагами інших.

П. міжнародної координації і кооперації /п. международной координации и кооперации/ — принцип формування політики в галузі криптографії, який передбачає міжнародну кооперацію й координацію з метою недопущення виникнення нездоланних бар'єрів для торгівлі.

П. об'єктивності /п. объективности/ — принцип вивчення об'єктів психологічної війни, який вимагає, щоб вивчення об'єктів здійснювалося на основі всебічно перевірених фактів, що зіставлені між собою. Не можна допускати упередженість у тлумаченні, поясненні й оцінці цих фактів, а тим більше виходити зі своїх домислів і гіпотез.

П. підготовки й проведення психологічних операцій /п. подготовки и проведения психологических операций/ — принципи, що лежать в основі підготовки й ведення війни психологічної: підготовка операцій психологічних повинна починатися заздалегідь, скрито, ретельно, з врахуванням індивідуальних і соціально-психологічних особливостей об'єктів впливу; психологічні операції планують і проводять з врахуванням виявлення слабких місць в морально-психологічному стані населення й особового складу військ противника, з урахуванням особливостей воєнно-політичної і оперативної обстановки, наявних сил та засобів; відповідні начальники органів психологічної війни особисто відповідають за проведення й ефективність психологічних операцій, а також за використання сил і засобів, що знаходяться в їхньому розпорядженні; психологічні операції різноманітних видів проводять за єдиним планом, узгоджують між собою, а також з бойовими діями військ; всі сили й засоби психологічних операцій необхідно використовувати масовано, комплексно й різноманітно.

П. побудови хибного об'єкта атаки /п. построения ложного об'єкта атаки/ — принципи, що лежать в

основі реалізації об'єкта атаки хибного (ХОА): візуальна подібність об'єктові атаки, включаючи інтерфейс взаємодії з користувачами (а, відповідно, і з противником) і формати даних вводу-виводу; розвинений інтерфейс з суб'єктом інформаційної боротьби (адміністратором мережі або оператором системи безпеки); керованість ХОА зі сторони суб'єкта інформаційної боротьби; модульність побудови ХОА, що забезпечує можливість його нарощування й оперативної реконфігурації.

П. рівної інформаційної безпеки /п. равной информационной безопасности/ — те ж що інформованість держав світового співтовариства адекватна.

П. розвитку криптографічних методів у відповідності до вимог ринку /п. развития криптографических методов в соответствии с требованиями рынка/ — принцип формування політики в галузі криптографії, який передбачає реалізацію розроблення й надання методів криптографії в умовах відкритого ринку. Такий підхід дає упевненість в тому, що рішення відповідають технічному прогресу й запитам користувачів.

П. системного підходу /п. системного подхода/ — принципи, що лежать в основі системного підходу: будь-яка система є підсистемою більш складної системи, яка впливає на структуру і функціонування системи, що розглядається; будь-яка система має ієрархічну структуру, елементами і зв'язками якої не можна нехтувати без достатніх підстав; при аналізі системи необхідне врахування зовнішніх і внутрішніх факторів впливу, прийняття рішень на основі невеликого числа факторів без розгляду решти факторів може призвести до нереальних результатів; накопичення і об'єднання властивостей елементів системи призводить до появи якісно нових властивостей, що відсутні у її елементів.

П. скритності захисту інформації /п. скрытности защиты информации/ — принцип технічного захисту інформації, що визначає загальні вимоги до способів і засобів захисту інформації, спрямовані на виключення ознайомлення сторонніх осіб із засобами і технологією захисту інформації.

П. скритності розвідки /п. скрытности разведки/ — принцип добування інформації, який передбачає таємне проведення заходів з підготовки і добування інформації та приховання фактів витоку або зміни

інформації. Реалізація цього принципу дозволяє розвідці підвищити безпеку органу добування та виграти час для більш ефективного застосування інформації, що добувається.

П. соціально-конфесіонального підходу /п. социально-конфессионального подхода/ — принцип вивчення об'єктів психологічної війни, який вимагає вивчення об'єктів шляхом аналізу особливостей їхнього соціально-економічного, релігійного, етнічного і правового положення. Звичайно існують суттєві психологічні відмінності між представниками різноманітних груп людей, які можна умовно виділити на основі вказаних ознак.

П. стандартизації методів криптографії /п. стандартизации методов криптографии/ — принцип формування політики в галузі криптографії, який передбачає узгоджений розвиток національних і міжнародних стандартів криптографії.

П. технічного захисту інформації /п. технической защиты информации/ — принципи, що лежать в основі технічного захисту інформації. Поділяються на дві групи: принципи, що визначають загальні вимоги до способів і засобів захисту інформації; принципи, що визначають підходи до організації та забезпечення захисту інформації. До принципів першої групи відносяться принципи, аналогічні принципам добування інформації: принцип безперервності захисту інформації; принцип активності захисту інформації; принцип скритності захисту інформації; принцип цілеспрямованості захисту інформації; принцип комплексного використання способів і засобів захисту інформації. Принципи другої групи дозволяють забезпечити раціональний рівень захисту інформації та скоротити витрати її організації. Ця група включає наступні принципи: принцип відповідності рівня захисту цінності інформації; принцип гнучкості захисту інформації; принцип багатозональності захисту інформації; принцип багаторубіжності захисту інформації. Крім указаних принципів при побудові конкретної системи захисту доцільно враховувати також наступні принципи: мінімізація додаткових завдань і вимог до співробітників організації, викликаних заходами захисту інформації; надійність в роботі технічних засобів системи, яка би виключала як нереагування на загрози безпеці (пропуски загроз) інформації, так і на реакції при їхній відсутності; обмежений і контрольований доступ

до елементів системи забезпечення безпеки інформації; безперервність роботи в будь-яких умовах функціонування об'єкта захисту, в тому числі при короткочасному вимкненні електроенергії; адаптованість (пристосованість) системи до змін навколишнього середовища. Реалізація вказаних принципів в системі захисту дозволять наблизити її до абсолютної, тобто забезпеченої усіма можливими способами захисту і здатної в будь-який момент свого існування прогнозувати настання загрозливої події за час, достатній для приведення в дію адекватних заходів.

П. Фейстела /п. Фейстела/ — див. шифр Фейстеловського типу.

П. формування політики в галузі криптографії /п. формирования политики и области криптографии/— принципи, які рекомендуються для керівництва при реалізації криптографічних методів захисту інформації в державі та в міждержавних відносинах. До таких принципів можна віднести наступні принципи: принцип довіри методам криптографії; принцип вибору криптографічних методів; принцип розвитку криптографічних методів у відповідності до вимог ринку; принцип стандартизації методів криптографії; принцип захисту таємниці особистого життя і персональних даних; принцип законності доступу; принцип відповідальності за надання криптографічних послуг; принцип міжнародної координації і кооперації.

П. цілеспрямованості /п. целенаправленности/ — принцип вивчення об'єктів психологічної війни, що припускає наявність чітко визначеної мети, відповідно до якої організовується вивчення об'єктів впливу психологічного. Як правило, цією метою повинно бути розкриття їхньої внутрішньої сутності: світогляду, потреб, мотивів і установок діяльності, специфіки поведінки. Виходячи з чітко поставленої мети, складається план і програма вивчення об'єктів психологічного впливу, які дозволяють виявити саме ті особистістні і групові психологічні особливості, які визначені поставленою метою.

П. цілеспрямованості захисту інформації /п. целеустремленности защиты информации/ — принцип технічного захисту інформації, що визначає загальні вимоги до способів і засобів захисту інформації

щодо зосередження зусиль на запобігання загроз найбільш цінній інформації.

П. цілеспрямованості розвідки /п. целеустремленности разведки/ — принцип добування інформації, який передбачає визначення завдань і об'єктів розвідки, ведення її за єдиним планом і зосередження зусиль органів розвідки на виконання основних завдань.

ПРИСТРІЙ /устройство/ [device, unit] — конструктивно закінчена технічна система, що має певне функціональне призначення.

П. верифікації голосу /у. верификации голоса/ — пристрій, призначений для ідентифікації користувачів за характеристиками голосових зв'язок.

П. закладні /у. закладные/ — пристрої для потайного підслухування. Забезпечують суттєве підвищення дальності підслухування. Перед підслухуванням потай установлюються в приміщенні зловмисниками. Створюють серйозні загрози безпеці мовної інформації практично в будь-яких приміщеннях, в тому числі в салоні автомобіля. За видом носія інформації від з. п. до зловмисника поділяються на пристрої закладні проводові і випромінюючі.

П. закладні випромінюючі /у. закладные излучающие/ — пристрої закладні, носієм інформації від яких є електромагнітне випромінювання в радіо- і оптичному діапазонах, що є їхньою демаскуючою ознакою. В залежності від виду первинного сигналу п. з. в. (в першу чергу це стосується радіозакладок) поділяються на апаратні і акустичні. За діапазоном частот закладні пристрої надзвичайно різноманітні. Для більш ніж 96% радіозакладок робочі частоти зосереджені в інтервалі 88–501 МГц, причому з частотами 92,5–169,1 виготовляються 42%, а з частотами 373,4–475,5 МГц — 52% закладок. Найбільш інтенсивно використовується діапазон 449,7–475,5 МГц, в якому зосереджені робочі частоти 36% зразків. Продовжується тенденція подальшого підвищення частот, в тому числі з переходом в ГГц діапазон. Це дозволяє зменшити рівень завад, понизити потужність передавача і, відповідно, його габарити, а також довжину антени. Для підвищення скритності для п. з. в. освоюється інфрачервоний діапазон електромагнітного випромінювання. Крім діапазону на умови передавання інформації закладкою впливає стабільність частоти її передавача. В

залежності від цього п. з. в. можуть бути з нестабілізованою частотою, з "м'якою" стабілізацією частоти і з "жорсткою" стабілізацією частоти. Іншою проблемою, що виникає при застосуванні п. з. в., є забезпечення закладок енергією протягом часу підслухування. В залежності від цього в. з. п. можуть бути з автономним живленням, з живленням від електромережі, з живленням від електроапаратів, з живленням від зовнішнього джерела електромагнітного випромінювання. Оперативне застосування п. з. в. полягає в раціональному розташуванні закладок в приміщенні або в радіоелектронному засобі. При цьому повинно забезпечуватися: надходження на вхід закладки сигналу з рівнем, необхідним для якісного передавання звукової або іншої інформації; скритність розташування і роботи закладки протягом часу, необхідного для підслухування. Встановлення закладних пристроїв можливе із заходом зловмисника в приміщення, де здійснюється їхнє розташування, або без заходу за допомогою спеціальних пристроїв.

П. закладні випромінюючі акустичні /у. закладные излучающие акустические/ — пристрої закладні випромінюючі, вхідними сигналами для яких є акустичні (найчастіше мовні) сигнали. До складу п. з. в. а. входять наступні основні функціонально необхідні пристрої: мікрофон, мікрофонний підсилювач, генератор несучої частоти, модулятор, підсилювач потужності і антена. Мікрофон перетворює акустичний сигнал з інформацією в електричний, який підсилюється до рівня входу модулятора. В модуляторі здійснюється модуляція коливань несучої частоти, тобто здійснюється перезапис інформації на високочастотний сигнал. Для забезпечення необхідної потужності проміння модульований сигнал підсилюється в підсилювачі потужності. Випромінювання радіосигналу у вигляді електромагнітної хвилі здійснюється антеною, як правило, у вигляді відрізка проводу. З метою зменшення ваги, габаритів і енергоживлення в закладці вказані функції реалізуються мінімально можливою кількістю активних і пасивних елементів.

П. закладні випромінюючі апаратні /у. закладные излучающие аппаратные/ — пристрої закладні випромінюючі, вхідними сигналами для яких є електричні сигнали, що несуть мовну інформацію (в телефонних апаратах), або інформаційні послідовності, що циркулюють в ПЕОМ при обробленні конфіденційної інформації. В таких закладках відсутній мікрофон, що значно спрощує їхню конструкцію, і існує

можливість використання для електроживлення енергії засобу, в якому встановлена закладка.

П. закладні проводові /у. закладные проводные/ — пристрої закладні, носієм інформації від яких є електричний струм, який розповсюджується електричними проводами. Поділяються на пристрої закладні проводові акустичні і пристрої закладні проводові ретранслюючі.

П. закладні проводові акустичні /у. закладные проводные акустические/ — пристрої закладні проводові, в яких для перетворення акустичних мовних сигналів в електричні використовуються мікрофони. Проводові акустичні закладки найчастіше являють собою субмініатюрні мікрофони, потай встановлені в побутових радіо- і електроприладах, в меблях і предметах інтер'єру і з'єднані тонким проводом з мікрофонним підсилювачем або аудіомагнітофоном, які розташовуються в інших приміщеннях; мініатюрні пристрої, що мають мікрофон, підсилювач і формувач сигналу, який передається, як правило, телефонними лініями і колами електроживлення. П. з. п. а. мають високу чутливість і завадостійкість, проте наявність проводу демаскує закладки і ускладнює їхню установку, особливо в умовах дефіциту часу. Закладки, що використовують кола електроживлення, розташовуються в місцях приєднання проводів електроживлення до вимикачів і мережних розеток.

П. закладні проводові ретранслюючі /у. закладные проводные ретранслирующие/ — пристрої закладні проводові, які ретранслюють електричні сигнали з мовною інформацією, що передаються телефонною лінією.

П. закладні програмні /у. закладные программные/ — програми типу бомба логічна, "троянський кінь", що заздалегідь впроваджуються в інформаційні системи і приводяться в дію за відповідним сигналом (навіть із супутника) або у встановлений час з метою знищення (модифікації), одержання інформації або ураження ЕОМ.

П. запам'ятовучий (ЗП) /у. запоминающее(ЗУ)/ [storage u.] — пристрій, що реалізує функцію пам'яті даних; пристрій, призначений для запису, зберігання і відтворення інформації.

П. запам'ятовуючий оперативний (ОЗП) /у. запоминающее оперативное (ОЗУ)/ — див. пам'ять

оперативна.

П. запам'ятовуючий постійний (ПЗП) /у. запоминающее постоянное (ПЗУ)/ [Read-Only Memory (ROM)] — 1) Пристрій запам'ятовуючий, який не здатний виконувати операцію запису даних. 2) Запам'ятовуючий пристрій, що безпосередньо зв'язаний з процесором центральним і призначений для даних, які оперативно беруть участь у виконанні арифметико-логічних операцій.

П. запам'ятовуючий постійний програмований (ППЗП) /у. запоминающее постоянное программируемое (ППЗУ)/ [Programmable Read-Only Memory (PROM)] — пристрій запам'ятовуючий постійний, в якому запис або зміна даних здійснюється шляхом електричної, магнітної або світлової дії на запам'ятовуючі елементи згідно заданої програми. Розрізняють ППЗП з однократним записом і ППЗП, що стираються.

П. зовнішній (периферійний) /у. внешнее (периферийное)/ [external (peripheral) d. (u.)] — пристрій, який виконує зовнішні функції машинного оброблення інформації (на відміну від внутрішніх функцій, які виконуються процесором центральним); пристрій, приєднаний до комп'ютера і працює під його управлінням.

П. захисту електронний /у. защиты електронное/ — електронний пристрій у складі комп'ютера, що виконує функції замка, відповідача і т.ін. і призначений для захисту програми та даних від несанкціонованого доступу.

П. захисту технічний /у. защиты техническое/ [physical protection d.] — пристрій захисту електронного чи іншого типу, що запобігає можливості роботи з програмою осіб, які не мають такого пристрою.

П. зчитування відбитків пальців /у. считывания оттисков пальцев/ — пристрій, призначений для ідентифікації користувачів за відбитками пальців.

П. ідентифікації особистості за геометрією руки /у. идентификации личности по геометрии руки/ — засіб ідентифікації людей, допущених в зону контрольовану або до носіїв інформації, призначений для визначення відповідності ідентифікаційного номера санкціонованої особистості із силуетом її руки, що

зберігається у пам'яті ЕОМ.

П. ідентифікації особистості за голосом /у. идентификации личности по голосу/ — засіб ідентифікації людей, допущених в контрольовану зону або до носіїв інформації на основі пристрою верифікації голосу, який спрацьовує при виголошенні санкціонованою особистістю кодового слова доступу до об'єкта.

П. ідентифікації особистості за динамікою підпису /у. идентификации личности по динамике подписи/ — засіб ідентифікації людей, допущених в зону контрольовану або до носіїв інформації, для визначення відповідності ідентифікаційного номера санкціонованої особистості з геометричними або динамічними ознаками рукописного відтворення підпису у реальному масштабі часу, що зберігаються у пам'яті ЕОМ. Особі, що перевіряється, пропонується написати своє прізвище або інше слово на спеціальній пластині, що перетворює зображення слова в еквівалентний електричний сигнал з наступним вимірюванням характеристик письма, накреслення підпису, інтенсивності кожного зусилля при написанні букв і швидкості завершення написання.

П. ідентифікації особистості за рисунком капілярних ліній пальця /у. идентификации личности по рисунку капиллярных линий/ — засіб ідентифікації людей, допущених в зону контрольовану або до носіїв інформації на основі ЕОМ і пристрою зчитування відбитків пальців, призначений для визначення відповідності ідентифікаційного номера санкціонованої особистості з рисунком капілярних ліній її пальців, що зберігаються в пам'яті ЕОМ.

П. ідентифікації особистості за узорами сітківки очей /у. идентификации личности по узорам сетчатки глаз/ — засіб ідентифікації людей, допущених в зону контрольовану або до носіїв інформації, призначений для визначення відповідності ідентифікаційного номера санкціонованої особистості з узорами сітківки її очей, які одержують за допомогою сканування оптичною системою сітківки одного або обох очей і вимірювання кутового розподілу кровоносних судин на поверхні сітківки відносно сліпої плями ока та інших ознак. Усього нараховується 250 ознак. Такі пристрої забезпечують високу достовірність

ідентифікації, проте потребують від людини фіксації погляду на об'єктиві сканера.

П. пам'яті /у. памяти/ [storage d.] — пристрій для запису, зберігання і зчитування даних.

П. підкладний /у. подкладное/ [secret intelligence d.] — див. закладка.

П. реєструючі /у. регистрирующие/ [recording d.] — пристрої, призначені для реєстрації (запису, запам'ятовування) сигналів з добутою в процесі перехоплення інформацією. Реєстрація сигналів здійснюється шляхом аудіо- і відеозапису, запису на магнітні й оптичні диски, на звичайному, електрохімічному, термочутливому і світлочутливому папері, запам'ятовування в пристроях напівпровідникової і інших видів пам'яті, фотографування зображень на екранах моніторів ПЕОМ, телевізійних приймачів, осцилографів, спектроаналізаторів.

ПРИХОВУВАННЯ /скрытие/ [hiding] — утаювання будь-чого для того, щоб воно не виявлялося явно.

П. активне /с.активное/ [active h.] — приховування інформації шляхом формування таких фізичних полів та речовин, які ускладнюють одержання інформації або створюють невизначеність її змісту.

П. енергетичне /с. энергетическое/ [energy h.] — приховування інформації, що передбачає застосування способів і засобів захисту інформації, які виключають або утруднюють виконання енергетичної умови контакту розвідувального. П. е. досягається зменшенням відношення енергії (потужності) сигналів, тобто носіїв (електромагнітного або акустичного полів і електричного струму) з інформацією, і завад. Зменшення відношення сигнал/завада здійснюється двома методами: пониженням потужності (ослаблення) сигналу або збільшенням потужності завади (зашумлення) на вході приймача.

П. енергетичне акустичних сигналів /с. акустических сигналов энерегетическое/ — спосіб протидії підслухуванню шляхом застосування способів і засобів, що зменшують енергію носія або збільшують енергію завад. Перший метод приховування акустичних сигналів реалізується за допомогою засобів звукоізоляції акустичного сигналу, засобів звукопоглинання акустичної хвилі та засобів глушення акустичних сигналів. Другий метод — засобами зашумлення приміщень або твердого середовища розповсюдження ін-

шими широкосмуговими звуками (шумами, завадами), що забезпечують маскування акустичних сигналів.

П. енергетичне акустичної інформації від підслухування лазерним мікрофоном /с. энергетическое акустической информации от подслушивания лазерным микрофоном/ — спосіб протидії підслуховуванню засобами лазерного підслухування. Приховування пасивне енергетичне акустичної інформації від підслухування лазерним мікрофоном полягає в послабленні енергії акустичної хвилі, що діє на віконне скло. Воно досягається використанням штор і жалюзі, а також подвійних віконних рам. Приховування активне енергетичне акустичної інформації передбачає застосування вібраційних генераторів шуму в акустичному діапазоні, датчики якого приклеюються до скла і викликають його коливання по випадковому закону з амплітудою, що перевищує амплітуду коливань скла від акустичної хвилі.

П. енергетичне в оптичному діапазоні /с. энергетическое в оптическом диапазоне/ — приховування ознак демаскуючих об'єктів шляхом зменшення яскравості об'єкта і фону нижче чутливості ока або технічного фотоприймача, а також їхнє засліплення. Найбільш природним способом енергетичного приховування є проведення заходів, що потребують захисту інформації про них, уночі. Яскравість об'єктів, які мають штучні джерела світла, понижується шляхом їхнього вимикання або екранування світлонепроникливими шторами і екранами. Енергетичне приховування об'єктів, що спостерігаються у відбитому світлі, забезпечують штучні оптичні маски, а також аерозолі природні і штучні в середовищі розповсюдження. Слід також враховувати, що при спостереженні в інфрачервоній частині оптичного діапазону з'являється додаткова демаскуюча ознака об'єкта, що не виявляється у видимій частині діапазону — температура поверхні відносно температури фону. В такому випадку для приховування об'єкта додатково використовуються теплоізолюючі екрани, в тому числі листя дерев і кущів, сіно, брезент та інші матеріали. Добрі теплоізолюючі властивості мають також повітряні піни.

П. енергетичне об'єкта від радіолокаційного спостереження /с. энергетическое объекта от радиолокационного наблюдения/ — вид протидії радіолокаційному спостереженню за рахунок зменшення ефективної поверхні розсіювання об'єкта. П. е. о. р. с. досягається зміною діаграми спрямованості відби-

ваючої поверхні об'єкта і поглинанням опромінюючої енергії РЛС. Зменшення відбитої енергії для об'єкта, що належить захисту від радіолокаційного спостереження, повинно передбачатися ще при його створенні шляхом виключення на поверхні об'єкта площин, що створюють кутові відбивачі. Готові об'єкти, що мають поверхні складної форми з різкими переходами, доцільно прикривати екранами, що спотворюють і відхиляють діаграму спрямованості об'єктів, найкраще кулястої форми. Для енергетичного приховування об'єктів від радіолокаційного спостереження його поверхню також покривають матеріалами радіопоглинаючими.

П. інформації /с. информации/ — спосіб технічного захисту інформації, що полягає у виключенні або суттєвому утрудненні несанкціонованого одержання інформації.

П. інформаційне /с. информационное/ — приховування інформації, яке досягається зміною портрета інформаційного або створенням неправдивого (хибного) інформаційного портрета семантичного повідомлення, фізичного об'єкта або сигналу (див. метод інформаційного приховування). Для зміни інформаційного портрета семантичного повідомлення може застосовуватися, наприклад, перетворення криптографічне інформації. Для створення хибного інформаційного портрета семантичного повідомлення можуть використовуватися методи стеганографії.

П. інформаційне мовної інформації /информационное с. речевой информации/ — спосіб протидії підслухуванню, заснований на зміні мовних повідомлень таким чином, щоб вони стали нерозбірливими для слухової системи людини, або на створенні неправдивих (хибних) мовних повідомлень. П. і. м. і. передбачає: закриття технічне і шифрування цифрове семантичної мовної інформації в функціональних каналах зв'язку; дезінформування (розповсюдження акустичними або складеними каналами витоку фальшивої семантичної мовної інформації.

П. інформаційне об'єкта радіолокаційного спостереження /с. информационное объекта радиолокационного наблюдения/ — спосіб протидії радіолокаційному спостереженню, що забезпечує руйнування структури радіолокаційного зображення об'єкта. Реалізується шляхом покриття об'єкта радіовідбивальними оболонками і екранами з іншою конфігурацією ніж об'єкт, розташуванням поряд з об'єктом додаткових

відбивачів, а також генеруванням радіозавад.

П. об'єкта радіолокаційного спостереження в завадах /с. объекта радиолокационного наблюдения в помехах/ — вид протидії радіолокаційному спостереженню, заснований на генерації завад радіолокаційних.

П. пасивне /с. пассивное/ [passive h.] — приховування інформації шляхом ослаблення енергетичних характеристик фізичних полів або зниження концентрації речовин.

ПРИЧЕТНІСТЬ /причастность/ [non-repudiation] — властивість системи оброблення інформації, яка полягає в тому, що суб'єкти системи захищені від заперечення причетності до утворення або передачі інформації та заперечення причетності до одержання інформації.

ПРОБЛЕМА /проблема/ [problem] (від грец. $\pi\rho\acute{o}\beta\lambda\eta\mu\alpha$ — задача, утруднення) — складне теоретичне або практичне питання, що потребує розв'язання, вивчення, дослідження.

П. дискретного логарифма /п. дискретного логарифма/ — задача обчислення логарифма дискретного, яка формулюється наступним чином: "Нехай відомі $\alpha, A \in M$, де M — деяка алгебраїчна структура. Знайти таке $x \in M' \subset M$, що $\alpha^x = A$." Найбільш вивчена задача дискретного логарифма коли M є полем, а α — породжуючий елемент мультиплікативної групи поля, але в сучасних системах цифрового підпису (наприклад, системі Шнорра, DSS, ГОСТ Р34.10) використовується варіант задачі, в якому M є підгрупою "великого" порядку мультиплікативної групи деякого поля, а α — її породжуючим елементом. Ефективних (поліноміальних за часом) алгоритмів вирішення цих задач невідомо (за винятком деяких спеціальних випадків, як в алгоритмі Поліга-Хеллмана), тому вони є основою для побудови важкооборотних функцій та функцій важкооборотних з секретом. На складності вирішення цієї задачі засновані криптосистеми асиметричні Ель-Гамаля, схема розповсюдження ключів Діффі-Хеллмана та інші.

П. електронної торгівлі /п. электронной торговли/ — сукупність проблем, що виникають при широкомасштабному впровадженні електронної торгівлі: фінансові (митні і податкові збори, електронні системи оплати); правові (універсальний торговельний код для торгівлі в Інтернеті, захист інтелектуальної вла-

сності, таємниці особистого життя, безпека торговельних операцій); доступ до ринку (телекомунікаційні інфраструктури і їхня взаємодія, зміст, технічні стандарти).

П. психофізична /п. психофизическая/ — у широкому розумінні — питання про відношення психічних явищ до фізіологічних, у вузькому — про співвідношення між психічними й фізіологічними процесами.

П. факторизації (розклад цілого числа на множники) /п. факторизации (разложение целого числа на множители/ [factorization p.] — задача обчислення дільників цілого числа, яка формулюється наступним чином: "Нехай відоме $N \in Z$. Знайти такі прості числа p_i та числа $e_i, i \in /1, ..., k/$, що $N = p_1^{e1} \cdot p_2^{e2} ... p_k^{ek}$." В криптографії використовується частковий вид цієї задачі, коли $N = p \cdot q$, $p \approx q$, а p, q — прості числа, які задовольняють спеціальним вимогам або є числами простими сильними. Ефективного (поліноміальних за часом) алгоритму вирішення останньої задачі невідомо, тому на складності її вирішення засновані криптосистеми асиметричні RSA, Люка, Рабина та інші.

ПРОВАЙДЕР /провайдер/ (від англ. provide — забезпечувати) — організація, що надає послуги доступу до Інтернету. Умови підключення визначаються договором, що укладається з користувачем.

ПРОВАЛ /провал/ [exposure] — викриття учасників, об'єктів (наприклад, квартири конспіративної) або яких-небудь інших елементів розвідувальної операції або організації.

ПРОВОКАЦІЯ /провокация/ [provocation] (від лат. provocatio — виклик) — навмисні дії проти окремих осіб, організацій, розвідувальних служб або урядів країн тощо з метою підбурити їх на згубні для них учинки або рішення. Агент-провокатор, як правило, вдається до розповсюдження фальшивих відомостей, дезінформації.

ПРОГРАМА /программа/ [program, routine] (від грец. $\pi\rho\acute{o}\gamma\rho\alpha\mu\mu\alpha$ — публічна об'ява, розпорядження) — 1) Наперед продуманий план якої-небудь діяльності, роботи і т.ін. 2) Дані, призначені для управління конкретними компонентами системи оброблення даних з метою реалізації певного алгоритму. 3) Впорядкована послідовність команд, яка підлягає обробленню; послідовність речень мови програмування, яка описує

алгоритм вирішення задачі. 4) Зміст передач усного, радіо і телевізійного мовлення.

П. Pretty Good Privacy (PGP) /п. Pretty Good Privacy (PGP) /[PGP p.] — комп'ютерна програма Філіпа Зіммермана для захисту пошти електронної та файлів. Перші версії програми використовували алгоритми DES, IDEA для шифрування та RSA (з довжиною ключа від 256 до 2047 біт) і MD5 для організації підпису цифрового. Для генерації відкритих ключів застосовувалися ймовірнісні тести на простоту, генератор псевдовипадкової послідовності ініціювався від клавіатури ЕОМ. Ключі сеансові для IDEA генерувалися за методом, описаним в ANSI 9.17. В останніх версіях під операційні системи Windows 95/98/NT/2000 з'явилася можливість вибору схеми цифрового підпису відповідно DSS та схеми розповсюдження ключів Діффі-Хелмана з довжиною ключа від 512 до 4096 біт. Генератор псевдовипадкової послідовності ініціюється від декількох джерел фізичної випадковості на ЕОМ (принаймні — клавіатури та маніпулятора "миша'). Починаючи з версії 6.5 PGP має засоби підтримки мереж віртуальних приватних VPN.

П. аналізу безпеки мережі для адміністратора /п. анализа безопасности сети для администратора/ [Security Analysis Network Tool for Administrator (SATAN, SANTA)] — програма пошуку можливих недоліків в системі захисту мережі, призначена в першу чергу для адміністраторів (офіцерів безпеки) мереж, однак може використовуватися порушниками для здійснення атак на систему захисту мережі. Відомі версії програми реалізовані на машинно-незалежних мовах програмування Perl та C.

П. антивірусна /п. антивірусна/ — програма, призначена для виявлення і (або) вилучення вірусів комп'ютерних.

П. входження держави в інформаційне суспільство /п. вхождения государства в информационное общество/ — план діяльності держави, спрямований на вирішення завдань формування сучасної сфери (середовища) інформаційної, що забезпечує ефективний розвиток засобів масової інформації, формування ресурсів інформаційних, підготовки інформаційних продуктів, надання послуг інформаційних, а також прийняття термінових заходів, спрямованих на створення простору інформаційного єдиного держави і його інтеграції в простір інформаційний світовий та встановлення жорсткого контролю за державними система-

ми зв'язку та телекомунікацій. Програма повинна передбачати розгляд наступних напрямків: формування і розвиток інфраструктури інформаційної держави; реалізація права на інформацію в мережах інформаційних; захист особистості, суспільства, держави від неякісної, фальшивої інформації і дезінформації; захист інтелектуальної власності в інформаційних мережах; захист інформації, в тому числі персональних даних, даних в інформаційних мережах; застосування можливостей технологій інформаційних для розвитку нових форм трудової діяльності, освіти і виховання; захист прав споживачів та розвиток конкуренції в мережах; реалізація відповідальності за правопорушення в інформаційній сфері; стандартизація як засіб сумісності в мережах; міжнародне співробітництво з проблем створення глобального інформаційного суспільства; координація робіт з реалізації програми.

П. з потенційно небезпечними наслідками /п. с потенциально опасными последствиями/ — окремі програми (набори інструкцій), що відносяться до зброї інформаційної програмної, які мають спроможність виконувати будь-яку непусту множину наступних функцій: приховування ознак своєї присутності в програмно-апаратного середовищі мережі обміну інформацією; здатність до самодублювання, асоціювання себе з іншими програмами і (або) перенесення своїх фрагментів в інші ділянки оперативної або зовнішньої пам'яті; руйнування (спотворення довільним чином) кодів програм в оперативній пам'яті; збереження фрагментів інформації з оперативної пам'яті в деякій ділянці зовнішньої пам'яті прямого доступу (локальної або віддаленої); спотворення довільним чином, блокування і (або) підміни масивів інформації, що виводиться у зовнішню пам'ять або в канал зв'язку, утворених в результаті роботи прикладних програм, або масивів даних, що уже знаходяться у зовнішній пам'яті; придушення інформаційного обміну в телекомунікаційних мережах, фальсифікування інформації в каналах державного й воєнного управління; нейтралізування роботи тестових програм і систем захисту інформаційних ресурсів. П. з п. н. н. умовно поділяють на наступні класи: віруси комп'ютерні; засоби несанкціонованого доступу; закладки програмні.

П. інтелектуальної протидії /п. интеллектуального противодействия/ — програмна реалізація об'-

єкта атаки хибного.

П. прикладна /п. прикладная/ [application p.] — програма, призначена для вирішення задач або класу задач в певній галузі застосування систем оброблення даних.

П. радіомовлення /п. радиовещания/ — сукупність різноманітних інформаційних і публіцистичних повідомлень, які об'єднані в єдине ціле і передаються протягом певного часу певним категоріям населення (військовослужбовців) противника у відповідності з поставленою метою та завданнями впливу психологічного. П. р. поділяються на наступні види: повідомлення інформаційне; коментар; інтерв'ю; репортаж. Рекомендують також використовувати в п. р. такі види передач, як нарис, політичний фейлетон, бесіда, огляд листів, трансляція мітингів і зборів, читання списків військовополонених.

П. резидентна /п. резидентная/ [resident p.] — програма, яка під час оброблення даних постійно знаходиться в частині основної пам'яті, що захищена від програм прикладних.

П. сервісна /п. сервисная/ [service p.] — програма, що виконує допоміжні функції при експлуатації системи обчислювальної.

П. системна /п. системная/ [system p.] — програма, що входить до складу системи операційної.

П. троянська /п. троянская/ [trojan p.] — закладка програмна, яка має законний доступ до системи, проте виконує також і приховані (неоголошені) функції. Див. також троянський кінь. Впровадження п. т. в системи керування автоматизовані противника здійснюється наступними способами: використанням атак віддалених; впровадженням закладок програмних в системи операційні та програмне забезпечення, що поставляються на експорт; агентурним шляхом.

П. усного мовлення /п. устного вещания/ — різноманітні тексти, що містять коротку, але цікаву інформацію, з додатковими (звуковими або шумовими) ефектами. П. у. м. класифікують за різноманітними ознаками. Так, за стилем викладення вони поділяються на інформаційні, аналітичні і ультимативні, а за способом підготовки — програми в запису, програми прямого передавання, змішані програми. П. у. м. мають певну структуру, а їхня підготовки включає декілька етапів. Різновидом п. у. м. є також так звані

програми стандартизовані.

П. усного мовлення аналітичні /п. устного вещания аналитические/ — програми усного мовлення, що роз'яснюють причини виникнення наявної воєнно-політичної обстановки, подій на фронті й у глибокому тилу, підштовхуючи таким чином слухачів до цілком визначених висновків. Аналітичним програмам властива широка жанрова різноманітність матеріалів: це повідомлення на різноманітні теми, бесіди з військовополоненими, їхні виступи і звернення, огляди листів військовослужбовців, коментарі службових документів і т.ін. Такі програми можуть бути і тематичними, тобто містити інформацію тільки з однієї теми.

П. усного мовлення в запису /п. устного вещания в записи/ — програми усного мовлення, що являють собою тексти, які повністю записані на магнітну плівку або інший носій. Вони, як правило, містять виступи військовополонених, перебіжчиків, представників громадськості противника. Трансляція попередньо записаних програм не потребує присутності диктора.

П. усного мовлення змішані /п. устного вещания смешанные/ — програми усного мовлення, утворені комбінацією програм усного мовлення в запису і програм усного мовлення прямого передавання. В таких передачах заздалегідь підготовлені тексти диктори доповнюють актуальною інформацією, що враховує зміни обстановки і психологічних особливостей конкретних об'єктів впливу, що в значній мірі збільшує їхню ефективність.

П. усного мовлення інформаційні /п. устного вещания информационные/ — ділові, без коментарів повідомлення про різноманітні факти і події, які здатні привернути увагу противника. Вони можуть містити інформацію як загального, так і місцевого значення, яка характеризує стан у світі, в конкретних країнах, на фронті й у тилу в цілому, в окремих районах. Особливу цінність така інформація має у тих випадках, коли вона ще не відома особовому складу противника і повідомляється дикторами вперше. Інформаційні програми не закликають слухачів приймати негайні рішення. Мета таких програм — оперативно доводити до них конкретні відомості, підштовхнути до осмислення подій і тим самим підготувати підґрунтя для

наступного рішення.

П. усного мовлення прямого передавання /п. устного вещания прямой передачи/ — програми усного мовлення, які найчастіше здійснюються на основі заздалегідь підготовлених і затверджених текстів, рідше — на основі тезисів, а у виняткових випадках — у формі діалогу диктора із слухачами (при умові, що ним заздалегідь підібрані необхідні факти і аргументи, яскраві мовні звороти. Прямі передачі мають високу ефективність, їх ведуть диктори, які не тільки дуже добре володіють відповідною мовою, але й добре знають психологію противника, здатні швидко і правильно реагувати на зміни в обстановці.

П. усного мовлення стандартизовані /п. устного вещания стандартизованные/ — програми усного мовлення, що являють собою готові тексти, написані заздалегідь, і призначені для використання в типовій бойовій обстановці. В них є пропуски для підстановки необхідних дат, географічних назв, прізвищ, найменування частин і т.ін. Такі програми використовують підрозділи психологічної війни нижньої ланки, якщо їхні співробітники недостатньо володіють мовою противника. В формі стандартизованих програм, звичайно, передають звернення до противника після успішного бою своїх військ на даній ділянці фронту, після артилерійського або авіаційного нальоту на його позиції, а також звернення до оточених і блокованих частин противника.

П. усного мовлення ультимативні /п. устного вещания ультимативные/ — програми усного мовлення, які містять звернення, заклики, ультиматуми, що потребують швидких практичних дій, а також роз'яснюють наслідки їхнього невиконання. Такі програми доцільні тоді, коли обстановка дозволяє диктувати військовослужбовцям і цивільним особам противника свої умови. До числа ультимативних програм відносяться накази воєнного командування, звернення політичного керівництва, заклики полонених офіцерів противника до особового складу їхніх колишніх підрозділів.

ПРОГРАМІСТ /программист/ [programmer] — особа, яка здійснює розробку і налагодження програм. За видом програмного забезпечення, що розробляється п. поділяються на системних і прикладних.

П. прикладний /п. прикладной/ [applications p.] — програміст, який здійснює розробку і налагодже-

ння програм прикладних. Такий програміст повинен бути одночасно фахівцем в прикладній галузі, до якої належать задачі, що їх треба розв'язати.

П. системний /п. системный/ [systems (software) p., toolsmith] — програміст, який займається розробкою, експлуатацією і супроводженням програмного забезпечення системного.

ПРОГРАМОТЕХНІКА /программотехника/ [software engineering] — 1) Техніка забезпечення програмного — сукупність технічних засобів, які забезпечують створення, зберігання, удосконалення і експлуатацію програм. 2) Технологія розробки, налагодження, верифікації і впровадження програмного забезпечення.

ПРОГРАМУВАННЯ /программирование/ [programming] — теоретична і практична діяльність, яка спрямована на забезпечення програмного керування обробленням даних, яка включає створення програм, а також вибір структури і кодування даних.

П. математичне /п. математическое/ [mathematical p.] — сукупність математичних методів знаходження екстремуму функції при певних обмеженнях у вигляді множини рівностей і нерівностей.

П. нейролінгвістичне (НЛП) /п. нейролингвистическое (НЛП)/ — див. вплив нейролінгвістичний.

П. системне /п. системное/ [system p.] — розробка загального програмного забезпечення — систем операційних, систем програмування, а також пакетів *програм прикладних* загального призначення.

П. стохастичне /п. стохастическое/ [stochastic p.] — розділ програмування математичного, який вивчає моделі вибору оптимальних рішень в ситуаціях, що характеризуються випадковими величинами.

ПРОДУКТ /продукт/ — 1) Предмет, що є матеріальним результатом людської праці, діяльності, виріб. 2) Наслідок, витвір, результат чого-небудь; твір.

П. інформаційних технологій (ІТ-продукт) /п. информационных технологий (IT-продукт)/ — сукупність апаратних і (або) програмних засобів, яка поставляється кінцевому споживачеві як готовий до використання засіб оброблення інформації. Сукупність ІТ-продуктів об'єднується в функціонально закінчений комплекс (продукт) для вирішення конкретного прикладного завдання в системі оброблення інформації. Принциповою відмінністю між ІТ-продуктом і системою оброблення інформації є наступне. ІТ-продукт зви-

чайно розробляється для використання в багатьох системах оброблення інформації, тому його розробник орієнтується тільки загальні вимоги до середовища його експлуатації (умови його застосування і потенційні загрози інформації). Навпаки, система оброблення інформації розроблюється вузько спеціалізованою для вирішення конкретних прикладних завдань і під конкретні вимоги споживачів, що дозволяє у повній мірі враховувати специфіку впливу зі сторони конкретного середовища експлуатації. Саме тому IT-продукт, а не система оброблення інформації, декларується в стандарті як універсальний компонент безпеки.

ПРОДУКЦІЯ /продукция/ [products] (лат. productio, від produco — виробляю) — сукупність продуктів діяльності, виробництва.

П. інформаційна /п. информационная/ [information p.] — інформація документована, підготовлена у відповідності до вимог користувачів і призначена або застосовується для задоволення потреб користувачів. До п. і. відносяться: документи, дані; відбірки документів, даних; довідки, аналітичні довідки; бази даних, банки даних; інші види інформаційних продуктів.

ПРОЕКТ /проект/ [design, project] (від лат. projectus — кинутий вперед) — 1) Сукупність документів (розрахунків, креслень тощо), необхідних для виготовлення виробу, зведення споруд тощо. 2) Попередній, гаданий текст будь-якого документа. 3) План, задум організації, влаштування, заснування будь-чого.

П. захисту /п. защиты/ [Security Target (ST)] — нормативний документ, що включає вимоги і завдання захисту продукту інформаційних технологій, а також описує рівень функціональних можливостей реалізованих в ньому засобів захисту, їхнє обґрунтування і підтвердження ступеню їхніх гарантій. П. з., з однієї сторони є відправною точкою для розробника системи, а з іншої являє собою еталон системи в ході аналізу кваліфікаційного. П. з. містить вступ, опис IT-продукту, середовище експлуатації, завдання захисту, вимоги безпеки, загальні специфікації IT-продукту, заявку на відповідність профілю захисту, обґрунтування. Багато розділів п. з. співпадають з однойменними розділами профілю захисту.

П. захисту: вимоги безпеки /п. защиты: требования безопасности/ [IT security requirements] — розділ проекту захисту, що містить вимоги безпеки до продукту інформаційних технологій, якими керувався

виробник у ході його розроблення. Цей розділ дещо відрізняється від аналогічного розділу профілю захисту. Розділ вимог безпеки функціональних до ІТ-продукту на відміну від відповідного розділу профілю захисту допускає використання крім типових вимог "Загальних критеріїв" і інших, специфічних для даного продукту й середовища його експлуатації. При описі таких спеціальних вимог необхідно зберігати стиль "Загальних критеріїв" і забезпечувати властиву їм ступінь деталізації. Розділ вимог гарантій безпеки може включати рівні гарантій, не передбачені в "Загальних критеріях". В даному випадку опис рівня гарантій повинен бути чітким, несуперечливим і мати ступінь деталізації, що допускає його використання в ході аналізу кваліфікаційного. При цьому бажано використати стиль і деталізації опису рівнів гарантій, прийняті в "Загальних критеріях".

П. захисту: вступ /п. защиты: введение/ [ST introduction] — розділ проекту захисту, який містить інформацію, необхідну для ідентифікації проекту захисту, визначення призначення, а також огляд його змісту та заявку на відповідність вимогам "критеріїв Загальних". Ідентифікатор проекту захисту — унікальне ім'я проекту захисту для його пошуку і ідентифікації, а також відповідного продукту інформаційних технологій. Огляд змісту — достатньо докладна анотація проекту захисту, що дозволяє споживачам визначати придатність ІТ-продукту для вирішення завдань. Заявка на відповідність "Загальним критеріям" — опис усіх властивостей ІТ-продукту, що підлягають аналізу кваліфікаційному на основі"Загальних критеріїв".

П. захисту: завдання захисту /п. защиты: задачи защиты/ [security objectives] — розділ проекту захисту, що відображає потреби користувачів у протидії потенційним загрозам безпеці і (або) реалізації політики безпеки. До складу завдань захисту входять завдання захисту продукту інформаційних технологій та інші завдання захисту. Завдання захисту ІТ-продукту повинні визначати й регламентувати потреби в протидії потенційним загрозам безпеці і (або) у реалізації політики безпеки. Інші завдання захисту повинні регламентувати потреби в протидії потенційним загрозам безпеці і (або) у реалізації політики безпеки інших компонентів комп'ютерної системи, що не відносяться до сфери технологій інформаційних.

П. захисту: загальні специфікації ІТ-продукту /п. защиты: общие спецификации ИТ-продукта/

[TOE summary specification] — розділ проекту захисту, який описує механізми здійснення завдань захисту за допомогою визначення багаторівневих специфікацій засобів захисту у відповідності до вимог безпеки функціональних і вимог гарантій безпеки, що пред'являються. Складаються з специфікацій функцій захисту і специфікацій рівня гарантій.

П. захисту: заявка на відповідність профілю захисту /п. защиты: заявка на соответствие профилю защиты/ [PP claims] — необов'язковий розділ проекту захисту, який містить матеріали, необхідні для підтвердження заявки. Для кожного профілю захисту, на реалізацію якого претендує проект захисту, цей розділ повинен містити посилання на профіль захисту, відповідність профілю захисту, удосконалення профілю захисту. Посилання на профіль захисту однозначно ідентифікує профіль захисту, на реалізацію якого претендує проект захисту, із указуванням випадків, в яких рівень захисту, що забезпечується, перевершує вимоги профілю з коректною реалізацією усіх його вимог без виключення. Відповідність профілю захисту визначає можливості продукту інформаційних технологій, які реалізують завдання захисту і вимоги, що містяться в профілі захисту. Удосконалення профілю захисту відображає можливості IT-продукту, які виходять за рамки завдань захисту і вимог, встановлених у профілі захисту.

П. захисту: обґрунтування /п. защиты: обоснование/ [rationale] — розділ проекту захисту, який повинен показувати, що проект захисту містить повну й зв'язну множину вимог, що продукт інформаційних технологій, який реалізує їх, буде ефективно протистояти загрозам безпеці. Крім того, обґрунтування містить підтвердження заявленої відповідності профілю захисту. Розділ деталізується у наступному. Обґрунтування завдань захисту повинно демонструвати, що завдання захисту, заявлені в проекті захисту, відповідають властивостям середовища експлуатації, тобто їхнє вирішення дозволить ефективно протидіяти загрозам безпеці і реалізувати вибрану під них політику безпеки. Обґрунтування вимог безпеки показує, що виконання цих вимог дозволяє вирішити завдання захисту тому, що: сукупність функціональних вимог безпеки і вимог гарантій безпеки, а також умов експлуатації IT-продукту відповідають завданням захисту; всі вимоги безпеки є несуперечливими і взаємно підсилюють одна одну; вибір вимог є оправданим; рівень

функціональних можливостей засобів захисту відповідає завданням захисту. Обґрунтування загальних специфікацій ІТ-продукту повинно демонструвати, що засоби захисту й методи забезпечення їхніх гарантій відповідають вимогам, що пред'являються, оскільки: сукупність засобів захисту задовольняє функціональним вимогам; необхідний рівень безпеки і надійності захисту забезпечується засобами, що запропоновані; заходи, спрямовані на забезпечення гарантій реалізації функціональних вимог, відповідають вимогам гарантій. Обґрунтування відповідності профілю захисту показує, що вимоги проекту захисту підтримують всі вимоги профілю захисту. Для цього повинно бути показано, що: всі удосконалення завдань захисту порівняно з профілем захисту реалізовані коректно і в напрямку їхнього розвитку й конкретизації; всі удосконалення вимог безпеки порівняно з профілем захисту реалізовані коректно і в напрямку їхнього розвитку й конкретизації; всі завдання захисту профілі захисту успішно реалізовані і всі вимоги профілю захисту вдоволені; ніякі додатково введені в проект захисту спеціальні завдання захисту й вимоги безпеки не суперечать профілю захисту.

П. захисту: опис ІТ-продукту /п. защиты: описание ИТ-продукта/ [TOE description] — розділ проекту захисту, який містить коротку характеристику продукту інформаційних технологій, призначення, принцип роботи, методи використання і т.ін. Ця інформація не підлягає кваліфікаційному аналізові та сертифікації, але подається розробникам і експертам для пояснення вимог безпеки й визначення їхньої відповідності завданням, що вирішуються за допомогою ІТ-продукту.

П. захисту: середовище експлуатації /п. защиты: среда эксплуатации/ [TOE security environment] — розділ проекту захисту, що містить опис усіх аспектів функціонування продукту інформаційних технологій, зв'язаних з безпекою. В середовищі експлуатації описуються умови експлуатації, загрози безпеці, політика безпеки. Опис умов експлуатації ІТ-продукту повинен містити вичерпну характеристику середовища його експлуатації з точки зору безпеки, в тому числі обмеження на умови його застосування. Опис загроз безпеці, що діють у середовищі експлуатації, яким повинен протистояти захист ІТ-продукту. Для кожної загрози повинно бути вказане її джерело, метод і об'єкт впливу. Опис політики безпеки повинен визначати і, при

необхідності, пояснювати правила політики безпеки, яка повинна бути реалізована в IT-продукті.

ПРОМИВАННЯ МОЗКІВ /промывание мозгов/ [brainwashing] — маніпулювання суспільною свідомістю за допомогою засобів масової інформації.

ПРОМІННЯ /излучение/ [radiation] — результат виділення променями теплової, електромагнітної та інших енергій.

П. видиме /и. видимое/ [visible r.] — проміння оптичне, що характеризується довжинами хвиль, які розташовані в діапазоні $4 \cdot 10^{-7}$ — $7,6 \cdot 10^{-7}$ м.

П. електромагнітне /и. электромагнитное/ [electromagnetic r.] — хвилі електромагнітні, що поширюються в просторі.

П. інфрачервоне /и. инфракрасное/ [InfraRed (IR, calorific r.)] — проміння оптичне, що характеризується довжинами хвиль, які розташовані в діапазоні $7,6 \cdot 10^{-7}$ — $2 \cdot 10^{-3}$ м.

П. немодульоване /и. немодулированное/ [unmodulated r.] — проміння, що не змінюється в часі за період його вимірювання. Як правило в інфрачервоній техніці рівень п. н. не є об'єктом вимірювання. При цьому постійну складову потоку проміння інфрачервоного називають фоном.

П. оптичне /и. оптическое/ [optical r.] — проміння електромагнітне, що характеризується довжинами хвиль, які розташовані в діапазоні $5 \cdot 10^{-9}$ — $2 \cdot 10^{-3}$ м. У зазначеному діапазоні електромагнітні хвилі найефективніше визначаються оптичними методами, для яких характерне формування керованих потоків електромагнітних хвиль за допомогою оптичних систем.

П. радіочастотне /и. радиочастотное/ [radio frequency r.] — електромагнітні коливання (хвилі) в діапазоні радіочастот, що поширюються (випромінюються) в просторі.

П. ультрафіолетове /и. ультрафиолетовое/ [ultraviolet r.] — проміння оптичне, що характеризується довжинами хвиль, які розташовані в діапазоні $5 \cdot 10^{-9}$ — $4 \cdot 10^{-7}$ м.

ПРОМІНЬ /луч/ [ray] — напрям поширення енергії хвиль (електромагнітних, теплових і т. ін.).

ПРОНИКНЕННЯ /проникновение/ [penetration] — 1) Попадання, пробирання куди-небудь всередину.

2) Успішне подолання механізмів захисту системи.

П. до джерела інформації із застосуванням сили /п. к источнику информации с применением силы/ — вид фізичного проникнення до джерела інформації. Здійснюється способом нападу на охорону організації з метою викрадення джерела інформації. Використовується, коли ціна інформації дуже велика.

П. до джерела інформації легальне /п. к источнику информации легальное/ — вид фізичного проникнення до джерела інформації. Реалізується упровадженням і легалізацією зловмисника на роботу в організацію, що цікавить органи розвідки або його особисто. При цьому зловмисник повинен мати переконливу легенду і відповідні документи. Найчастіше використовується для забезпечення регулярного потайного доступу до інформації.

П. до джерела інформації приховане /п. к источнику информации скрытное/ — вид фізичного проникнення до джерела інформації. Полягає в таємному попаданні зловмисника до місця, де зберігається носій інформації. Приховане проникнення має ряд переваг порівняно з іншими, але потребує ретельної підготовки і апріорної інформації про місце знаходження носія, системи безпеки (охорони), можливі маршрути пересування і т.ін. Приховане проникнення не може носити регулярний характер, так як воно пов'язане із великим ризиком для зловмисника.

П. до джерела інформації фізичне /п. к источнику информации физическое/ — метод доступу до інформації, що ґрунтується на попаданні зловмисника до джерела інформації. Конкретний спосіб проникнення залежить від виду інформації і способів її використання. Розрізняють приховане (потайне) проникнення зловмисника до місця зберігання носія інформації, проникнення із застосуванням зловмисником сили, а також легальне проникнення до джерела інформації шляхом вступу зловмисника на роботу в організацію, яка його цікавить.

ПРОПАГАНДА /пропаганда/ [propaganda] (від лат. propaganda — те, що підлягає розповсюдженню) — 1) Поширення і постійне, глибоке та детальне роз'яснення яких-небудь поглядів, ідей, вчень, політичних, наукових та інших знань; агітація, популяризація. 2) Ідейний вплив на широкі маси або певні групи людей,

що носить політичний або релігійний характер. 3) Система масового поширення ідей, поглядів і т. ін.

П. біла /п. белая/ — пропаганда, при якій посилаються на офіційні джерела інформації (наприклад, інформацію урядових органів). Б. п. є відкритою, використовує перевірені дані і не маскує свої цілі.

П. науково-технічна (НТП) /п. научно-техническая (НТП)/ [p. of scientific and technical knowledge] — вид діяльності науково-інформаційної з розповсюдження досягнень науки, техніки та передового досвіду з метою їхнього впровадження і підвищення рівня знань фахівців з використанням форм, методів та засобів масової інформації.

П. сіра /п. серая/ — пропаганда, при якій не завжди показують джерела інформації, використовують як достовірні, так і неперевірені відомості, намагаються підтасовувати факти й думки, щоб таким чином нав'язувати свої висновки й оцінки.

П. чорна /п. черная/ — пропаганда, що завжди приховує справжні джерела інформації, і ставить за мету обман.

ПРОСТІР /пространство/ [space] — протяжність, місце, не обмежене видимими краями.

П. імен /п. имен/ [name s.] — множина усіх можливих імен, доступних через службу імен (див. служба каталогів). П. і. декларує угоди і синтаксис іменування об'єктів.

П. імен DNS /п. имен DNS/ [DNS name s.] — набір або дерево імен доменів і правила створення цих імен. Кожний вузол в імені домену являє деякий об'єкт, наприклад, комп'ютер або псевдонім для електронної пошти. Для будь-якого домену виділений DNS-сервер, з якого здійснюється його адміністрування. Компанії або великі мережі вправі поділяти домен на декілька піддоменів для спрощення адміністрування або інших потреб. В цьому випадку кожний з піддоменів повинен мати свій DNS-сервер, який містить його базу даних. Усі зміни в базі даних здійснюються тільки цим сервером, і він обробляє запити клієнтів і інших DNS-серверів. Сервер, що зберігає базу, називають відповідальним (authoritive) сервером цього домену або піддомену.

П. інформаційний єдиний держави /единое информационное п. государства/ — сукупність баз і

банків даних, технологій їхнього ведення і використання, інформаційно-телекомунікаційних мереж і систем, які функціонують на основі єдиних принципів і за загальними правилами, що забезпечують інформаційну взаємодію організацій і громадян, а також задоволення їхніх інформаційних потреб. П. і. е. д. складається з наступних головних компонентів: ресурсів інформаційних, що містять дані, відомості і знання, зафіксовані на відповідних носіях інформації; організаційні структури, що забезпечують функціонування і розвиток єдиного інформаційного простору, тобто збирання, оброблення, зберігання, розповсюдження, пошук і передачу інформації; засоби інформаційної взаємодії громадян і організацій, які забезпечують їм доступ до інформаційних ресурсів на основі відповідних інформаційних технологій, включаючи програмно-технічні засоби і організаційно-нормативні документи. Організаційні структури та засоби інформаційної взаємодії утворюють інфраструктуру інформаційну.

П. інформаційний світовий /п. информационное мировое/ — основа суспільства інформаційного, в якому діють великі інформаційні конгломерати, що об'єднують системи створення інформації (видавничі будинки, редакції газет і журналів, телемережі, телестудії) і мережі її розповсюдження (кабельні, телефонні, комп'ютерні, супутникові) та функціонують глобальні міжнародні інформаційно-телекомунікаційні мережі, що охоплюють більшість країн світу. Мережі надають споживачеві широкий набір інформаційних продуктів і послуг. Це ділова, освітня, розважальна інформація, електронні газети і журнали, бази даних практично в усіх галузях життєдіяльності суспільства, електронна пошта, доступ до різноманітних інформаційних ресурсів бібліотек, державних і приватних закладів і компаній.

П. ключовий /п. ключевое/ [key s.] — множина всіх можливих ключів.

ПРОТИБОРСТВО /противоборство/ [confrontation, opposition, antagonism] — боротьба проти будь-чого, будь-кого, протидія.

П. інформаційне /п. информационное/ [information c.] — процес реалізації впливів інформаційних, спрямованих на досягнення мети державної політики в мирний і воєнний часи. Має місце у відносинах між державами незалежно від розвитку співробітництва між ними.

ПРОТИВНИК /противник/ [adversary, enemy, opponent] — 1) Особа, що вороже ставиться до кого-, чого-небудь, протидіє комусь, чомусь. 2) Вороже військо, ворожі збройні сили; ворог.

ПРОТИДІЯ /противодействие/ [counteraction, opposition] — дія, що перешкоджає іншій дії.

П. гідроакустичному спостереженню /п. гидроакустическому наблюдению/ — сукупність дій, що забезпечують захист від гідроакустичного спостереження. Способи захисту враховують особливості каналу витоку інформації. Основними способами п. г. с. є: маскування з використанням природних явищ (наприклад, при перепаді температури шарів води виникають акустичні екрани, що відбивають акустичні хвилі); використання звукопоглинальних покриттів стільникової конструкції з нейлону, поліетилену, поліпропілену і різноманітних пластмас, а також таких, що містять натуральний каучук; створення активних завад гідролокаторам, в тому числі шляхом ретрансляції опромінюючих сигналів з підсиленням їхньої потужності.

П. загрозам безпеки /п. угрозам безопасности/ — основне завдання захисту системи оброблення інформації, вирішення якої визначає ступінь захищеності системи. Вирішується двома методами: створенням засобів захисту від кожного виду загроз; усуненням причин, що зумовлюють успішну реалізацію загроз.

П. інтелектуальна /п. интеллектуальное/ — комплекс завдань, що вирішуються в процесі реагування на дії несанкціоновані в інформаційно-обчислювальній мережі на основі оперативного аналізу стратегії противника, зброї інформаційної, що застосовується противником, технічних можливостей ІОМ, поточних завдань боротьби інформаційної і керування корпорацією, в тому числі, і з використанням засобів штучного інтелекту. Див. також вплив у відповідь на інформаційний напад. П. і. підпорядкована наступним цілям інформаційної війни в ІОМ: зниження часу безконтрольної присутності противника в інформаційно-обчислювальній мережі; дезінформування противника в інформаційно-обчислювальній мережі; дезорганізація дій противника в інформаційно-обчислювальній мережі; зниження нецільового навантаження на інформаційно-обчислювальну мережу; впливу на ресурси противника.

П. інформаційна /п. информационное/ [information c.] — сукупність заходів боротьби інформаційної, спрямованих на протидію інформаційному забезпеченню протиборчої сторони. П. і. включає блокування

добування, оброблення і обміну інформацією та впровадження дезінформації на всіх етапах інформаційного забезпечення. Завдання п. і. вирішуються шляхом маскування, контррозвідки, придушення радіоелектронного і руйнування систем інформаційних противника.

П. інформаційна в мережі обміну інформацією /п. информационное в сети обмена информацией/ — один з основних аспектів забезпечення переваги над противником в інформаційній війні, що полягає в дезінформуванні противника, дезорганізації дій противника, зниженні нецільового навантаження на мережу обміну інформацією та в організації впливів на ресурси інформаційні противника. Одночасно проводяться заходи, спрямовані на зменшення часу безконтрольної присутності противника в мережі обміну інформацією та вирішуються завдання простого реагування та протидії інтелектуальної.

П. інформаційній зброї /п. информационному оружию/ — сукупність заходів, що включають: захист матеріально-технічних об'єктів, які складають фізичну основу інформаційних ресурсів; забезпечення нормального і безперебійного функціонування баз і банків даних; захист інформації від доступу несанкціонованого, спотворення або знищення; збереження якості інформації (своєчасності, точності, повноти) і необхідної доступності; створення технологій виявлення впливів на інформацію, в тому числі і у відкритих мережах.

П. підслухуванню /п. подслушиванию/ — сукупність дій, спрямованих на блокування будь-яких каналів (акустичних і складених), за допомогою яких здійснюється витік інформації акустичної. У відповідності до загальних методів захисту інформації для захисту від підслухування застосовуються наступні способи: приховування інформаційне мовної інформації; приховування енергетичне акустичних сигналів; запобігання витоку інформації через закладні підслуховуючі пристрої.

П. радіолокаційному спостереженню /п. радиолокационному наблюдению/ — сукупність дій, спрямованих на запобігання одержання радіолокаційного зображення об'єкта. Заходи захисту в даному випадку спрямовані на пониження ЕПР об'єкта в цілому і його характерних ділянок, що містять інформативні демаскуючі ознаки. Можна виділити два основних способи п. р. с. — приховування інформаційне об'єкта

радіолокаційного спостереження та приховування енергетичне об'єкта радіолокаційного спостереження.

П. спостереженню /п. наблюдению/ — сукупність дій, що запобігають добуванню зловмисниками інформації (в основному про ознаки видові і іноді семантичної) шляхом спостереження (візуального або за допомогою різноманітних приладів) джерел інформації в оптичному, акустичному і радіоелектронному каналах витоку. Можна виділити наступні види п. с.: протидія спостереженню в оптичному діапазоні; протидія радіолокаційному спостереженню; протидія гідроакустичному спостереженню.

П. спостереженню в оптичному діапазоні /п. наблюдению в оптическом диапазоне/ — сукупність дій, що запобігають добуванню інформації про об'єкт шляхом спостереження в оптичному діапазоні.

ПРОТОКОЛ /протокол/ [protocol] (грец. $\pi\rho\omega\tau\acute{o}\kappa\varnothing\lambda\lambda\varnothing\nu$, від — $\pi\rho\tilde{\omega}\tau\varnothing\varsigma$ — перший і $\kappa\varnothing\lambda\lambda\acute{\alpha}\omega$ — приклеюю) — 1) Результат реєстрації в хронологічному порядку інформації про хід деякого процесу. 2) В мережах обчислювальних — сукупність правил, що визначають формат і процедури обміну інформацією між двома або більше незалежними пристроями або процесами.

П. BGP /п. BGP/ [Border Gateway Protocol (BGP)] (англ. — п. розмежувальних маршрутизаторів) — протокол маршрутизації, що реалізує динамічну, міждоменну, розподілену, однорівневу, багатошляхову маршрутизацію і керується маршрутизатором. Розроблений для заміни протоколу EGP. В BGP передбачене виявлення кільцевих маршрутів і використання при прийнятті рішень різноманітних метрик (числа переходів, пропускної здатності каналу і т. ін.). Спочатку маршрутизатори, що працюють за п. BGP, обмінюються повними таблицями маршрутизації, а по мірі їхнього змінювання, розсилаються оновлення — послідовні, що відображають тільки зміни. В таблицях маршрутизації п. BGP можливі декілька маршрутів до одного місця призначення, проте іншим маршрутизаторам повідомляються тільки оптимальні. Оновлення таблиць BGP розсилаються за допомогою протоколу TCP. Вони містять інформацію про те, які домени досяжні з конкретного вузла.

П. EGP /п. EGP/ [Exterior Gateway Protocol] (англ. — зовнішній п. маршрутизації) — протокол маршрутизації, що реалізує динамічну, міждоменну, розподілену, однорівневу і одношляхову маршрутизацію

і керується маршрутизатором. Інформація про досяжність вузла передається через оновлення (updates), які містять рядки типу "куди можна попасти з вузла X" або "звідси можна попасти туди-то", тобто такі маршрутизатори і хости, які досяжні від таких маршрутизаторів. Оновлення регулярно розсилаються усім сусіднім вузлам, причому кожне містить інформацію про сусідів маршрутизатора, який послав повідомлення. Маршрутизатори збирають цю інформацію і з нею складають свої таблиці маршрутизації.

П. FTP /п. FTP/ [File Transfer Protocol] (англ. — п. передачі файлів) — протокол Інтернету прикладний, що реалізує відносно безпечний спосіб переміщення файлів між різноманітними комп'ютерами. Транспортним механізмом для передавання даних FTR служить протокол TCP. Засобами FTR користувач може пред'являти "посвідчення особи" сервера, а потім переглядати папки і передавати файли в обидва напрямки. FTR дозволяє передавати дані як між клієнтом і FTR-сервером, так і між двома віддаленими комп'ютерами.

П. HTTP /п. HTTP/ [Hypertext Transfer Protocol (HTTP)] (англ. — п. передачі гіпертексту) — протокол Інтернету прикладний, що реалізує передачу даних між Web-сервером і клієнтом.

П. ICMP /п. ICMP/ [Internet Control Message Protocol (ICMP)] — букв. міжмережний протокол керуючих повідомлень. Використовується хостами і маршрутизаторами для обміну керуючою інформацією, наприклад, про помилки або про процес початкового завантаження. Вважається протоколом Інтернету прикладним.

П. IGRP /п. IGRP/ [Interior Gateway Routing Protocol (IGRP)] (англ. — внутрішній п. межової маршрутизації) — протокол маршрутизації, що реалізує динамічну, внутрішньодоменну, розподілену, однорівневу, багатошляхову і векторну маршрутизацію. Розроблений для застосування в складних мережах. При виборі маршруту враховується ціла множина факторів, наприклад, пропускна здатність мережі, її надійність і завантаженість, а також розміри повідомлень.

П. IMAP /п. IMAP/ [Internet Message Access Protocol (IMAP)] (англ. — протокол доступу до повідомлень в Інтернеті) — протокол пошти електронної клієнт-серверної. Переважно використовується, коли

програмне забезпечення клієнта виконується на портативному комп'ютері. При застосуванні IMAP користувач може завантажувати повідомлення вибірково і навіть частково. Це дуже корисно при доступі до електронної пошти по низькошвидкісній телефонній лінії. Через IMAP клієнт може завантажувати з сервера поштового на свій комп'ютер тільки вибрані повідомлення, а потім від'єднуватися. При від'єднанні клієнт вправі модифікувати будь-яке з прийнятих повідомлень. Щоб забезпечити синхронізацію, IMAP присвоює повідомленню унікальний ідентифікатор, дійсний в будь-якому IMAP-сеансі.

П. IP /п. IP/ [Internet Protocol (IP)] (англ. — міжмережний п.) — протокол Інтернету базовий рівня мережного. Одержав широке поширення завдяки його інваріантності до середовища передавання, апаратних платформ, характеру даних. IP визначає формат адрес і механізм передавання даних у вигляді дейтаграм IP, які вкладаються в поле даних протоколу, що стоїть нижче, наприклад, Ethernet, TokenRing, ATM, або PPP. IP несе відповідальність за доставку окремого пакета повідомлення за заданою адресою. Спочатку пакет попадає на вузол провайдера, де спеціальні програми, користуючись таблицями маршрутизації, вибирають подальший маршрут прямування. При цьому різні пакети одного і того ж повідомлення можуть дійти до адресата різними маршрутами через різні вузли Інтернету. Доля повідомлення майже не залежить від несправностей в окремих дільницях мережі: при необхідності пакет можу бути переправлений обхідним шляхом.

П. IPSec /п. IPSec/ [Internet P. Security (IPSec)] — протокол безпеки Інтернету. який визначає модель мережного рівня для шифрування й автентифікації IP-пакетів даних. Протокол передбачає заголовок автентифікації і корисне навантаження, що інкапсулює секретність для автентифікації і конфіденційності пакетів.

П. NTP /п. NTP/ [Network Time Protocol (NTP)] — протокол, призначений для синхронізації часу на комп'ютерах, об'єднаних в мережу.

П. OAEP /п. OAEP/ [Optimal Asymmetric Encryption P.] — технологія кодування (шляхом доповнення

спеціальною інформацією) даних, які підлягають шифруванню за допомогою алгоритму RSA.

П. OSPF /п. OSPF/ [Open Shortest Path First (OSPF)] (англ. — відкритий п. переваги найкращого шляху) — протокол маршрутизації, що реалізує динамічну, внутрішньодоменну, розподілену, ієрархічну, багатошляхову і канальну маршрутизацію. При зміні таблиці маршрутизації OSPF-маршрутизатори обмінюються оновленнями. Для виявлення збоїв маршрутизатори розсилають повідомлення "ще живий". П. OSPF підтримує запити, коли повідомляється про терміновість деяких даних. В цьому випадку OSPF на свій розсуд використовує наявні канали, щоб як можна швидше відправити дані.

П. POP /п. POP/ [Post Office Protocol (POP)] — протокол пошти електронної клієнт-серверної, стосовно її автономної моделі. Використовуючи п. POP, клієнт поштовий при приєднані до сервера і перевірці нової пошти одержує відразу всі накопичені для нього повідомлення. POP-клієнт не може вибірково приймати повідомлення з сервера поштового — або всі. або нічого. Після того як повідомлення завантажені, поштовий клієнт вправі їх вилучати або змінювати, причому з сервером електронної пошти він уже не взаємодіє.

П. RIP /п. RIP/ [Routing Information Protocol (RIP)] (англ. — протокол маршрутної інформації) — протокол маршрутизації, що реалізує динамічну, внутрішньодоменну, розподілену, одноріневу, одношляхову і векторну маршрутизацію. Використовується для малих і середніх мереж, оскільки максимальне число переходів обмежене числом 16. П. RIP не може оперативно враховувати властивості мережі (наприклад, час затримки або завантаженість каналів).

П. S-HTTP /п. S-HTTP/ [Secure HyperText Transfer protocol (S-HTTP)] — протокол захищеного передавання гіпертексту, розроблений фірмою Enterprise Integration Techn. Призначений для застосуванні на прикладному рівні моделі ВВС (OSI). Об'єднує різні формати криптографічних повідомлень в браузерах WWW та серверах, в тому числі для систем, сумісних з PEM, PGP та PKCS-7.

П. SKIP /п. SKIP/ [Simple Key management for Internet P. (SKIP)] — протокол, що реалізує схему керування відкритими ключами, розроблену фірмою Sun Microsystems для обміну криптографічними ключами. В ньому описаний спосіб обчислення ключа на основі сертифікатів відкритих ключів. Використання

SKIP накладає певні обмеження на вибір алгоритмів шифрування і хешування. SKIP є необов'язковою компонентою специфікації протоколу IPSec.

П. SMTP /п. SMTP/ [Simple Mail Transfer (SMTP)] — простий протокол передавання пошти електронної. Його застосовують для передачі пошти від клієнта сервера, а також від одного сервера до іншого. В моделі ISO/OSI п. SMTP розташовується над протоколом TCP.

П. SSL /п. SSL/ [Secure Sockets Layer protocol (SSL)] — криптографічний протокол для забезпечення конфіденційності та автентичності даних, що передаються каналами зв'язку, розроблений фірмою Netscape. Призначений для застосуванні на сеансовому рівні моделі ВВС (OSI). Для розповсюдження ключів сеансових застосовується схема Діффі-Хеллмана. Застосовується в широко відомому браузері Internet Netscape Navigator.

П. TCP /п. TCP/ [Transmissin Control Protocol (TCP)] (англ. — п. керування передачею) — протокол Інтернету базовий рівня транспортного. TCP розбиває вихідне повідомлення на декілька невеликих фрагментів — пакетів. До кожного пакета прилаштовується заголовок, який містить службову інформацію (адресу відправника і одержувача, ідентифікатор повідомлення, номер пакета в повідомленні і т. ін.). Відправлені за допомогою протоколу IP пакети TCP-модулем адресата збираються докупи, і на основі службової інформації "склеюються" у вихідне повідомлення. Відсутні або спотворені фрагменти повідомлення пересилаються повторно.

П. Telnet /п. Telnet/ — додаток до протоколів TCP/IP, який дозволяє користувачеві працювати на віддаленій машині.

П. UDP /п. UDP/ [User Datagram Protocol (UDP)] (англ. протокол користувальницьких дейтаграм) — протокол рівня транспортного. Забезпечує передавання дейтаграм IP (негарантоване доставляння даних без установлення логічних з'єднань), але для безпосередньої роботи використовує протокол IP.

П. Діффі-Хеллмана /п. Диффи-Хеллмана/ [Diffie-Hellman p.] — протокол криптографічний для розповсюдження ключів, який використовує принципи асиметричної криптографії. Один з абонентів обирає

досить велике просте число p та породжуючий елемент g мультиплікативної групи поля p. Елементи p, g є відкритими довгостроковими ключами та використовуються усіма учасниками протоколу. Для генерації спільного ключа сеансового абонент A випадково обирає елемент $X \in Z_p$, обчислює $K_a = g^X \ mod p$ та надсилає його абоненту B. Абонент B випадково обирає елемент $Y \in Z_p$, обчислює $K_b = g^Y \ mod p$ та надсилає його абоненту A. Абоненти A B обчислюють ключ $K_{ba} = K_b^X \ mod p$ $K_{ab} = K_a^Y \ mod p$ відповідно. Внаслідок комутативності операції множення в мультиплікативній групі поля p $K_{ba} = K_{ab} = K$. Для забезпечення стійкості протоколу p повинно задовольняти спеціальним вимогам, саме — бути сильним простим числом. При правильному виборі p, g, X, Y, розподіл отриманого ключа K майже не відрізняється від рівномірного. Протокол Діффі-Хеллмана відноситься до методів формування ключів за класифікацією методів розповсюдження ключів та до криптосистем з довідною стійкістю — за класифікацією за стійкістю.

П. з арбітром /п. с арбитром/ — криптографічний протокол, в якому використовується одна або декілька незацікавлених довірених сторін (арбітрів). довіреність означає, що усі учасники протоколу визнають, що будь-які твердження або дії арбітра щирі і коректні.

П. заперечення /п. отрицания/ — протокол підпису безперечного, який не дозволяє особі, що підписується, відмовитися від підписаного повідомлення.

П. Інтернету /п. Интернета/ — набір погоджень про правила формування і формати повідомлень в Інтернеті, про способи обміну інформацією між абонентами мережі. В Інтернеті слід розрізняти два типи протоколів: базові і прикладні.

П. Інтернету базові /базовые п. Интернета/ — протоколи Інтернету рівнів мережного і транспортного, що відповідають за фізичну пересилку повідомлень будь-якого типу між комп'ютерами мережі (протоколи IP і TCP). Ці протоколи настільки тісно зв'язані між собою, досить часто їх позначають терміном "протокол TCP/IP".

П. Інтернету прикладні /п. Интернета прикладные/ — протоколи більш високого рівня, ніж базові протоколи. Відповідають за функціонування спеціалізованих служб Інтернету: протокол HTTP, протокол

FTP, протоколи пошти електронної і т. ін.

П. криптографічний /п. криптографический/ [cryptographic p.] — алгоритм розв'язання деякого завдання захисту інформації методами криптографічними.

П. маршрутизації /п. маршрутизации/ [routing protocol] — протокол, який реалізує алгоритми маршрутизації (див. маршрутизація). П. м. працюють поверх мережних протоколів IP і IPX, які іноді називають маршрутизованими протоколами (routed protocols).

П. обміну /п. обмена/ [communication p.] — послідовність узгоджених приписів, згідно з якими відбувається обмін повідомленнями (token) між сторонами (учасниками) протоколу для досягнення певної мети.

ПРОФІЛЬ /профиль/ [profile] (франц. profil, від італ. profilo — обрис) — 1) Обриси будь-чого збоку. 2) Сукупність основних типових рис будь-чого.

П. захисту /п. защиты/ [Protection P. (PP)] — спеціальний нормативний документ, що регламентує сукупність завдань захисту, функціональних вимог безпеки, вимог гарантій безпеки та їхнього обґрунтування. П. з. визначає вимоги безпеки до певної певної категорії продуктів інформаційної технології, не уточнюючи методи й засоби їхньої реалізації. За допомогою п. з. споживачі формують свої вимоги до розробників IT-продуктів. П. з. містить вступ, опис IT-продукту, середовище експлуатації, завдання захисту, вимоги безпеки, додаткові відомості, обґрунтування. Він служить керівництвом для виробника і розробника IT-продукту, які повинні на його основі і технічних рекомендацій, що запропоновані ним, розробити проект захисту, який служить керівництвом для аналізу кваліфікаційного і сертифікації IT-продукту.

П. захисту: вимоги безпеки /п. защиты: требования безопасности/ [IT security requirements] — розділ профілю захисту, що містить вимоги, яким повинен задовольняти продукт інформаційних технологій для вирішення завдань захисту (типових, спеціальних і т. ін.). В розділі виставляються функціональні вимоги безпеки, вимоги гарантій безпеки, вимоги до середовища експлуатації. Функціональні вимоги повинні містити тільки типові вимоги, передбачені тільки відповідними розділами "критеріїв Загальних". Необхідно

забезпечити такий рівень деталізації вимог, який дозволяє продемонструвати їхню відповідність завданням захисту. Функціональні вимоги можуть дозволяти або забороняти використання конкретних методів і засобів захисту. Вимоги гарантій містять посилання на типові вимоги рівнів гарантій "Загальних критеріїв", проте допускають і визначення додаткових вимог гарантій. Вимоги до середовища експлуатації є необов'язковими і можуть містити функціональні вимоги та вимоги гарантій, яким повинні задовольняти компоненти інформаційних технологій, що складають середовище експлуатації ІТ-продукту. На відміну від попередніх розділів, використання типових вимог "Загальних критеріїв" є бажаними, але не обов'язковими.

П. захисту: вступ /п. защиты: вступление/ [PP introduction] — розділ профілю захисту, який містить всю інформацію для пошуку профілю захисту в бібліотеці профілів. Вступ складається з ідентифікатора профілю захисту та огляду змісту. Ідентифікатор профілю захисту являє собою унікальне ім'я для його пошуку серед подібних йому профілів і позначення посилань на нього. Огляд змісту профілю захисту містить коротку анотацію профілю захисту, на основі якої споживач може зробити висновок про придатність даного профілю захисту.

П. захисту: додаткові відомості /п. защиты: дополнительные сведения/ [PP application notes] — необов'язковий розділ профілю захисту, що містить будь-яку додаткову інформацію, корисну для проектування, розробки, аналізу кваліфікаційного і сертифікації ІТ-продукту.

П. захисту: завдання захисту /п. защиты: задачи защиты/ [security objectives] — розділ профілю захисту, що відображає потреби користувачів у протидії потенційним загрозам безпеці і (або) реалізації політики безпеки. До складу завдань захисту входять завдання захисту продукту інформаційних технологій та інші завдання захисту. Завдання захисту ІТ-продукту повинні визначати й регламентувати потреби в протидії потенційним загрозам безпеці і (або) в реалізації політики безпеки. Інші завдання захисту повинні регламентувати потреби в протидії потенційним загрозам безпеці і (або) в реалізації політики безпеки інших компонентів комп'ютерної системи, що не відносяться до сфери інформаційних технологій.

П. захисту: обґрунтування /п. защиты: обоснование/ [rationale] — розділ профілю захисту, який

повинен демонструвати, що профіль захисту містить повну й зв'язну множину вимог і що продукт інформаційних технологій, який задовольняє їм, буде протистояти загрозам безпеці середовища експлуатації. Розділ складається з обґрунтування завдання захисту і обґрунтування вимог безпеки. Обґрунтування завдань захисту повинно демонструвати, що завдання, які пропонуються у профілі, відповідають параметрам середовища експлуатації, а їхнє вирішення дозволить ефективно протистояти загрозам безпеці і реалізувати політику безпеки. Обґрунтування вимог безпеки показує, що вимоги безпеки дозволяють ефективно вирішувати завдання захисту, оскільки: сукупність цілей окремих вимог безпеки функціональних відповідають встановленим завданням захисту; вимоги безпеки є пов'язаними, тобто не суперечать, а взаємно підсилюються; вибір вимог є виправданим (особливо це відноситься до додаткових вимог); вибраний набір функціональних вимог і рівень гарантій відповідають завданням захисту.

П. захисту: опис IT-продукту /п. защиты: описание ИТ-продукта/ [TOE description] — розділ профілю захисту, який містить коротку характеристику продукту інформаційних технологій, призначення, принцип роботи, методи використання і т.ін. Ця інформація не підлягає аналізу кваліфікаційному і сертифікації, але подається розробникам і експертам для пояснення вимог безпеки й визначення їхньої відповідності завданням, що вирішуються за допомогою IT-продукту.

П. захисту: середовище експлуатації /п. защиты: среда эксплуатации/ [TOE security environment] — розділ профілю захисту, що містить опис усіх аспектів функціонування продукту інформаційних технологій, зв'язаних із безпекою. В середовищі експлуатації описуються умови експлуатації, загрози безпеці, політика безпеки. Опис умов експлуатації IT-продукту повинен містити вичерпну характеристику середовища його експлуатації з точки зору безпеки, в тому числі обмеження на умови його застосування. Опис загроз безпеці, що діють в середовищі експлуатації, яким повинен протистояти захист IT-продукту. Для кожної загрози повинно бути вказане її джерело, метод і об'єкт впливу. Опис політики безпеки повинен визначати і, при необхідності, пояснювати правила політики безпеки, яка повинна бути реалізована в IT-

продукті.

П. захищеності функціональний /п. защищенности функциональный/ — перелік необхідних рівнів послуг безпеки, які повинен реалізовувати комплекс засобів захисту автоматизованої системи, щоб задовольнити певні вимоги щодо захищеності інформації, яка оброблюється в даній автоматизованій системі. Стандартні п. з. ф. будуються на підставі існуючих вимог щодо захисту певної інформації від певних загроз і відомих на сьогоднішній день послуг функціональних, що дозволяють протистояти даним загрозам і забезпечувати виконання вимог, які пред'являються.

П. повноважень /п. полномочий/ — список об'єктів, що захищаються, і прав доступу до них, асоційованих із кожним суб'єктом. При зверненні до об'єкта профіль суб'єкта перевіряється на наявність відповідних прав доступу. профіль представляється у вигляді рядка матриці доступу.

П. функціональний /п. функциональный/ [functionality p.] — упорядкований перелік рівнів функціональних послуг, який може використовуватися як формальна специфікація функціональності системи комп'ютерної.

ПРОЦЕДУРА /процедура/ (франц. procédure, від лат. procedo — просуваюсь, проходжу) — офіційно встановлений чи прийнятий за звичаєм порядок, послідовність дій для здійснення або оформлення якихось справ.

П. автентифікації в телекомунікаційних системах /п. аутентификации в телекоммуникационных системах/ — процедура, призначена для захисту при передаванні в мережі паролів, автентифікаторів логічних об'єктів і т.ін. Для цього використовуються криптографічні методи і протоколи, засновані, наприклад, на процедурі "трикратного рукостискання". Метою таких протоколів є захист від установлення з'єднання з логічним об'єктом, утвореним порушником або діючим під його керуванням з метою імітації роботи справжнього об'єкта.

П. допуску до державної таємниці /п. допуска к государственной тайне/ — офіційно встановлений порядок, послідовність дій для здійснення допуску посадової особи або громадянина до таємниці державної.

Як правило така процедура передбачає: прийняття на себе зобов'язань перед державою за нерозповсюдження довірених їм відомостей, що складають державну таємницю; згоду на часткові, тимчасові обмеження їхніх прав у відповідності до закону; письмова згода на проведення по відношенню до них повноважними органами перевірочних заходів; визначення видів, розмірів і порядку надання пільг, передбачених законом; ознайомлення з нормами законодавства держави про державну таємницю, які передбачають відповідальність за його порушення; прийняття рішення керівником органу державної влади, підприємства, закладу або організації про допуск особи, що оформляється, до державної таємниці.

П. забезпечення цілісності даних в телекомунікаційних системах /п. обеспечения целостности данных в телекоммуникационных системах/ — процедура, яка передбачає введення в кожне повідомлення деякої додаткової інформації, яка є функцією від змісту повідомлення. В рекомендаціях МОС розглядаються методи забезпечення цілісності двох типів: перші забезпечують цілісність поодинокого блока даних, інші — цілісність потоку блоків даних або окремих полів цих блоків. При цьому забезпечення цілісності потоку блоків даних не має сенсу без забезпечення цілісності окремих блоків. Ці методи застосовуються в двох режимах — при передаванні даних по віртуальному з'єднанню і при використанні дейтаграмного передавання. В першому випадку виявляються невпорядкованість, втрати, повтори, вставки даних за допомогою спеціальної нумерації блоків або введенням міток часу. В дейтаграмному режимі мітки часу можуть забезпечити тільки обмежений захист цілісності послідовності блоків даних і запобігти переадресуванню окремих блоків.

П. заповнення потоку в телекомунікаційних системах /п. заполнения потока в телекоммуникационных системах/ — процедура, призначена для запобігання аналізу трафіка. Ефективність застосування цієї процедури підвищується, якщо одночасно з нею передбачене лінійне шифрування всього потоку даних, тобто потоки інформації і заповнення стають нерозбірливими.

П. керування доступом до ресурсів телекомунікаційної системи /п. управления доступом к ресурсам телекоммуникационной системы/ — процедура, що виконується на основі множини правил і фор-

мальних моделей, що використовуються як аргумент доступу до інформації про ресурси (класифікацію) та ідентифікатори абонентів. Службова інформація для керування доступом (паролі абонентів, списки дозволених операцій, персональні ідентифікатори, часові обмежувачі і т. ін.) містяться в локальних базах даних забезпечення безпеки мережі.

П. керування маршрутом в телекомунікаційній системі /п. управления маршрутом в телекоммуникационной системе/ — процедура, призначена для організації передавання тільки маршрутами, утвореними за допомогою надійних і безпечних технічних засобів і систем. При цьому може бути організований контроль з боку одержувача, який у випадку виникнення підозри про компрометацію використовуваної системи захисту може вимагати зміну маршруту.

П. підтвердження характеристик даних в телекомунікаційних системах /п. подтверждения характеристик данных в телекоммуникационных системах/ — процедура, яка передбачає наявність арбітра, який є довіреною особою взаємодіючих абонентів і може підтвердити цілісність, час передавання документів, а також запобігти можливості відмови джерела від видачі будь-якого повідомлення, а споживача — від його приймання.

П. цифрового підпису в телекомунікаційних системах /п. цифровой подписи в телекоммуникационных системах/ — процедура, яка служить для підтвердження правильності змісту повідомлення. Вона засвідчує факт його відправлення власне тим абонентом, який вказаний в заголовку як джерело даних. Підпис цифровий є функцією від змісту таємного повідомлення, відомого тільки абоненту-джерелу, і загальної інформації, відомої всім абонентам системи.

П. шифрування даних в телекомунікаційних системах /п. шифрования данных в телекоммуникационных системах/ — процедура, призначена для закриття всіх даних абонента або декількох полів повідомлення. Може мати два рівні: шифрування в каналі зв'язку (шифрування лінійне) і міжкінцеве (абонентське).

ПРОЦЕС /процесс/ [process] (лат. processus — течія, хід) — послідовність передбачених подій, яка визна-

чається об'єктом або явищем і відбувається в заданих умовах; хід подій, що відбуваються у відповідності з наміченою метою або результатом.

П. випадковий (імовірнісний, стохастичний) /п. случайный (вероятностный, стохастический)/ [random (probability, stochastic) p.] — процес, один або декілька параметрів якого міняються випадково, у відповідності з деяким імовірнісним законом розподілу.

П. випадковий стаціонарний /п. случайный стационарный/ [stationary random p.] (від лат. stationarius — нерухомий) — процес випадковий, властивості якого не залежать від часу.

П. інформаційні /п. информационные/ [information p.] — процеси створення, збирання, оброблення, накопичення, зберігання, пошуку, розповсюдження і споживання інформації в державі і суспільстві, а також процеси створення і застосування систем інформаційних, технологій інформаційних і засобів їхнього забезпечення, засобів і механізмів безпеки інформаційної.

П. інформаційно-обчислювальний /п. информационно-вычислительный/ — процес функціонування інформаційно-обчислювального комплексу. Включає вирішення задач обчислювальних і забезпечення користувача інформацією.

П. марківський /п. марковский/ [Markoff (Markovian) p.] — випадковий процес, значення якого в моменти часу, що являють собою послідовність, яка збільшується, створюють ланцюг Маркова, тобто послідовність випадкових величин, для якої при відомому значенні будь-якої з цих величин сукупність попередніх їй величин не залежить від сукупності наступних за нею величин. Ланцюгом Маркова називають також послідовність випробувань з випадковими виходами, якщо при відомому результаті довільного випробування сукупність результатів попередніх випробувань не залежить від сукупності результатів наступних випробувань.

П. нестаціонарні випадкові /п. нестационарные случайные/ — процеси випадкові, властивості яких змінюються у часі.

П. обчислювальний /п. вычислительный/ [calculation p.] — процес вирішення різноманітних задач

на ЕОМ.

ПРОЦЕСОР /процессор/ [processor] (англ. processus, від лат. procedo — просуваюся) — 1) Пристрій або функціональна частина ЕОМ, призначена для виконання обчислень за програмою. 2) Машинна програма, яка здійснює деяке попереднє обчислення або організацію.

П. центральний (ЦП) /п. центральный (ЦП)/ [Central Processing Unit (CPU)] — процесор, що виконує в даній обчислювальній системі основні функції з оброблення даних і керування роботою інших частин цієї системи.

ПСЕВДОНІМ /псевдоним/ [pseudonym] (від грец. *ψευδώνυμος* — несправжньо іменований) — кличка або символічне позначення, яке присвоюється розвідникові або агентові з метою забезпечення безпеки його листування або переговорів з керівним центром (на випадок перехоплення повідомлення противником).

ПСИХІКА /психика/ [psyche] (від грец. *ψυχικός* — душевний) — функція мозку, що полягає у відображенні об'єктивної дійсності. Виникла і розвинулася у вищих тварин у процесі біологічної еволюції у зв'язку з розвитком нервової системи, що регулює відносини організму із середовищем. Найважливіша особливість — активність. Вища форма п. — свідомість — притаманна тільки людині. Психічна діяльність (відчуття, сприйняття, пам'ять, почуття, воля, мислення і т. ін.) вивчається психологією.

П. людини /п. человека/ — система споживчо-мотиваційних (знання, переконання, ціннісні орієнтації, потяг, бажання), інтелектуально-пізнавальних (відчуття, сприйняття, уявлення, пам'ять і мислення), емоційно-вольових (емоції, почуття, настрої, вольові процеси) і комунікативно-поведінкових (характер і особливості спілкування, взаємодії, взаємовідносин, міжособистісного сприйняття) компонентів. Є об'єктом впливу психологічного. П. л. може функціонувати врівноважено або з перекосом в існуючих взаємозв'язках. Цей чи інший стан визначається ефектом дисонансу когнітивного.

ПСИХО... /психо.../ [psycho...] (від грец. *ψυχή* — душа) — у складних словах відповідає поняттям психіка, психічний.

ПСИХОЛОГІЯ /психология/ [psychology] (від психо... і ...логія, що від грец. *λόγος* — слово, вчення) —

наука про закономірності, розвиток і форми психічної діяльності (психіки) живих істот як особливої форми життєдіяльності. Вона вивчає процеси активного відображення людиною й тваринами об'єктивної реальності у формі психічних явищ — сприйняття, інтелекту, здібностей, пам'яті, почуття і т.ін. Предметом п. є як свідомі, так і неусвідомлювані психічні процеси і явища. П. виявляє характер відповідності дійсних мотивів, установок, орієнтації особистості уявленням, які склалися в неї. П. розвивається в тісному контакті з фізіологією й неврологією з одного боку і філософією, соціологією з іншого боку,. Взаємне збагачення ідеями здійснюється також між п. і інформатикою, п. і мовознавством, п. і економічними та іншими науками. Існують різноманітні галузі п. такі, як вікова, інженерна, воєнна, медична, соціальна п., п. мистецтва, праці, творчості, нейропсихологія, психолінгвістика, психофізика та багато інших.

П. когнітивна /п. когнитивная/ [cognitive p.] — складова частина когнітології і психології, що вивчає, як люди одержують інформацію про світ, як ця інформація уявляється людиною, як вона зберігається в пам'яті і перетворюється в знання і як ці знання впливають на її увагу і поведінку. П. к. охоплює весь діапазон психологічних процесів — від відчуття до сприйняття, розпізнавання образів, уваги, навчання, пам'яті, формування понять, мислення, уяви, запам'ятовування, мови, емоцій і процесів розвитку.

П. національна /п. национальная/ — складова частина духовного життя суспільства, яка відображає те спільне, що у представників цілої нації (етносу) в уяві, стійких формах поведінки, рисах психологічного складу, в реакціях, мовленні і мові, відносинах з іншими людьми та природою.

П. соціальна /п. социальная/ — розділ психології, який вивчає закономірності діяльності людей в умовах взаємодії в групах соціальних. Основними проблемами п. с. є: закономірності спілкування й взаємодії людей, діяльність великих (нації, класи) і малих соціальних груп, соціалізація особистості й розвиток соціальних установок.

ПСИХОТРОНІКА /психотроника/ (від психо... і (елек)троніка) — наука про механізми інформаційних зв'язків, регуляції і керування психікою, енергетикою і фізіологією людини.

ПСІ-ПРОБЛЕМА /ПСИ-проблема/ — психофізична проблема ідентифікації і управління станом свідо-

мості і психіки.

ПУБЛІЦИСТИКА /публицистика/ [publicism] (нім. Publizistik, від лат. publicus — суспільний, народний) — рід літератури, що висвітлює актуальні суспільно-політичні та інші проблеми сучасності в періодичній пресі й окремих виданнях.

ПУЛЬТ /пульт/ [console, panel] (нім. Pult, від лат. pultitum — підмостки) — панель з органами керування і індикації, яка призначена для керування системою або пристроями і контролю за їхньою роботою.

П. централізованого спостереження /п. централизованного наблюдения/ — пульт, призначений для централізованого приймання, оброблення і індикації інформації комплексів технічних засобів охорони з об'єктів охорони. Він забезпечує: контроль стану об'єкта, що охороняється; узяття об'єкта під охорону і зняття з охорони; автоматичне перемикання апаратури автоматичної телефонної станції на засоби охорони; реєстрацію порушення шлейфів об'єктів, що охороняються, з виявленням номера об'єкта і характеру порушення; світлову індикацію номера об'єкта, де відбулося порушення. Для забезпечення більш ефективної охорони в системах охорони об'єктів разом із комплексами технічних засобів охорони застосовують засоби спостереження телевізійні, що складають основу підсистеми спостереження. Це дозволяє не тільки одержувати інформацію про факт порушення рубежів захисту, але і бачити зловмисників та спостерігати за їхніми діями з метою вибору раціональних дій у відповідь.

ПУНКТ /пункт/ [post, point, subscriber station, terminal] (нім. Punkt, від лат. punctum — крапка — місце зосередження чого-небудь.

П. абонентський (АП) /п. абонентский (АП)/ [subscriber t.] — комплекс технічних засобів в системі телеоброблення даних, призначений для обміну інформацією між віддаленим користувачем і ЕОМ; робоче місце віддаленого користувача (абонента). АП забезпечує введення даних, передачу їх лініями зв'язку в ЕОМ і назад, виведення даних.

П. контрольно-проїзний /п. контрольно-проездной/ — пункт контрольно-пропускний, призначений для контрольованого пропускання на територію, що охороняється, транспорту. П. к.-п. для пропускання

авто- та залізничного транспорту обладнуються: розсувними або розкривними воротами і шлагбаумами з механічним, електромеханічним і гідравлічним приводами, а також пристроями для аварійного зупинення воріт і відкривання їх руками; контрольними площадками з підмостками для перегляду транспорту; світлофорами, попереджувальними знаками і відповідними світловими табло; телефонним і тривожним зв'язком і освітленням для огляду транспорту.

П. контрольно-пропускний (КПП) /п. контрольно-пропускной (КПП)/ [check-point] — споруда конструкцій захисту інженерних об'єкта, призначена для контрольованого пропускання на територію, що охороняється, людей і транспорту. КПП бувають автоматизовані і автоматичні, прохідні для людей і проїзні для транспорту. В найзагальнішому випадку КПП містить: зал із засобами керування доступом для проходу людей; бюро перепусток; камеру зберігання речей персоналу і відвідувачів, не дозволених для проносу в організації; приміщення для начальника охорони, чергового контролера, розташування охоронної сигналізації і зв'язку та інші; засоби керування доступом транспорту. Конструкція, склад і кількість КПП визначаються розмірами території і кількістю персоналу. КПП повинні забезпечувати необхідну пропускну здатність людей і транспорту. Запасні входи і проїзди для пропускання людей і транспорту в аварійних ситуаціях у нормальних умовах закриваються, пломбуються або запечатуються.

П. радіоконтролю /п. радиоконтроля/ [radio monitoring p.] — підрозділ (заклад), призначений для контролю за роботою засобів радіоелектронних з метою попередження витоку інформації з обмеженим доступом. Може бути стаціонарним або рухомим.

Р

РАДІО... /радио.../ [radio...] (від лат. radius — промінь) — частина складних слів, що вказує на зв'язок із поняттям "радіо" або "радіоактивність".

РАДІОВИПРОМІНЮВАННЯ /радиоизлучение/ [radio frequency emission] (від радіо... і випромінювання) — те ж, що випромінювання радіочастотне.

РАДІОВІДБИВАЧІ /радиоотражатели/ — засоби приховування інформаційного об'єктів радіолокаційного спостереження. До р. відносяться кутові, лінзові, дипольні та перевипромінюючі антенні решітки. Відбивачі кутикові, лінзові, перевипромінюючі антенні решітки, розташовані поблизу об'єкта, що потребує захисту, створюють на екрані РЛС багаточисельні яскраві засвітлення, серед яких важко виявити сам об'єкт. Для маскування повітряних об'єктів застосовують відбивачі дипольні.

РАДІОГРА /радиоигра/ (від радіо... і гра) — див. гра оперативна.

РАДІОГРАМА /радиограмма/ [radiogram] (від радіо... і ...грама, що від грец. $\gamma\rho\acute{\alpha}\mu\mu\alpha$ — літера, риска, написання) — повідомлення, передане по радіо; скорочена назва радіотелеграми.

РАДІОДАНІ /радиоданные/ [radiodate] (від радіо... і дані) — частоти (пакети частот), індекси, паролі, позивні (адресні коди) радіостанцій (див. робоча частота, радіопароль, радіопозивний, а також ключі до таблиць позивних та інші дані, необхідні для радіообміну.

РАДІОДЕЗІНФОРМАЦІЯ /радиодезинформация/ [radio misinformation] (від радіо... і дезінформація) — навмисне перекручення повідомлень, що передаються по радіозв'язку, з метою створення у користувачів цих повідомлень хибного уявлення. Р. використовується для введення противника в оману шляхом передавання фальшивих повідомлень, перекручень дійсного режиму роботи та розташування випромінюючих засобів радіоелектронних за рахунок уведення в дію фальшивих станцій, посилення роботи передавальних РЕЗ на другорядних напрямках при збереженні попереднього або скороченні режиму їхньої роботи на головному напрямку і т.ін.

РАДІОДІАПАЗОН /радиодиапазон/ [radio-frequency region](від радіо... і діапазон) — діапазон (ділянка, смуга) частот або довжин радіохвиль.

РАДІОЗАВАДИ /радиопомехи/ [radio-(frequency) n.] (від лат. radius — промінь і завади) — радіосигнали, що ускладнюють або зовсім порушують роботу радіотехнічних засобів, систем радіозв'язку, заважають розбірливості та якості звукового прийому, створюють порушення телевізійного і радіолокаційного зображення, спотворюють телеграфні знаки і т.ін. В залежності від походження завади можуть бути природні і

штучні, навмисні і ненавмисні.

РАДІОЗАКЛАДКА /радиозакладка/ [radio b.] — пристрій закладний випромінюючий, носієм інформації від якого є випромінювання електромагнітне в радіодіапазоні.

РАДІОЗВ'ЯЗОК /радиосвязь/ [radiocommunication] (від радіо... і зв'язок) — електрозв'язок, що здійснюється шляхом випромінювання та приймання хвиль електромагнітних за допомогою радіостанцій.

РАДІОКОНТРОЛЬ /радиоконтроль/ [radiomonitoring] (від радіо... і контроль) — спостереження за встановленим порядком роботи радіозв'язку з метою перевірки виконання вимог скритого управління, режимів роботи, заходів радіомаскування, норм технічної експлуатації та правил ведення радіозв'язку. Здійснюється за допомогою пунктів радіоконтролю.

РАДІОЛОКАТОР /радиолокатор/[radar (device)] (від радіо... і локатор) — див. станція радіолокаційна.

РАДІОЛОКАЦІЯ /радиолокация/ [radiolocation] (від радіо... і локація) — галузь науки і техніки, предметом якої є спостереження різних об'єктів (цілей) радіотехнічними методами: виявлення, розпізнавання, визначення місцезнаходження (координат) цілей і т.ін. Під р. розуміють також сам процес радіолокаційного спостереження (локації) об'єктів за допомогою РЛС. Для цього використовують відбиті від об'єктів або випромінювані об'єктами радіохвилі різної довжини (від часток мм до сотень м). Розрізнюють активну та пасивну радіолокацію Відстань від об'єкта вимірюється шляхом визначення часу, необхідного для проходження радіохвилями відстані від пункту спостереження (пряма хвиля) і назад (відбита хвиля).

РАДІОМАСКУВАННЯ /радиомаскировка/ [radio ca-mouflage] — комплекс радіотехнічних і організаційних заходів, спрямованих на зниження ефективності радіорозвідки противника. Досягається шляхом обмеження часу роботи своїх радіостанцій на передавання, зменшення потужності випромінювання, використання спрямованих антен, апаратури швидкої дії, створення фальшивих радіомереж і радіонапрямків та іншими методами.

РАДІОМЕТР /радиометр/ [radiometer] — 1) Прилад для реєстрації і вимірювання енергії радіовипромінювання малої потужності. 2) Прилад для виявлення і вимірювання енергії електромагнітного випроміню-

вання оптичного діапазону, яке випромінюється нагрітими тілами. 3) Прилад для виявлення і вимірювання ступеню радіоактивного зараження різноманітних поверхонь і середовищ.

РАДІОМІКРОФОН /радиомикрофон/ [radiomicrophone] (від радіо... і мікрофон) — мікрофон, об'єднаний з радіоканалом передавання звукової інформації. Р., що використовуються як пристрої закладні, називають ще радіозакладками, радіобагами, радіокапсулами, а іноді "жучками".

РАДІОМОВЛЕННЯ /радиовещание/ [radio broadcasting] (від радіо... і ...мовлення) — засіб масової інформації, що забезпечує передавання текстових і музичних передач на відстань за допомогою електромагнітних хвиль.

РАДІОМОНІТОРИНГ /радиомониторинг/ [radio monitoring] (від радіо... і моніторинг) — безперервне слідкування за випромінюваннями радіочастотними в навколишньому середовищі з метою інформування про стан їхніх джерел та параметри випромінювань.

Р. приміщень /р. помещений/ — безперервне і послідовне слідкування за радіочастотними випромінюваннями в приміщенні з метою запобігання витоку інформації по каналу радіоелектронному. Р. п. здійснюється за допомогою комплексів радіомоніторингу приміщень автоматизованих. При безперервному контролі накопичується великий обсяг інформації про електромагнітну обстановку в приміщенні, що полегшує і прискорює процес виявлення нових джерел випромінювання. При цьому виявляються не тільки закладки, що випромінюють безперервно або вмикаються при дії акустичного сигналу, але і радіовипромінювання закладок, що управляються дистанційно, в період їхньої активної роботи, тобто створюються передумови для боротьби із закладними пристроями у реальному масштабі часу. При р. п. виявляються інформативні побічні випромінювання різноманітних радіоелектронних засобів, для виявлення яких із-за великої невизначеності їхнього прояву і малої потужності потрібний більш ретельний аналіз радіообстановки в приміщенні.

РАДІООБМІН /радиообмен/ (від радіо... і обмін) — процедура приймання і передавання інформації в системах радіозв'язку. Відмінності у використання правил р. є формою прояву ознак систем радіозв'язку.

РАДІОПЕЛЕНГАТОР /радиопеленгатор/ [radio direction finder] (від радіо... і пеленгатор) — радіотехнічний приймально-індикаторний пристрій для визначення радіопеленга (пеленга) на джерела випромінювання електромагнітного. Основу р. складає радіоприймач з антеною, діаграма спрямованості якої має гострий максимум або мінімум. Обертаючи антену в напрямку досягнення максимуму (мінімуму) сигналу на виході антени, визначають напрямок на джерело радіовипромінювання.

РАДІОПЕРЕДАВАЧ /радиопередатчик/ [radio transmitter] (від радіо... і передавач) — технічний пристрій для одержання модульованих електричних коливань в діапазонах радіочастот з метою їхнього послідовного випромінювання (антеною) у вигляді хвиль електромагнітних. Р. — важлива частина систем і засобів передавання інформації за допомогою радіохвиль (радіозв'язок, радіолокація і т. ін.).

РАДІОПЕРЕДАЧА /радиопередача/ [radio broadcast, radio transmission] (від радіо... і передача) — формування і випромінювання сигналу радіочастотного.

РАДІОПРИЙМАННЯ (РАДІОПРИЙОМ, ПРИЙМАННЯ) /радиоприем (прием)/ [reception] — виділення сигналів із випромінювання радіочастотного.

РАДІОПРИЙМАЧ /радиоприемник/ [radio receiver] (від радіо... і приймач) — технічний засіб перехоплення, що здійснює пошук, селекцію, приймання й оброблення радіосигналів. За принципом побудови розрізняють два види приймачів: прямого підсилення і супергетеродинні. Можливості р. визначаються наступними технічними характеристиками: діапазоном частот, що приймаються; чутливістю; вибірковістю; динамічним діапазоном; якістю відтворення сигналу, що приймається; експлуатаційними параметрами.

РАДІОПЕРЕХОПЛЕННЯ /радиоперехват/ [radiointerseption] (від радіо... і перехоплення) — перехоплення інформації шляхом виявлення, приймання та реєстрації радіовипромінювання з метою подальшого розкривання змісту повідомлень, які передаються за допомогою різноманітних засобів радіозв'язку; спосіб радіорозвідки.

РАДІОРЕЛЕЙНИЙ /радиорелейный/ [radiorelaying] (від радіо... і реле) — пов'язаний з передаванням сигналів через ряд приймально-передавальних радіостанцій (див. зв'язок радіорелейний, лінія зв'язку ра-

діорелейна).

РАДІОРОЗВІДКА /радиоразведка/ [COMmunications INTelligence (COMINT)] (від радіо... і розвідка) — вид розвідки радіоелектронної, призначений для добування інформації семантичної шляхом перехоплення радіосигналів з інформацією конфіденційною.

РАДІОСИГНАЛ /радиосигнал/ [radio-frequency signal] (від радіо... і сигнал) — сигнал у вигляді радіовипромінювання або сигнал в електричному колі на одній з радіочастот.

РАДІОСЛУЖБА /радиослужба/ [radio service] (від радіо... і служба) — служба, яка здійснює передавання та (або) приймання радіовипромінювання з певною метою.

РАДІОСТАНЦІЯ /радиостанция/ [broadcasting station, radio station] (від радіо... і станція) — 1) Сукупність технічних пристроїв і апаратури для передавання й приймання інформації за допомогою радіохвиль. 2) Один або декілька радіопередавачів або радіоприймачів, або комбінація радіопередавачів і радіоприймачів, включаючи допоміжне обладнання, необхідне в певному місці для організації радіозв'язку.

РАДІОТЕЛЕГРАФ /радиотелеграф/ [radiotelegraph] (від радіо... і телеграф) — телеграф, який передає повідомлення кодом за допомогою радіохвиль.

РАДІОТЕЛЕТАЙП /радиотелетайп/ [radio teletype] (від радіо... і телетайп) — літеродрукувальний апарат (телетайп) з радіозв'язком.

РАДІОТЕЛЕФОН /радиотелефон/ [radiophone, radiotelephone] (від радіо... і телефон) — сукупність передавальної і приймальної апаратури для зв'язку телефонного по радіо.

Р. стільникового зв'язку /р. сотовой связи/ [cellular r.] — радіостанція рухома системи стільникового радіозв'язку.

РАДІОТЕПЛОЛОКАТОР /радиотеплолокатор/ (від радіо... і теплолокатор) — радіоелектронний пристрій для виявлення об'єктів (цілей), визначення їхніх кутових координат і одержання відомостей про деякі їхні фізичні характеристики методами радіотеплолокації. Складовими частинами являються: радіометр, який забезпечує вимірювання рівнів радіотеплового випромінювання, антенне, індикаторне обладнання,

допоміжні пристрої і джерела електроживлення.

РАДІОТЕПЛОЛОКАЦІЯ /радиотеплолокация/ [radio-heat location] (від радіо..., тепло і локація) — визначення місцезнаходження об'єктів за їхнім радіотепловим випромінюванням; вид пасивної радіолокації. Радіотеплове випромінювання властиве усім фізичним тілам, температура яких вища абсолютного нуля (–273,15°С). Воно має відносно малу інтенсивність (від сотих до десятих часток процента в міліметровому та дециміліметровому і від сотих до тисячних часток процента в сантиметровому та дециметровому діапазонах радіохвиль від загального теплового випромінювання. Виявлення об'єктів здійснюється за рахунок контрасту інтенсивності радіотеплового випромінювання цих об'єктів відносно радіотеплового випромінювання фону, на якому проводиться спостереження. Безпосередніми вимірюваннями за допомогою радіотеплолокаторів визначають кутові координати об'єктів. Дальність та швидкість їхнього переміщення одержують непрямими (базовими) методами. Основним режимом роботи при р. є радіотеплопеленгація. За допомогою р. вирішуються задачі визначення координат наземних, надводних, повітряних та космічних об'єктів. Вона може використовуватися також для навігації, самонаведення засобів ураження на джерела радіотеплового випромінювання, виявлення джерел теплової енергії, вимірювання розподілення температур на об'єктах і т.ін. Поєднання скритності і всепогодності є позитивною якістю р. у порівнянні з інфрачервоною технікою і засобами активної радіолокації. Недоліком р. є неможливість безпосереднього вимірювання дальності і швидкості руху об'єкта (цілі), а також великий вплив на роботу радіотеплолокаторів штучних та природних завад.

РАДІОХВИЛЕВОДИ /радиоволноводы/ [radio waves](від радіо... і хвилевід) — металеві труби і діелектричні стрижні або канали, в яких розповсюджуються радіохвилі. Р. служать фідерними системами (див. фідер) в радіолокаційних та інших системах для передавання радіосигналу від передавача в передавальну антену і від приймальної антени до приймача.

РАДІОХВИЛІ /радиоволны/ [radio waves] (від радіо... і хвилі) — електромагнітні коливання (хвилі) частотою до 3 ТГц, що поширюються у просторі без штучних напрямних ліній. В залежності від довжини

та особливостей випромінювання антенними пристроями, р. поширюються в просторі як уздовж земної (водної) поверхні (хвилі поверхневі), так і вгору, під кутом до горизонту (хвилі просторові). За частотою р. класифікуються у відповідності до Регламенту радіозв'язку, затвердженого на Всесвітній адміністративній конференції в Женеві у 1979 р. (див. діапазон радіочастот). В залежності від довжини, а також особливостей генерування, випромінювання, розповсюдження і приймання виділяють діапазони радіохвиль.

РАДІОЧАСТОТА /радиочастота/ [radio frequency] (від радіо... і частота) — частота радіохвилі. Р., що використовуються в радіотехніці, розподіляються між державами за міжурядовими угодами та рекомендаціями міжнародних організацій.

РАДІОШПІОНАЖ /радиошпионаж/ (від радіо... і шпіонаж)— цілеспрямовані приховані дії з перехоплення сигналів, якими обмінюються між собою люди або технічні засоби за допомогою засобів електрозв'язку.

РАНДОМІЗАЦІЯ /рандомизация/[randomization] — надання випадкового характеру відкритому текстові. При цьому звичайно відкритий текст з алфавітом A перетворюється в текст з більшим розміром алфавіту $\acute{A}$, а кожний символ заміщується символами з групи символів алфавіту $\acute{A}$. Кількість символів в групі визначається частотою символу у відкритому тексті. Р. застосовується як один з практичних методів підвищення стійкості криптосистем.

РЕАГУВАННЯ /реагирование/ [response] (від лат. префікса re..., що означає зворотну або повторну дію та ago — дія) — виявлення свого ставлення до чогось, відповідь якимось чином на ту чи іншу дію, дія під впливом чого-небудь.

Р. просте /р. простое/ [simple r.] — реакція системи захисту інформації на несанкціоновані дії в інформаційно-обчислювальній мережі (ІОМ). Р. п. може включати наступні дії: сигналізацію про доступ несанкціонований; блокування (вимкнення термінала, групи терміналів, елементів ІОМ і т. ін.); відмову в запиті.

РЕАКЦІЯ /реакция/ [reaction] — дія, стан, процес, що виникають за певних умов у відповідь на будь-які впливи, подразнення, враження.

РЕВІЗІЯ /ревизия/ [audit, inspection] (від лат. revisio — перегляд) — обстеження, перевірка стану або результатів діяльності.

Р. бази даних /р. базы данных/ [database a.] — перевірка цілісності, несуперечливості, ненадлишку та інших показників бази даних, а також ефективності функціонування банка даних в цілому, що здійснюється за допомогою спеціальних перевірочних програм.

РЕВІЗОР /ревизор/ [auditor] (від лат. revisor — той, що перевіряє) — в обчислювальній техніці — антивірусна програма (див. антивірус), яка перевіряє диски шляхом їхнього читання на фізичному рівні, що дозволяє виявляти такі віруси, як вірус-невидимка та вірус-мутант.

РЕГІСТР /регистр/ [register] (від лат. registrum — список, перелік) — 1) Список, показник будь-чого, книга для записів. 2) Ряд клавіш в друкувальних та обчислювальних машинках. 3) В обчислювальній техніці - внутрішній запам'ятовуючий пристрій процесора або адаптера для тимчасового збереження інформації та забезпечення швидкого доступу до неї.

Р. зсуву лінійний /р. сдвига линейный/ [linear shift feedback r.] — пристрій, який обчислює лінійну функцію з лінійним зворотнім зв'язком від "вхідних" даних. Послідовність "вихідних" даних р. з. л. є лінійною рекурентною послідовністю. Л. р. з. є одним з елементів побудови схем шифрів потокових.

РЕГЛАМЕНТ /регламент/ [regulations] (польс. reglament, від франц. reglement, від лат. regula — правило) — звід, система правил, які визначають порядок організації і діяльності органів державної влади в цілому та їхніх складових частин.

Р. радіозв'язку /р. радиосвязи/ — звід правил, що регулюють порядок використання країнами — членами Міжнародної спілки радіозв'язку будь-яких радіостанцій (а також інших радіо- і електротехнічних пристроїв), що випромінюють радіохвилі (і власне тим здатних створювати завади радіоприйому). Прийнятий в 1906 році на 1-й Міжнародній адміністративній конференції в Берліні; і відтоді багатократно переглядався і доповнювався.

РЕГЛАМЕНТАЦІЯ /регламентация/ [regulation] (франц. réglementation) — установлення певних пра-

вил.

Р. доступу до інформації /р. доступа к информации/ — установлення часових, територіальних і режимних обмежень в діяльності співробітників організації і роботі технічних засобів, спрямовані на забезпечення безпеки інформації. Регламентація доступу передбачає: установлення меж зон контрольованих і охоронних; визначення рівнів захисту інформації в зонах; регламентацію діяльності співробітників і відвідувачів (розроблення розпорядку дня, правил поведінки співробітників в організації і поза нею і т. ін.); визначення режимів роботи технічних засобів, в тому числі збирання, оброблення і зберігання інформації, що потребує захисту, на ПЕОМ, передавання документів, порядку складування продукції і т. ін.

РЕЄСТРАЦІЯ /регистрация/ [registration, recording] (від польс. rejestr, що від лат. regesta — списки, перелік) — 1) Взяття на облік, внесення до списку якихось даних, записів про певні факти. 2) Послуга безпеки, що забезпечує збирання й аналіз інформації щодо використання користувачами і процесами функцій і об'єктів, контрольованих комплексом засобів захисту. 3) Запис інформації на паперовий або інший носій з метою її збереження і наступного використання.

Р. доменної адреси /р. доменного адреса/ — внесення імені і відповідної йому IP-адреси в базу даних DNS-сервера. Реєстрація в доменах верхнього рівня платна. Реєстрація доменів нижнього рівня безкоштовна і виконується провайдером.

Р. інформаційних ресурсів /р. информационных ресурсов/ — процес, який разом з обліком інформаційних ресурсів забезпечує реалізацію функцій контролю за станом ресурсів інформаційних та компонентів системи захисту інформації в системі обчислювальній.

Р. користувачів /р. пользователей/ [user logging] — процес входу користувача в інформаційну систему.

Р. сервера в пошуковій системі /регистрация сервера в поисковой системе/ — процедура внесення адреси сервера в базу даних, що індексуються, серверів системи пошукової. Якщо необхідно, щоб інформацією, розташованою на сайтах, познайомилася достатня кількість користувачів мережі, необхідно зареєструвати покажчик URL сервера в пошуковій системі. Для проведення реєстрації досить звернутися

по посиланню Add URL на першій сторінці пошукової системи.

РЕЖИМ /режим/ [mode] (франц. régime, від лат. regimen — правління) — система правил, заходів, запроваджуваних для досягнення певної мети.

Р. блочних шифрів /р. блочных шифров/ [block cipher modes of operation] — варіанти застосування блочного шифру до відкритого тексту, довжина якого більше довжини блока. Найпростіший варіант — відкритий текст розбивають на блоки та шифрують кожний блок окремо. Такий режим іменується режимом електронної кодової книги (Electronic Codebook) (як в DES) або режимом звичайної заміни (як в ГОСТ 28147-89). Однак цей режим в багатьох практичних застосуваннях має істотні недоліки, пов'язані, наприклад, з тим що однакові блоки відкритого тексту шифруються однаково, незалежно від положення блоків в цілому тексті. Це обумовлює використання таких режимів як режим зчеплення блоків (Cipher Block Chaining), режим шифрування зі зворотним зв'язком за криптотекстом (Cipher Feedbback) та режим шифрування зі зворотним зв'язком за виходом (Output Feedback). В ГОСТ 28147 цим режимам відповідають режим вироблення імітовставки, гаммування зі зворотним зв'язком та гаммування. Застосування різних режимів блочних шифрів викликане передусім можливістю застосування цих криптографічних примітивів для побудови кодів автентифікації повідомлень, генераторів псевдовипадкових послідовностей, шифрів потокових.

Р. забезпечення безпеки /р. обеспечения безопасности/ [security processing m.] — опис усіх категорій допуску усіх користувачів у відповідності до всіх категорій захисту інформації, що повинна зберігатися і оброблятися в системі.

Р. спеціальний /р. специальный/ [dedicated m.] — режим забезпечення безпеки, при якому вся інформація в системі розглядається як інформація одного рівня секретності, рівнодоступна для всіх користувачів системи.

РЕЗИДЕНТ /резидент/ [resident, fixed-post spy, chief of a country's intelligence operations in another country] (франц. résident, від лат. residens (residentis) — той, що залишається на місці) — 1) За часів середньовіччя

дипломатичний представник, що постійно перебуває в даній країні. 2) Таємний уповноважений іноземної розвідки, який на території даної держави спрямовує діяльність своїх агентів; керівник мережі агентурної або групи за кордоном.

РЕЗИДЕНТУРА /резидентура/ — розвідувальна група, що діє за кордоном, якою керує резидент.

Р. нелегальна /р. нелегальная/ — група агентів, що підпорядковуються нелегальному резидентові і займаються збиранням інформації розвідувальної.

РЕКВІЗИТИ /реквизиты/ [Essential Elements (EE)] (лат. requisitum — необхідне, потрібне, від requiro — потребую) — обов'язковий елемент оформлення офіційних документів: дата, місце складання, адреса, підписи, печатка і т. ін.

Р. носіїв відомостей, що складають державну таємницю /р. носителей ведомостей, составляющих государственную тайну/ — реквізити, які наносяться на носії інформації, що складає таємницю державну. Вони включають наступні дані: про ступінь секретності наявних відомостей з посиланням на відповідний пункт діючого в даному органі державної влади, на даному підприємстві, в даних закладі або організації переліку відомостей, що належать засекречуванню; про орган державної влади, про підприємство, заклад, організацію, що здійснила засекречування носія; про реєстраційний номер; про дату або умови розсекречення відомостей або про подію, після настання якої відомості можуть бути розсекречені. При неможливості нанесення таких реквізитів на носій відомостей, що складають державну таємницю, ці дані вказуються в супроводжувальній документації на цей носій. Якщо носій містить складові частини з різноманітними ступенями секретності, кожній зі складових частин надається відповідний гриф секретності, а носієві в цілому надається гриф секретності, відповідно до того грифа секретності, який надається його складовій частині, що має вищу для даного носія ступінь секретності відомостей. Окрім перелічених реквізитів на носії і (або) супроводжувальній документації до нього можуть проставлятися додаткові відмітки, що визначають повноваження посадових осіб стосовно ознайомлення з відомостями, що містяться в цьому носії.

РЕКОМЕНДАЦІЇ /рекомендации/ [recommendation] (від лат. recommendatio — доручення) — вказівки, поради.

Р. до збирання персональної інформації /р. к сбору персональной информации/ — сукупність рекомендацій, щодо збирання інформації персональної в суспільстві інформаційному: збирання й зберігання інформації, що ідентифікує людину, повинні бути мінімальними; інформаційні системи повинні надавати людям право вирішувати самим, чи відкривати або закривати відомості про них; проектування інформаційних систем повинно враховувати необхідність захисту персональної інформації; громадяни повинні мати доступ до можливостей, які надає найновіша технологія захисту особистої таємниці; захист персональних відомостей і особистого життя повинен стати центральним пунктом політики, що забезпечує право громадян на анонімність в інформаційних системах. Основними засобами реалізації рекомендацій можуть стати криптографічні механізми захисту інформації, зокрема підпис цифровий і шифрування.

Р. МОС для захисту інформації в телекомунікаціях /р. МОС по защите информации в телекоммуникациях/ [ISO Recommendations] — процедури, рекомендовані Міжнародною організацією зі стандартизації (ISO) для створення служб сервісних захисту інформації в мережах телекомунікацій.

РЕКОМЕНДАЦІЇ МСЕ /рекомендации МСЭ/ [ITU-T Recommendations] — стандарти зв'язку, рекомендовані сектором телекомунікаційної стандартизації Міжнародної спілки електрозв'язку (МСЕ) [International Telecommunication Union Telecommunication standardization sector (ITU-T)] для використання в усьому світі.

Р. МСЕ X.509 /р. МСЭ X.509/ [ITU-T Recommendations X.509] — рекомендації МСЕ серії X, які визначають формат для сертифікатів відкритого ключа і списків скасованих сертифікатів. Рекомендації використовує стандарт міжнародний ISO/IES 9694-8.

Р. МСЕ X.800 /р. МСЭ X.800/ [ITU-T Recommendations X.800] — рекомендації МСЕ серії X, присвячені опису архітектури по відношенню до моделі взаємодії відкритих систем, включаючи опис розташування механізмів і служб безпеки на рівнях моделі. Рекомендації складають основу стандарту міжнародного ISO

7498-2.

Р. МСЕ Х.810-Х.816 /р. МСЭ Х.810-816/ [ITU-T Recommendations X.810-816] — рекомендації МСЕ серії Х із захисту інформації. Складаються з опису семи архітектур безпеки, а саме: архітектура контролю доступу; архітектура забезпечення ненегативності й розбору конфліктних ситуацій; архітектура забезпечення цілісності; архітектура забезпечення конфіденційності; архітектура аудита систем безпеки. Рекомендації складають основу стандарту ISO/IES 10181.

Р. МСЕ серії Х /р. МСЭ серии Х/ [Series X Recommendations] — сукупність рекомендацій МСЕ щодо мереж передавання даних загального користування. Охоплює питання сполучення відкритих систем [Open Systems Interconnection (OSI)], міжмережний обмін, системи оброблення повідомлень, роботу і системні аспекти OSI, управління OSI.

РЕПОРТАЖ /репортаж/ [report(ing)] (франц. reportage) — 1) Жанр публіцистики; розповідь кореспондента з місця подій в пресі, по радіо, телебаченню. 2) Вид програми радіомовлення, яка містить розповідь про подію, що відбувається, в момент її здійснення, та відображення події звуковими виразними засобами. Головна мета р. полягає в досягненні “ефекту присутності”, що викликає у слухача почуття співпереживання та здійснює емоційний вплив особливої сили. Р. триває в середньому біля 5 хвилин. Він використовує три основні виразні засоби: слово, що звучить, шуми й музику. Перші два — слово і шуми — він використовує обов’язково. Вдале використання шумів робить передачу яскравішою. Вони допомагають більш точно передати атмосферу події, на зоровому рівні уявити все те, про що розказується.

РЕСПОНДЕНТ /респондент/ [respondent] — особа, що відповідає на питання анкети або дає інтерв’ю.

РЕСУРСИ /ресурсы/ [resources] (франц. ressources, від лат. resurgo — підіймаюся, виникаю знову) — 1) Матеріальні засоби, цінності, запаси, кошти, що в разі потреби можна використати. 2) Будь-які з компонентів (засобів) системи обчислювальної та можливості, які можуть бути надані нею для процесу оброблення

даних на певний проміжок часу.

Р. загальнодоступні /р. общедоступные/ [public r.] — ресурси, доступ до яких не обмежений.

Р. захищені (блоковані) /р. защищенные (блокированные)/ [locked r.] — ресурси ЕОМ, для яких визначений замок секретності (див. замок), тобто специфіковане керування доступом.

Р. інформаційні /р. информационные/ [information r.] — 1) Результат об'єктивного цілеспрямованого відображення закономірностей і фактів реалізації будь-яких процесів, що відбуваються у суспільстві та в навколишньому середовищі (природі). Вони являють собою сукупність наукових знань, зафіксованих на паперових чи інших носіях (мікрофішах, магнітних стрічках, відеодисках і т.ін.)., що зберігаються у довідково-інформаційних фондах інформаційних органів та бібліотек. 2) Окремі документи і окремі масиви документів, документи і масиви документів в системах інформаційних (бібліотеках, архівах, фондах, банках, банках даних і т. ін.), що містять інформацію з усіх напрямків життєдіяльності суспільства. Р. і. можна класифікувати: за видом інформації; за режимом доступу; за видом носія; за способом формування і розповсюдження; за способом організації зберігання і використання; за формою власності. 3) Сукупність даних, що являє собою цінність для установи (підприємства) і виступає як матеріальні ресурси. До р. і. відносяться основні та допоміжні масиви, що зберігаються у зовнішній пам'яті комп'ютерних систем, та вхідні документи.

Р. інформаційні за видом інформації /р. информационные по виду информации/ — ресурси інформаційні, що можуть містити інформацію наступних видів: правову інформацію; науково-технічну інформацію; політичну інформацію; економічну (фінансово-економічну) інформацію; статистичну інформацію; інформацію про стандарти і регламенти, метрологічну інформацію; соціальну інформацію; інформацію про охорону здоров'я; інформацію про надзвичайні ситуації; особисту інформацію (персональні дані); кадастри (земельний, містобудівний, лісовий, майновий і т. ін.); інформацію іншого виду.

Р. інформаційні за видом носія /р. информационные по виду носителя/ — ресурси інформаційні, інформація в яких може бути записана на папері, на машиночитаних носіях, у вигляді зображення на екрані

ЕОМ, в пам'яті ЕОМ, в каналах зв'язку, на інших видах носіїв.

Р. інформаційні за режимом доступу /р. информационные по виду доступа/ — ресурси інформаційні, що містять інформацію відкриту (без обмежень) або інформацію обмеженого доступу (державну таємницю, конфіденційну інформацію, комерційну таємницю, професійну таємницю, службову таємницю, особисту (персональну) таємницю).

Р. інформаційні за способом організації зберігання і використання /р. информационные по способу организации хранения и использования/ — ресурси інформаційні, для зберігання і використання інформації в яких можуть використовуватися традиційні форми (масиви документів, фонди документів, архіви) або автоматизовані форми (банки даних, системи інформаційні автоматизовані, бази знань).

Р. інформаційні за способом формування і розповсюдження /р. информационные по способу формирования и распространения/ — ресурси інформаційні, що знаходяться у стаціонарному або рухомому (мобільному) стані.

Р. інформаційні за формою власності /р. информационные по форме собственности/ — ресурси інформаційні, що можуть складати: загальнодержавне національне надбання; державну власність; муніципальну власність; приватну власність; колективну власність.

Р. обчислювальні /р. вычислительные/ [computational r.] — сукупність апаратних, програмних і інформаційних засобів даного закладу, підприємства, обчислювального центру або окремого користувача.

РЕТРАНСЛЯТОР /ретранслятор/[retransmitter, repeater] (від лат. re... (префікс, що означає зворотну, повторну дію) і транслятор)— проміжна радіо, радіорелейна або телевізійна станція в мережі передавальних і приймальних станцій.

Р. супутниковий /р. спутниковый/ [satellite t.] — ретранслятор, встановлений на космічному літальному апараті (штучному супутнику Землі). Використовується для обміну інформацією між абонентами, віддаленими один від одного на тисячі кілометрів. Р. с. є елементом супутникових ліній зв'язку (див. зв'язок супутниковий) і забезпечує зв'язок у випадку, коли супутники знаходяться у зоні видимості обох земних

станцій. Для ретрансляції радіосигналів застосовуються супутники на геостаціонарній (стаціонарній) і еліптичній орбітах, а також низькоорбітальні космічні апарати.

РЕТРАНСЛЯЦІЯ /ретрансляция/[relaying, retransmission] (від лат. re...(префікс, що означає зворотну, повторну дію) і translatio — перенесення) — приймання сигналів на проміжному пункті (ретранслятори), їхнє підсилення і передавання на інший проміжний або кінцевий пункт. Використовується для збільшення дальності зв'язку. Розрізняють р. з підсиленням і передаванням сигналів у тому ж вигляді, в якому вони були прийняті, та регенеративну р. — з перетворенням сигналів і виправленням помилок, що виникають при передаванні. Р. може здійснюватися із затримкою (сигнал запам'ятовується в спеціальному пристрої і передається в передбачений час).

Р. кадрів /р. кадров/[frame relay] — служба телекомунікацій, створена для з'єднання локальних мереж. Їх називають кінцевими точками в мережі ретрансляції кадрів. Служба ретрансляції кадрів упаковує дані в кадри змінної довжини (фрейми) і пересилає їх на зв'язану кінцеву точку. Усе виправлення помилок здійснюється в кінцевій точці, що збільшує швидкість передавання даних.

РЕЧОВИНА /вещество/ [substance, matter] — будь-що, що складається з часток одного або декількох хімічних елементів і знаходиться у твердому, рідкому або в газоподібному стані, має масу і об'єм. Р. поділяються на прості і складні (хімічні з'єднання).

Р. демаскуюча /в. демаскирующее/ — речовина, що містить ознаки демаскуючі іншої речовини або технології її виготовлення. В результаті фізико-хімічного аналізу р. д. добувається інформація про склад, структуру, властивості і технологію виготовлення продукції, інформація про яку складає державну або комерційну таємницю.

Р. проста /в. простое/ [elementary s.] — речовина, що складається з атомів одного хімічного елемента. За властивостями хімічні елементи (прості речовини) умовно поділяються на метали і неметали. Метали — прості речовини, що мають у звичайних умовах кристалічну структуру (окрім ртуті), хорошу теплопровідність і електропровідність. В свою чергу метали за щільністю поділяють на легкі (із щільністю до 5 г/^{3})

і важкі, за температурою плавлення — легкоплавкі (з температурою плавлення до 1000°С) і тугоплавкі, за хімічною стійкістю до кислот — благородні (срібло, золото) і неблагородні. Р. п., що не мають ознак металів, відносяться до неметалів.

Р. складна /в. сложное/ [compound m.] — речовина, що складаються з хімічних з'єднань атомів різних хімічних елементів. Більшість с. р., до складу яких входить елемент вуглець, відносять до органічних речовин. Проте найпростіші з'єднання вуглецю (оксиди — з'єднання з вуглецю і кисню, вугільна кислота та її солі, деякі інші), а також речовини, що не містять вуглецю, відносять до неорганічних речовин.

РИГЕЛЬ /засов/ [girth rail] (нім. Riegel, букв. засув, запор) — частина замка, що безпосередньо закриває двері, ящик, кришку і т.ін. Р. складається з головки, на яку діє ключ, і з однієї або декількох засувок. Для більш надійного закривання дверей р. сучасних замків роблять з міцної сталі і рухають при закриванні (відкриванні) у вертикальній і горизонтальній площинах. Роль засува в навісних замках виконує його дужка.

РИЗИК /риск/ [risk] — функція ймовірності реалізації певної загрози, виду и величини завданих збитків. Величина р. може бути виражена у грошовому вимірі або у вигляді формальної оцінки (високий, низький і т. ін.).

Р. залишковий /р. остаточный/ [residual r.] — ризик, що залишається після впровадження заходів забезпечення безпеки.

РИНОК /рынок/ [market] — сфера товарного обміну; пропозиція і платоспроможний попит на товари у масштабі світового господарства, країни або окремих її районів.

Р. інформаційний /р. информационный/ — ринок, за допомогою якого реалізується продукція інформаційна та інші послуги інформаційні. Виділяють три сегменти ринку інформаційних послуг: для населення, бізнесу і держави.

Р. інформаційних послуг /р. информационных услуг/ — див. ринок інформаційний.

Р. інформаційних послуг для бізнесу /р. информационных услуг для бизнеса/ — ринок інфор-

маційний для реалізації наступних послуг: електронний обмін даними і електронними посланнями, відео- і комп'ютерні конференцій, корпоративне навчання, мультимедійні бази даних, презентації і настільні видавничі системи, групові методи роботи, електронна торгівля і т. ін.

Р. інформаційних послуг для населення /р. информационных услуг для населения/ — ринок інформаційний для реалізації в основному розважальних і фінансових послуг: платне телебачення, відео-за-вимогою, інтерактивне телебачення, музика-за-вимогою, відеоігри, електронні покупки, банківські операції й керування персональними фінансами, керування домашніми побутовими приладами, охорона й спостереження.

РІВЕНЬ /уровень/ [level, layer] — 1) Ступінь величини, розвитку, значимості будь-чого. 2) Шар логічної структури обчислювальної мережі, який описує певний комплекс завдань, що виконуються цією мережею.

Р. безпеки в "Європейських критеріях" /у. безопасности в "Европейских критериях"/ — рівні для визначення ступеню безпеки системи. В "Европейских критеріях" визначені три рівні безпеки — базовий, середній і високий. Безпека вважається базовою, якщо засоби захисту здатні протистояти окремим випадковим атакам. Безпека вважається середньою, якщо засоби захисту здатні протистояти зловмисникам, що мають обмежені ресурси й можливості. Безпеку можна вважати високою, якщо є упевненість, що засоби захисту можуть бути подолані тільки зловмисниками з високою кваліфікацією, набір можливостей і ресурсів яких виходить за межі розумного.

Р. безпеки інформації /у. безопасности информации/ [security clearance information] — оцінка ступеня безпеки інформації. Найчастіше визначається співвідношенням між вартістю інформації і витратами на її захист. Р. з. і. раціональний у випадку, коли забезпечується необхідна безпека інформації і мінімізуються витрати на інформацію, що складаються з витрат на захист інформації та збитків за рахунок попадання інформації до зловмисника і використання її на шкоду власника.

Р. важливості інформації /у. важности информации/ — категорія розподілу інформації за її важливістю. Розрізняють наступний розподіл інформації за рівнем важливості: життєво важлива незамінна

інформація, наявність якої необхідна для функціонування організації; важлива інформація — інформація, яку можна замінити або відновити, але процес відновлення дуже важкий і зв'язаний з великими затратами; корисна інформація — інформація, яку важко відновити, але організація може ефективно функціонувати і без неї; несуттєва інформація — інформація, яка більше не потрібна організації.

Р. гарантій /у. гарантий/ [access l.] — 1) Міра впевненості в тому, що система комп'ютерна коректно реалізує політику безпеки. 2) У "критеріях Загальних" — сім стандартизованих наборів вимог гарантій безпеки, що регламентують застосування різноманітних методів і технологій розробки, тестування, контролю й верифікації продукту інформаційних технологій (функціональне тестування; структурне тестування; методичне тестування й перевірка; методична розробка, тестування й аналіз; напівформальні методи розробки й тестування; напівформальні методи верифікації розробки й тестування; формальні методи верифікації розробки й тестування), кожний з яких визначає ступінь відповідності IT-продукту кожній вимозі гарантій (гарантії зростають від першого рівня до сьомого). Назви рівнів відображають можливості засобів контролю й верифікації, що застосовуються в ході розробки й аналізу IT-продукту.

Р. гарантій в "Європейських критеріях" /уровни гарантий в "Европейских критериях"/ — сім рівнів гарантій від E0 до E6 (в порядку зростання). Рівень E0 означає мінімальні гарантії (аналог рівня D "Жовтогарячої книги"). При перевірці гарантій аналізується весь життєвий цикл системи — від початкової фази проектування до експлуатації й супроводження. Рівні гарантій від E1 до E6 вишикувані з наростанням вимог ретельності контролю. Так, на рівні E1 аналізується тільки загальна архітектура системи, а гарантії засобів захисту підтверджують функціональним тестуванням. На рівні E3 до аналізу залучаються вихідні тексти програм і схеми апаратного забезпечення. На рівні E6 потрібний формальний опис функцій безпеки, загальної архітектури, а також політики безпеки.

Р. допуску /у. допуска/ [clearance] — ієрархічна частина категорії доступу користувача або процесу, що визначає максимальний рівень доступу пасивного об'єкта, до якого може одержати доступ користувач

або процес.

Р. доступу /у. доступа/ [access l.] — ієрархічна частина категорії доступу пасивного об'єкта.

Р. захисту інформації /у. защиты информации/ — те ж, що рівень безпеки інформації.

Р. захисту мовної інформації /у. защиты речевой информации/ — поняття, що використовується для визначення можливостей різноманітних методів закриття мови. Основні рівні захисту визначаються як тактичний та стратегічний, що в деякій мірі перекликається з поняттями практичної та теоретичної стійкості криптографічних систем закриття даних. Засоби з тактичним, або низьким, рівнем використовується для захисту інформації від підслухування сторонніми особами на період часу, що вимірюється хвилинами або днями. Існує велика кількість простих методів, здатних забезпечити такий рівень захисту при прийнятній вартості (див. скремблери аналогові). Засоби зі стратегічним, або високим, рівнем захисту інформації від перехоплення використовується у випадках, коли високо кваліфікованому, технічно добре озброєному фахівцеві потрібно буде для дешифрування перехопленого повідомлення період часу від декількох місяців до багатьох років (див. шифрування мовної інформації цифрове). Часто використовується і поняття середнього ступеня захисту, що займає проміжне положення між тактичним та стратегічним рівнем закриття.

Р. канальний /у. канальный/ [link l.] — другий рівень архітектури мережі обчислювальної, що забезпечує передавання даних каналами інформаційними.

Р. мережний /у. сетевой/ [network l.] — третій рівень програмної структури мережі обчислювальної, що здійснює керування маршрутизацією інформації.

Р. методичного тестування й перевірки /у. тестирования и проверки/ [EAL3 — methodically tested and checked] — третій рівень гарантій, призначений для використання при обставинах, коли розробникам або користувачам потрібна помірна ступінь незалежного підтвердження властивостей продукту інформаційних технологій, а також повне й послідовне дослідження властивостей продукту й контроль в процесі створення без проведення дорогого зворотного проектування [reengineering]. Відповідає наступним вимогам гарантій безпеки. У класі ВГБ: керування проектом: в розділі ВГБ: керування версіями — контроль цілісно-

сті версій; в розділі ВГБ: конфігурація проекту — основні компоненти проекту (алгоритми, вихідні тексти, тексти, документація). У класі ВГБ: дистрибуція: в розділі ВГБ: поставка — регламентована процедура поставки; в розділі ВГБ: установка, настройка, запуск — регламентовані процедури установки, настройки, запуску. У класі ВГБ: розробки: в розділі ВГБ: загальні функціональні специфікації — неформальні специфікації засобів захисту; в розділі ВГБ: архітектура захисту — відповідність архітектури захисту політиці безпеки; в розділі ВГБ: відповідність описів різного рівня — неформальне підтвердження відповідності. У класі ВГБ: документація: в розділі ВГБ: керівництво адміністратора — адміністрування засобів захисту; в розділі ВГБ: керівництво користувача — використання засобів захисту. У класі ВГБ: процес розробки в розділі ВГБ: безпека середовища розробки — застосування заходів безпеки в ході розробки. У класі ВГБ: тестування: в розділі ВГБ: повнота тестування — аналіз повноти тестування; в розділі ВГБ: глибина тестування — архітектура; в розділі ВГБ: методика тестування — функціональне тестування й протоколювання результатів тестів; в розділі ВГБ: незалежне тестування — вибіркове незалежне тестування. У класу ВГБ: оцінка захисту: в розділі ВГБ: аналіз можливостей неправильного використання засобів захисту — аналіз керівництв з адміністрування; в розділі ВГБ: аналіз стійкості засобів захисту — оцінка стійкості засобів захисту; в розділі ВГБ: аналіз продукту на наявність уразливостей — виявлення уразливостей розробником продукту.

Р. методичної розробки, тестування й аналізу /у. методической разработки, тестирования и анализа/ [EAL4 — methodically designed, tested and reviewed] — четвертий рівень гарантій, призначений для використання при обставинах, коли розробники або користувачі вимагають помірного або високого ступеню незалежного підтвердження гарантій захисту продукту інформаційних технологій и готові нести певні додаткові витрати. Відповідає наступним вимогам гарантій безпеки. У класі ВГБ: керування проектом: в розділі ВГБ: засоби керування проектом — застосування автоматизованих засобів керування проектом; в розділі ВГБ: керування версіями — авторизація розробників при поновленні версій; в розділі ВГБ: конфігурація проекту — включення до складу конфігурації проекту виявлених помилок і уразливостей. У класі

ВГБ: дистрибуція: в розділі поставка — виявлення спотворень в процесі поставки; в розділі ВГБ: установка, настройка, запуск — регламентовані процедури установки, настройки, запуску. У класі ВГБ: розробка: в розділі ВГБ: загальні функціональні специфікації — неформальні специфікації для усіх інтерфейсів засобів захисту; в розділі ВГБ: архітектура захисту — відповідність архітектури захисту політиці безпеки; в розділі ВГБ: форма надання продукту на сертифікацію — опис реалізації обмеженої підмножини засобів захисту; в розділі ВГБ: часткові специфікації засобів захисту — неформальні часткові специфікації засобів захисту; в розділі ВГБ: відповідність описів різного рівня — неформальне підтвердження відповідності; в розділі ВГБ: політика безпеки — неформальний опис політики безпеки. У класі ВГБ: документація: в розділі ВГБ: керівництво адміністратора — адміністрування засобів захисту; в розділі ВГБ: керівництво користувача — використання засобів захисту. У класі ВГБ: процес розробки: в розділі ВГБ: безпека середовища розробки — застосування заходів безпеки в ході розробки; в розділі ВГБ: технологія розробки — визначена розробником технологія розробки; в розділі ВГБ: засоби розробки — використання певного набору засобів розробки. У класі ВГБ: тестування: в розділі ВГБ: повнота тестування — обґрунтування повноти тестування; в розділі ВГБ: глибина тестування — архітектура; в розділі ВГБ: методика тестування — функціональне тестування й протоколювання результатів тестів; в розділі ВГБ: незалежне тестування — вибіркове незалежне тестування. У класі ВГБ: оцінка захисту: в розділі ВГБ: аналіз можливостей неправильного використання засобів захисту — підтвердження повноти керівництв з адміністрування й безпеки їхнього застосування; в розділі ВГБ: аналіз стійкості засобів захисту — оцінка стійкості засобів захисту; в розділі ВГБ: аналіз продукту на наявність уразливостей — незалежний аналіз уразливостей.

Р. напівформальних методів верифікації розробки й тестування /у. полуформальных методов верификации разработки и тестирования/ [EAL6 — semiformally verified design and tested] — шостий рівень гарантій, призначений для використання в ситуаціях з високим ступенем ризику, де цінність інформації, що захищається, виправдовує високі додаткові витрати. Відповідає наступним вимогам гарантій безпеки. У класі ВГБ: керування проектом: в розділі ВГБ: засоби керування проектом – повна автоматизація керува-

ння проектом і контролю версій; в розділі ВГБ: керування версіями — контроль цілісності й автентичності дистрибутива системи; в розділі ВГБ: конфігурація проекту — включення до складу конфігурації проекту інструментальних засобів розробки. У класі ВГБ: дистрибуція: в розділі ВГБ: поставка — виявлення спотворень в процесі поставки; в розділі ВГБ: установка, настройка, запуск — регламентовані процедури установки, настройки, запуску. У класі ВГБ: розробка: в розділі ВГБ: загальні функціональні специфікації — напівформальні специфікації для засобів захисту; в розділі ВГБ: архітектура захисту — відповідність напівформального опису архітектури захисту політиці безпеки; в розділі ВГБ: форма надання продукту на сертифікацію — структурований опис реалізації усіх засобів захисту; в розділі структура засобів захисту — ієрархічність; в розділі ВГБ: часткові специфікації засобів захисту — напівформальні часткові специфікації засобів захисту; в розділі ВГБ: відповідність описів різного рівня — напівформальний доказ відповідності; в розділі ВГБ: політика безпеки — формальна модель політики безпеки. У класі ВГБ: документація: в розділі ВГБ: керівництво адміністратора — адміністрування засобів захисту; в розділі ВГБ: керівництво користувача — використання засобів захисту. У класі ВГБ: процес розробки: в розділі ВГБ: безпека середовища розробки — підтвердження заходів безпеки в ході розробки; в розділі ВГБ: технологія розробки — стандартизована технологія розробки; в розділі ВГБ: засоби розробки — використання тільки засобів розробки, що відповідають певним стандартам. У класі ВГБ: тестування: в розділі ВГБ: повнота тестування — строгий аналіз повноти тестування; в розділі ВГБ: глибина тестування — функціональні специфікації; в розділі ВГБ: методика тестування — тестування у відповідності з певною методикою; в розділі ВГБ: незалежне тестування — вибіркове незалежне тестування. У класі ВГБ: оцінка захисту: в розділі ВГБ: аналіз схованих каналів — пошук схованих каналів на основі певних методів; в розділі ВГБ: аналіз можливостей неправильного використання засобів захисту — незалежний аналіз можливостей неправильного використання засобів захисту; в розділі ВГБ: аналіз стійкості засобів захисту — оцінка стійкості засобів захисту; в розділі ВГБ: аналіз продукту на наявність уразливостей — вичерпний аналіз уразливостей.

Р. напівформальних методів розробки й тестування /у. полуформальных методов разработки

и тестирования/ [EAL5 — semiformally verified design and tested] — п'ятий рівень гарантій, призначений для використання в тих випадках, коли розробники або користувачі вимагають високого ступеню незалежного підтвердження гарантій засобів захисту, а також строгого застосування певних технологій розробки продукту інформаційних технологій, але без надмірних витрат. Відповідає наступним вимогам гарантій безпеки. У класі ВГБ: керування проектом: в розділі ВГБ: засоби керування проектом — застосування автоматизованих засобів керування проектом; в розділі ВГБ: керування версіями — авторизація розробників при поновленні версій; в розділі ВГБ: конфігурація проекту — включення до складу конфігурації проекту інструментальних засобів розробки. У класі ВГБ: дистрибуція: в розділі ВГБ: поставка — виявлення спотворень в процесі поставки; в розділі ВГБ: установка, настройка, запуск — регламентовані процедури установки, настройки, запуску. У класі ВГБ: розробка: в розділі ВГБ: загальні функціональні специфікації — напівформальні специфікації для засобів захисту; в розділі ВГБ: архітектура захисту — напівформальний опис архітектури захисту; в розділі ВГБ: форма надання продукту на сертифікацію — повний опис реалізації усіх засобів захисту; в розділі ВГБ: структура засобів захисту — модульність; в розділі ВГБ: часткові специфікації засобів захисту — неформальні часткові специфікації засобів захисту; в розділі ВГБ: відповідність описів різного рівня — напівформальне підтвердження відповідності; в розділі ВГБ: політика безпеки — формальна модель політики безпеки. У класі ВГБ: документація: в розділі ВГБ: керівництво адміністратора — адміністрування засобів захисту; в розділі ВГБ: керівництво користувача — використання засобів захисту. У класі ВГБ: процес розробки: в розділі ВГБ: безпека середовища розробки — застосування заходів безпеки в ході розробки; в розділі ВГБ технологія розробки — стандартизована технологія розробки; в розділі ВГБ: засоби розробки — використання основних засобів розробки, що відповідають певним стандартам. У класі ВГБ: тестування: в розділі ВГБ: повнота тестування — обґрунтування повноти тестування; в розділі ВГБ: глибина тестування — функціональні специфікації; в розділі ВГБ: методика тестування — функціональне тестування й протоколювання результатів тестів; в розділі ВГБ: незалежне тестування — вибіркове незалежне тестування. У класі ВГБ: оцінка захисту: в розділі ВГБ: аналіз схованих

каналів — пошук і документування схованих каналів; в розділі ВГБ: аналіз можливостей неправильного використання засобів захисту — підтвердження повноти керівництв з адміністрування й безпеки їхнього застосування; в розділі ВГБ: аналіз стійкості засобів захисту — оцінка стійкості засобів захисту; в розділі ВГБ: аналіз продукту на наявність уразливостей — систематичний аналіз уразливостей на основі заданих методик.

Р. повноважень найвищий /у. полномочий наивысший/ [system high] — режим захисту даних, при якому користувачі системи забезпечуються допуском, що дозволяє одержати доступ до всієї інформації в системі, не зважаючи на те, що різні частини бази даних можуть мати різні категорії захисту.

Р. повноважень суб'єкта доступу /у. полномочий субъекта доступа/ [subject privilege] — сукупність прав доступу суб'єкта доступу.

Р. послуги /у. услуги/ [l. of service] — міра ефективності і (або) стійкості механізмів, що реалізують послугу безпеки, відносно введеної для даної послуги шкали оцінки.

Р. представницький /у. представительный/ [presentation l.] — шостий рівень програмної структури мережі обчислювальної, призначений для подання й оброблення форматних і синтаксичних атрибутів даних, що приймаються й передаються.

Р. прикладний /у. прикладной/ [application l.] — сьомий рівень програмної структури мережі обчислювальної, в якому виконуються прикладні процеси.

Р. сеансовий /у. сеансовый/ [session l.] — п'ятий рівень програмної структури мережі обчислювальної, що забезпечує сеанси взаємодії між прикладними процесами.

Р. секретності /у. секретности/ — адміністративна або законодавча міра, що відповідає мірі відповідальності особи за витік або втрату конкретної секретної інформації, регламентованої спеціальним документом, з врахуванням державних, воєнно-стратегічних, комерційних, службових або особистих інтересів.

Р. структурного тестування /у. структурного тестирования/ [EAL2 — structurally tested] — другий рівень гарантій, призначений для використання при обставинах, коли розробники або користувачі згодні

задовольнитися низьким або помірним ступенем незалежного підтвердження гарантій рівня безпеки, який необхідно забезпечити. Особливо рекомендують застосування даного рівня для успадкованих систем, які вже знаходяться в експлуатації. Другий рівень гарантій відповідає наступним вимогам гарантій безпеки. У класі ВГБ: керування проектом в розділі ВГБ: керування версіями — ідентифікація компонентів. У класі ВГБ: дистрибуція: в розділі ВГБ: поставка — регламентована процедура поставки; в розділі ВГБ: установка, настройка, запуск — регламентовані процедури установки, настройки, запуску. У класі ВГБ: розробка: в розділі ВГБ: загальні функціональні специфікації — неформальні специфікації засобів захисту; в розділі ВГБ: архітектура захисту — опис архітектури захисту; в розділі ВГБ: відповідність описів різного рівня — неформальне підтвердження відповідності. У класі ВГБ: документація: в розділі ВГБ: керівництво адміністратора — адміністрування засобів захисту; в розділі ВГБ: керівництво користувача — використання засобів захисту. У класі ВГБ: тестування: в розділі ВГБ: повнота тестування — обґрунтування повноти тестування; в розділі ВГБ: методика тестування — функціональне тестування й протоколювання результатів тестів; в розділі ВГБ: незалежне тестування — вибіркове незалежне тестування. У класу ВГБ: оцінка захисту: в розділі ВГБ: аналіз стійкості засобів захисту — оцінка стійкості засобів захисту; в розділі ВГБ: аналіз продукту на наявність уразливостей — виявлення уразливостей розробником продукту.

Р. технічного захисту інформації /у. технической защиты информации/ [technical protection information l.] — сукупність вимог, у тому числі й нормованих, що визначається режимом доступу до інформації та загрозами для інформації.

Р. транспортний /у. транспортный/ [transport l.] — четвертий рівень програмної структури мережі обчислювальної, який забезпечує передачу масивів інформації від одного порту до іншого.

Р. фізичний /у. физический/ [physical l.] — перший рівень програмної структури мережі обчислювальної, що описує сполучення системи з фізичним середовищем.

Р. формальних методів верифікації розробки й тестування /у. применения методов верификации разработки и тестирования/ [EAL7 — formally verified design and tested] — сьомий рівень гарантій,

призначений для використання в ситуаціях з виключно високим ступенем ризику, і (або) там, де цінність об'єктів, що захищаються, виправдовує високі додаткові витрати. Практичне застосування цього рівня на даний час обмежене компактними продуктами інформаційних технологій, в яких сконцентровані засоби захисту, і які легко піддаються формальному аналізові. Сьомий рівень гарантій відповідає наступним вимогам гарантій безпеки. У класі ВГБ: керування проектом: в розділі ВГБ: засоби керування проектом – повна автоматизація керування проектом і контролю версій; в розділі ВГБ: керування версіями — контроль цілісності й автентичності дистрибутива системи; в розділі ВГБ: конфігурація проекту — включення до складу конфігурації проекту інструментальних засобів розробки. У класі ВГБ: дистрибуція: в розділі ВГБ: поставка — захист від спотворень в процесі поставки; в розділі ВГБ: установка, настройка, запуск — регламентовані процедури установки, настройки, запуску. У класі ВГБ: розробка: в розділі ВГБ: загальні функціональні специфікації — формальні специфікації для засобів захисту; в розділі ВГБ: архітектура захисту — формальний опис архітектури захисту й доказ її відповідності політиці безпеки; в розділі ВГБ: форма надання продукту на сертифікацію — структурований опис реалізації усіх засобів захисту; в розділі ВГБ: структура засобів захисту — мінімізація складності; в розділі ВГБ: часткові специфікації засобів захисту — напівформальні часткові специфікації засобів захисту; в розділі ВГБ: відповідність описів різного рівня — формальний доказ відповідності; в розділі ВГБ: політика безпеки — формальна модель політики безпеки. У класі ВГБ: документація: в розділі ВГБ: керівництво адміністратора — адміністрування засобів захисту; в розділі ВГБ: керівництво користувача — використання засобів захисту. У класі ВГБ: процес розробки: в розділі ВГБ: безпека середовища розробки — підтвердження заходів безпеки в ході розробки; в розділі ВГБ: технологія розробки — технологія розробки, що дозволяє оцінювати розроблюваний продукт; в розділі ВГБ: засоби розробки — використання тільки засобів розробки, що відповідають певним стандартам. У класі ВГБ: тестування: в розділі повнота тестування — строгий аналіз повноти тестування; в розділі ВГБ: глибина тестування — реалізація; в розділі ВГБ: методика тестування — тестування у відповідності з певною методикою; в розділі ВГБ: незалежне тестування — повне незалежне тестування. У класі ВГБ:

оцінка захисту: в розділі ВГБ: аналіз схованих каналів — пошук схованих каналів на основі певних методів; в розділі ВГБ: аналіз можливостей неправильного використання засобів захисту — незалежний аналіз можливостей неправильного використання засобів захисту; в розділі ВГБ: аналіз стійкості засобів захисту — оцінка стійкості засобів захисту; в розділі ВГБ: аналіз продукту на наявність уразливостей — вичерпний аналіз уразливостей.

Р. функціонального тестування /у. функционального тестирования/ [EAL1 — functionally tested] — перший рівень гарантій для випадків, коли загрозам безпеці не надається великого значення. Пропонується використати його в тих ситуаціях, коли все що необхідно — це незалежна гарантія того, що до складу продукту інформаційних технологій входять засоби захисту персональної або подібної інформації. Відповідає наступним вимогам гарантій безпеки. У класі ВГБ: керування проектом в розділі ВГБ: керування версіями — нумерація версій. У класі ВГБ: дистрибуція в розділі ВГБ: установка, настройка, запуск — регламентовані процедури установки, настройки, запуску. У класі ВГБ: розробка: в розділі ВГБ: загальні функціональні специфікації — неформальні специфікації для засобів захисту; в розділі ВГБ: відповідність описів різного рівня — неформальне підтвердження відповідності. У класі ВГБ: документація: в розділі ВГБ: керівництво адміністратора — адміністрування засобів захисту; в розділі ВГБ: керівництво користувача — використання засобів захисту. У класі ВГБ: тестування в розділі ВГБ: незалежне тестування — готовність продукту до незалежного тестування.

РІШЕННЯ /решение/ [decision, solution] — висновок про необхідність будь-яких дій, прийнятий після деякого обдумування.

Р. інформаційне /р. информационное/ — одиничний акт сприйняття органом керування поточної інформації про обстановку і її віднесення до будь-якої відомості кадастру інформаційного. Процес прийняття р. і. передує усім іншим етапам процесу мислення людини або етапам оброблення інформації в сучасних інформаційних системах. При моделюванні р. і. орган керування описується у вигляді системи інформаційної із самонавчанням, що сприймає поточну інформацію про обстановку. Процедура прийняття р. і. полягає в

послідовній селекції і класифікації поточної інформації. Селекція і класифікація здійснюється з використанням тезауруса апріорної інформації, основу якого складає інформаційний кадастр. Одержана в результаті прийняття р. і. інформація доповнює тезаурус і змінює ступінь інформованості органу управління про обстановку.

РОБОТА /работа/ [work, operation, processing] — 1) Процес, дія, функціонування. 2) Заняття, праця, діяльність.

Р. інформаційна /р. информационная/ — 1) Сукупність процесів збирання, нагромадження, аналізу, перетворення, зберігання, пошуку і розповсюдження інформації (а також інших допоміжних процесів, що забезпечують ці основні процеси), які систематично здійснюються будь-якою організацією (установою, підрозділом, групою осіб і т. ін.). 2) В розвідці — сукупність процесів збирання даних і відомостей від органів добування інформації та перетворення їх в закінчену продукцію розвідувальної діяльності (документ інформаційний), призначену для подання споживачеві інформації.

РОЗВІДКА /разведка/ [intelligence, reconnaissance, scouting, surveillance, intelligence/secret service] — 1) Сукупність процесів добування, оброблення та доведення споживачам інформації, необхідної для прийняття рішень. В залежності від статусу споживача інформації розвідку можна розділити на розвідку державну (споживачем інформації є державні структури) і розвідку комерційну (споживачем інформації є комерційні структури), а в залежності від переважання людського або технічного фактора у процесах р. — на агентурну і технічну. 2) У військовій справі — сукупність заходів, що проводяться з метою збирання даних про наявного або ймовірного противника, необхідних для оцінки обстановки і прийняття рішення. 3) Орган розвідки.

Р. агентурна /р. агентурная/ [HUMan I. (HUMINT)] — добування інформації шляхом проникнення агента-розвідника до джерела інформації на відстань доступності його органів чуття або технічних засобів, що використовуються агентом, з метою копіювання інформації і передавання її споживачеві інформації.

Р. акустична /р. акустическая/ [ACOUStic I. (ACOUSINT)] — вид розвідки технічної, призначений

для одержання інформації з носіїв у вигляді хвиль акустичних. В залежності від середовища розповсюдження хвиль р. а. поділяється на власне акустичну (повітряно-акустичну), гідроакустичну (середовище розповсюдження — вода) і сейсмічну (середовище розповсюдження — земна поверхня).

Р. в Інтернеті /р. в Интернете/ — сукупність заходів, спрямованих на використання можливостей і ресурсів Інтернету для виконання завдань розвідувальних. При належному використанні Інтернету можна одержати економний інструмент, який допоможе аналітикам швидко готувати розвідувальні зведення за темами, які раптово стали актуальними. Інтернет є одним з важливих складових нового застосування розвідки по відкритих джерелах, а також може надати велику допомогу у підготовці персоналу розвідувальних служб та відпрацюванні методик виконання задач розвідки.

Р. видова /р. видовая/ [IMagery i. (IMINT)] — розвідка повітряна і космічна з використанням оптико-електронних засобів. У р. в. використовуються найновіші досягнення в галузі електроніки, оптики, техніки обчислювальної, зв'язку, дистанційного зондування і технологій інформаційних. Об'єднання р. в. і картографування дає можливість одержання точної видової і геокосмічної інформації.

Р. внутрішня /р. внутренняя/ [internal i.] — вид розвідки, яка ведеться з метою виявлення і нейтралізації діяльності всередині країни, яка створює, за думкою властей, загрозу безпеці держави. В авторитарних країнах р. в. це продовження контррозвідувальної роботи спеціальних служб. При демократії в. р. ведення з метою виявлення фактів порушення громадянських прав.

Р. воєнна /р. военная/ [military i.] — добування, збирання та вивчення даних про воєнно-політичну обстановку в окремих країнах та коаліціях держав ймовірного або діючого противника, його збройні сили і воєнно-економічний потенціал, склад, положення, характер дій та наміри угруповань військ (сил), а також про театр воєнних дій; вид забезпечення воєнних дій.

Р. гідроакустична /р. гидроакустическая/ [hydroacoustic i., sonar i.] — добування відомостей про противника гідроакустичними засобами шляхом приймання, реєстрації та аналізу акустичних (звукових)

коливань, що випромінюються або відбиваються кораблем, торпедою і т. ін.

Р. державна /р. государственная/ [State i.] — розвідка, яка ведеться з метою забезпечення керівництва країни інформацією, необхідною для прийняття ним політичних, економічних, воєнних, науково-технічних рішень в умовах жорсткої міждержавної конкуренції. Основними сферами інтересів р. д. є: стан воєнно-економічних і науково-технічних потенціалів інших держав, насамперед, потенційних противників, і прогнозування їхнього розвитку; розташування воєнно-технічних об'єктів, їхні виробничі потужності, характер і розподіл продукції, що випускається; зміст і характер робіт, що ведуться в галузі створення нових видів озброєння і військової техніки; склад і дислокація угруповань військ і сил флоту; ефективність озброєння і військової техніки, їхні тактико-технічні характеристики; масштаб навчань, що проводяться, склад сил та засобів, що залучаються до них, зміст завдань, що вирішуються на навчаннях; принципи побудови і технічного оснащення систем державного і воєнного управління; інженерне обладнання континентальних і навігаційно-гідрографічне забезпечення морських і океанських театрів воєнних дій; наявність паливо-енергетичних, рудних, водних, рослинних та інших природних ресурсів; метеорологічні умови на території держав, що розвідуються; виконання умов міжнародних договорів, насамперед, про обмеження озброєнь. Крім того, органи державної розвідки добувають великі об'єми різноманітної інформації, аж до стану здоров'я, характеру, звичок, стилю мислення політичних і військових керівників іноземних держав.

Р. джерел електромагнітних сигналів /р. источников электромагнитных сигналов/ [SIGnal I.(SIGINT)] (ам.) — приймання, моніторинг, аналіз і, наскільки це можливо, порушення всіх способів передавання інформації з використанням випромінювання електромагнітного. Складовими частинами SIGINT є розвідка і перехоплення повідомлень в системах зв'язку (радіорозвідка), розвідка радіотехнічна і розвідка систем телеметрії.

Р. економічна /р. экономическая/ [economic i.] — збирання інформації, що забезпечує переваги над конкурентами, корпораціями, державами, і стосується наступних сторін їхньої господарської діяльності: наявних ресурсів, процесів виробництва та економічних благ (технологій), процесів розподілу і обернення

капіталів, процесів споживання, процесів моделювання виробництва і економічних явищ, науково-дослідних процесів. Часто в рамках р. е. виділяють розвідки промислову і комерційну.

Р. комерційна /р. коммерческая/ [commercial i., business i.] — розвідка, яка ведеться з метою забезпечення відповідних комерційних структур інформацією, необхідною для успішної діяльності на ринку в умовах гострої конкурентної боротьби. Основними сферами інтересів р. к. можуть бути: комерційна філософія і ділова стратегія керівників фірм-конкурентів, їхні особисті та ділові якості; науково-дослідні і конструкторські роботи; фінансові операції фірм; організація виробництва, в тому числі дані про введення нових, розширення і модернізацію існуючих потужностей, об'єднання з іншими фірмами; технологічні процеси виробництва нової продукції, результати її випробувань; маркетинг фірми, в тому числі режими поставок, відомості про замовників і угод з ними, показники реалізації продукції. Крім того, р. к. займається: вивченням і виявлення організацій, що потенційно є або союзниками, або конкурентами; добуванням, збиранням і обробленням інформації про діяльність потенційних і реальних конкурентів; врахуванням і аналізом спроб несанкціонованого одержання комерційних секретів конкурентами; оцінкою реальних відношень між організаціями, що співпрацюють та конкурують; аналізом можливих каналів витоку конфіденційної інформації. Збирання і аналіз даних здійснюється також з великої кількості інших питань, в тому числі вивчаються з метою наступного вербування співробітники фірм-конкурентів, визначаються їхні потреби і фінансовий стан, схильності і дошкульні місця.

Р. комп'ютерна /р. компьютерная/ [computer i.] — вид розвідки радіоелектронної, призначений для добування інформації із комп'ютерів і мереж обчислювальних.

Р. космічна /р. космическая/ [space r.] — комплекс заходів з добування інформації розвідувальної з використанням космічних засобів. Для ведення р. к. використовуються спеціальні космічні системи, які за цільовим призначенням поділяються на системи оглядової і детальної фоторозвідки, розвідки телевізійної і радіотехнічної, комплексної розвідки, раннього виявлення запусків ракет, контролю ядерних вибухів і т.

ін.

Р. лазерна /р. лазерная/ [laser r.] — виявлення, розпізнавання та визначення координат об'єктів (цілей) за допомогою приладів, що працюють за принципом використання енергії лазерного випромінювання; складова частина розвідки оптико-електронної.

Р. магнітометрична /р. магнитометрическая/ [magnetometric i.] — вид розвідки технічної, призначений для виявлення об'єктів, що мають власне поле магнітне, наприклад, підводних човнів в зануреному стані.

Р. методами вимірювань і аналізу сигнатур /р. методами измерений и анализа сигнатур/ [Measurement And Signature I. (MASINT)] (ам.) — розвідувальна система, призначена для добування інформації (окрім інформації про джерела електричних сигналів і традиційної видової інформації), яка після збирання, оброблення і аналізу містить відомості для визначення місцезнаходження виявлених об'єктів (цілей), їхньої ідентифікації і слідкування за ними або опис їхніх сигнатур (комплекс характерних ознак). Датчиками системи служать радіолокаційні, лазерні, оптичні, інфрачервоні, акустичні, ядерні, радіаційні, спектрорадіометричні, сейсмічні системи та пристрої.

Р. наукова /р. научная/ [scientific i.] — спосіб одержання випереджаючих даних про появу у потенційного або реального противника нових видів і типів озброєння.

Р. науково-технічна /р. научно-техническая/ [scientific and technical i.] — напрямок розвідки промислової, в рамках якої формуються дві підсистеми: розвідка в галузі фундаментальних наук і в галузі дослідно-конструкторських робіт. Перша підсистема визначає принципові напрямки вирішення окремих проблем, друга — забезпечує реальні підходи до одержання можливих прибутків через виробництво найновішої техніки. Інтерес представляють фундаментальні і прикладні дослідження іноземних учених, науково-технічні характеристики, можливості і недоліки воєнних технологій, а також оборонний аспект промислових

галузей.

Р. оптико-електронна /р. оптико-электронная/ [optic-electronic i.] — див. розвідка оптична.

Р. оптична /р. оптическая/ [optical i.] — вид розвідки технічної, призначений для одержання інформації про ознаки видові об'єктів, які містять джерела випромінювання електромагнітного у видимому і інфрачервоному діапазоні. Р. о. включає: візуально-оптичну; фотографічну; інфрачервону; телевізійну; лазерну. Останні три види р. о., в яких використовується електронна техніка, утворюють розвідку оптико-електронну.

Р. по відкритих джерелах /р. по открытых источниках/ — розвідувальних відомостей добування з відкритих джерел інформації. Традиційно службами розвідувальними завжди широко використовувались відкриті джерела інформації: від вивчення іноземної преси до опитування туристів і бізнесменів, а також залучення до співробітництва фахівців, вчених, студентів. В період інформаційного буму поняття розвідки на основі відкритих джерел трактується в більш широкому контексті, враховуючи широкий діапазон потенційних цілей розвідки, розмивання меж між відкритими і закритими джерелами інформації, необхідність більш тонкого комплексного аналізу питань, що досліджуються, та зменшення витрат, що виділяються на безпеку національну. Найкраще демонструє перспективи такої розвідки розвідка в Інтернеті.

Р. повітряна /р. воздушная/ [air i.] — добування відомостей про наземні, морські та повітряні об'єкти противника. Проводиться розвідувальною авіацією, всіма екіпажами, що виконують бойові завдання, апаратами літальними безпілотними . Основні способи ведення п. р.: візуальне спостереження, аерофоторозвідка і розвідка за допомогою радіоелектронних засобів (повітряна розвідка радіоелектронна).

Р. політична /р. политическая/ [political i.] — розвідка, що ведеться з метою збирання інформації про внутрішню ситуацію в іноземній державі, яку можна використати з користю для своєї держави. Див. також інформація політична.

Р. промислова /р. промышленная/ [industrial i.] — вид розвідки економічної, що охоплює наукові дослідження, технології, організацію виробничих процесів, розвідку ресурсів. В р. п. визначаються декілька

основних напрямків: розвідка науково-технічна, шпіонаж технологічний і розвідка ресурсів.

Р. радіаційна /р. радиационная/ [nuclear i. (NUCINT)] — вид розвідки технічної, призначений для виявлення, локалізації, визначення характеристик і зміни рівнів випромінювань радіоактивних речовин.

Р. радіоелектронна (РЕР) /р. радиоэлектронная (РЭР/ [ELectronic I. (ELINT)] — вид розвідки технічної, призначений для добування інформації про об'єкти, що містять джерела сигналів функціональних сигналів) з носіями у вигляді випромінювання електромагнітного у діапазоні радіочастот або у вигляді електричного струму В залежності від характеру інформації, що добувається, РЕР поділяється на: радіорозвідку; розвідку радіотехнічну; розвідку радіолокаційну; розвідку радіотеплову; розвідку комп'ютерну.

Р. радіолокаційна /р. радиолокационная/ [RADar i. (RADINT)] — вид розвідки радіоелектронної, призначений для добування інформації про ознаки видові радіолокаційного зображення об'єкта (див. також радіолокація).

Р. радіотеплова /р. радиотепловая/ [thermal i.] — вид розвідки радіоелектронної, призначений для добування інформації про ознаки, зумовлені власними випромінюванням електромагнітним об'єктів у діапазоні радіочастот.

Р. радіотехнічна /р. радиотехническая/ — вид розвідки радіоелектронної, призначений для добування інформації про ознаки (параметри) радіотехнічних сигналів.

Р. спеціальна /р. специальная/ [special i.] — вид розвідки, що проводиться з метою підриву морально-політичного, економічного і воєнного потенціалів імовірного або діючого противника. Основні задачі: добування відомостей про економічні та військові об'єкти; знищення або виведення з ладу цих об'єктів; організація саботажу та диверсійно-терористичних актів; підготовка повстанських загонів і т. ін. Р. с. організується військовими органами і спеціальними службами, ведеться силами розвідки агентурної і військ спеціального призначення.

Р. телевізійна /р. телевизионная/ [television r.] — добування відомостей про противника за допомогою телевізійної розвідувальної апаратури; складова частина розвідки оптико-електронної. Використання

р. т. ефективне разом з іншими видами розвідки, особливо з розвідкою тепловою. В цих випадках телевізійні засоби використовуються для передавання на Землю інформації розвідувальної, що поступає від інфрачервоних засобів, які розміщуються на повітряних і космічних носіях.

Р. теплова (інфрачервона) /р. тепловая (инфракрасная)/ [IR (infrared) r.] — добування відомостей про об'єкти (цілі) противника за їхнім тепловим (інфрачервоним) випромінюванням за допомогою спеціальних приладів — теплолокаторів; складова частина розвідки радіоелектронної. Р. т. дозволяє виявити і визначити місцезнаходження об'єктів (цілей), що мають теплову (інфрачервону) контрастність.

Р. технічна /р. техническая/ [technical intelligence] — добування та оброблення інформації за допомогою технічних засобів розвідки. На відміну від розвідки агентурної, р. т. забезпечує дистанційний контакт з джерелом інформації та одержання інформації з носіїв, що не здійснюють безпосереднього впливу на органи чуття людини. Найбільш широко розповсюджені дві системи класифікації р. т.: за фізичною природою носіїв інформації (оптична, радіоелектронна, акустична, хімічна, радіаційна, магнітометрична) та за видом носіїв технічних засобів розвідки (наземна, повітряна, космічна, морська).

Р. фотограмметрична /р. фотограмметрическая/ [photogrammetry i.] — добування відомостей в результаті оброблення фотографічних (фототелевізійних), радіолокаційних, теплових та інших зображень поверхні землі і об'єктів. Див. також фотограмметрія.

Р. фотографічна /р. фотографическая/ [photographic i., photographic r.] — одержання відомостей про противника шляхом використання апаратів фотографічних. Ведеться із землі, повітря, кораблів та з космосу. За допомогою сучасної апаратури може вестись з малих та великих висот, на великих швидкостях, як вдень, так і вночі.

Р. хімічна /р. химическая/ — вид розвідки технічної, призначений для добування інформації про склад, структуру і властивості речовин шляхом здобування проб і аналізу їхніх мікрочасток.

РОЗВІДНИК /разведчик/ [secret service man, spy, intelligence agent, reconnaissanceman, scout] — особа,

яка займається добуванням, вивченням, узагальненням відомостей про діючого або ймовірного противника.

Р. легальний /р. легальный/ — співробітник розвідки, який їде за кордон як офіційний представник своєї країни, тобто має легальне прикриття співробітника дипломатичної або торгівельної місії.

РОЗГОЛОШЕННЯ /разглашение/ [disclosure] — піддавання розголосові, обнародуванню чого-небудь; поширювання, розповсюдження.

Р. інформації /р. информации/ [information d.] — передача інформації будь-кому, хто не має до неї авторизованого доступу.

Р. привілеїв на доступ /р. привилегий на доступ/ — сукупність заходів, спрямованих на виділення з числа осіб, допущених до інформації, певної групи, якій надається доступ тільки при одночасному пред'явлення повноважень всіх членів групи.

РОЗДІЛ /раздел/ [chapter] — присвячена одній темі частина книжки, твору, документа і т. ін.

Р. ВГБ /р. ТГБ/ [assurance family] — складова частина класу ВГБ. Структура розділу містить наступні елементи: назва й позначення розділу [family name]; мета [objectives]; ранжирування вимог [component levelling]; опис застосування [application notes]; вимоги [assurance component]. Кожний розділ має свою унікальну назву і семисимвольний ідентифікатор, який складається з трибуквеного ідентифікатора класу, знаку підкреслення і трибуквеного позначення розділу. Ранжирування стандартних вимог представлене у вигляді впорядкованих списків.

Р. ВГБ: аналіз можливостей неправильного використання засобів захисту /р. ТГБ: анализ возможностей неправильного использования средств защиты/ [MiSUse (AVA_MSU)] — розділ ВГБ у класі ВГБ: оцінка захисту. Включає наступні вимоги гарантій безпеки: аналіз керівництв з адміністрування [examination of guidance (AVA_MSU.1)]; підтвердження повноти керівництв з адміністрування і безпеки їхнього застосування [validation of analysis (AVA_MSU.2)]; незалежний аналіз можливостей неправильного використання засобів захисту [analysis and testing for insecure states (AVA_MSU.3)].

Р. ВГБ: аналіз прихованих каналів /р. ТГБ: анализ скрытых каналов/ [Covert Channel Analysis

(AVA_CCA)] — розділ ВГБ у класі ВГБ: оцінка захисту. Включає наступні вимоги гарантій безпеки: пошук і документування прихованих каналів [covert channel analysis (AVA_CCA.1)]; пошук прихованих каналів на основі певних методик [systematic covert channel analysis (AVA_CCA.2)]; вичерпний пошук прихованих каналів [exhaustive covert channel analysis (AVA_CCA.3)].

Р. ВГБ: аналіз продукту на наявність уразливостей /р. ТГБ: анализ продукта на наличие уязвимостей/ [VuLnerability Analysis (AVA_VLA)] — розділ ВГБ у класі ВГБ: оцінка захисту. Включає наступні вимоги гарантій безпеки: виявлення уразливостей розробником продукту [developer vulnerability analysis (AVA_VLA.1)]; незалежний аналіз уразливостей [independent vulnerability analysis (AVA_VLA.2)]; систематичний незалежний аналіз уразливостей на основі заданих методик [(AVA_VLA.3)]; вичерпний аналіз уразливостей [moderately resistant (AVA_VLA.4)].

Р. ВГБ: аналіз стійкості засобів захисту /р. ТГБ: анализ стойкости средств защиты/ [Strength Of TOE security Functions (AVA_SOF)] — розділ ВГБ у класі ВГБ: оцінка захисту. Включає вимогу гарантій безпеки — оцінка стійкості засобів захисту [strength of TOE security function evaluation (AVA_SOF.1)].

Р. ВГБ: архітектура захисту /р. ТГБ: архитектура защиты/ [High-Level Design (ADV_HLD)] — розділ ВГБ у класі ВГБ: розробка. Включає наступні вимоги гарантій безпеки: опис архітектури захисту [descriptive high-level design (ADV_HLD.1)]; відповідність архітектури захисту політиці безпеки [security enforcing high-level design (ADV_HLD).2]; напівформальний опис архітектури захисту [semiformal high-level design (ADV_HLD.3)]; відповідність напівформального опису архітектури захисту політиці безпеки [semiformal high-level explanation (ADV_HLD.4)]; формальний опис архітектури захисту й доказ її відповідності політиці безпеки [formal high-level design (ADV_HLD.5)].

Р. ВГБ: безпека середовища розробки /р. ТГБ: безопасность среды разработки/ [DeVelopment Security (ALC_DVS)] — розділ ВГБ у класі ВГБ: процес розробки. Включає наступні вимоги гарантій безпеки: застосування заходів безпеки в ході розробки [identification of security measures (ALC_DVS.1)];

підтвердження заходів безпеки в ході розробки [sufficiency of security measures (ALC_DVS.2)].

Р. ВГБ: виправлення помилок і ліквідація уразливостей /р. ТГБ: исправление ошибок и устранение уязвимостей/ [FLaw Remediation (ALC_FLR)] — розділ ВГБ у класі ВГБ: процес розробки. Включає наступні вимоги гарантій безпеки: виправлення виявлених помилок і ліквідація уразливостей [basic flaw remediation (ALC_FLR.1)]; регулярне виправлення помилок і ліквідація уразливостей [flaw reporting procedures (ALC_FLR.2)]; гарантоване виправлення виявлених помилок і ліквідація виявлених уразливостей [systematic flaw remediation (ALC_FLR.2)].

Р. ВГБ: відповідність описів різного рівня /р. ТГБ: соответствие описаний разного уровня/ [Representation CorRespondente (ADV_RCR)] — розділ ВГБ у класі ВГБ: розробка. Включає наступні вимоги гарантій безпеки: неформальне підтвердження відповідності [informal correspondence demonstration (ADV_RCR.1)]; напівформальне підтвердження відповідності [semiformal correspondence demonstration (ADV_RCR.2)]; формальний доказ відповідності [formal correspondence demonstration (ADV_RCR.3)].

Р. ВГБ: глибина тестування /р. ТГБ: глубина тестирования/ [DePTh (ATE_DPT)] — розділ ВГБ у класі ВГБ: тестування. Включає наступні вимоги гарантій безпеки: архітектура [testing: high-level design (ALC_DPT.1)]; функціональні специфікації [testing: low-level design (ALC_DPT.2)]; реалізація [testing: implementation representation (ALC_DPT.3)].

Р. ВГБ: загальні функціональні специфікації /р. ТГБ: общие функциональные спецификации/ [Functional SPecification (ADV_FSP)] — розділ ВГБ у класі ВГБ: розробка. Включає наступні вимоги гарантій безпеки: неформальні специфікації для засобів захисту [informal functional specification (ADV_FSP.1)]; неформальні специфікації для усіх інтерфейсів засобів захисту [fully defined external interfaces (ADV_FSP.2)]; напівформальні специфікації для засобів захисту [semiformal functional specification (ADV_FSP.3)]; формальні специфікації для засобів захисту [formal functional specification (ADV_FSP.4)].

Р. ВГБ: засоби керування проектом /р. ТГБ: средства управления проектом/ [Configuration Management AUTomation (ACM_AUT)] — розділ ВГБ у класі ВГБ: керування проектом. Включає наступні

вимоги гарантій безпеки: застосування автоматизованих засобів керування проектом [partial configuration management automation (ACM_AUT.1)]; повна автоматизації керування проектом і контролю версій [complete configuration management automation (ACM_AUT.2)].

Р. ВГБ: засоби розробки /р. ТГБ: средства разработки/ [Tools And Techniques (ALC_TAT)] — розділ ВГБ у класі ВГБ: процес розробки. Включає наступні вимоги гарантій безпеки: використання певного набору засобів розробки [well-defined development tools (ALC_TAT.1)]; використання основних засобів розробки, що відповідають певним стандартам [compliance with implementation standards (ALC_TAT.2)]; використання тільки засобів розробки, що відповідають певним стандартам [compliance with implementation standards - all parts (ALC_TAT.3)].

Р. ВГБ: керівництво адміністратора /р. ТГБ: руководство администратора/ [ADMinistrator guidance (AGD_ADM)] — розділ ВГБ у класі ВГБ: документація. Включає вимогу гарантій безпеки — адміністрування засобів захисту [administrator guidance (AGD_ADM.1)].

Р. ВГБ: керівництво користувача /р. ТГБ: руководство пользователя/ [USeR guidance (AGD_USR)] — розділ ВГБ у класі ВГБ: документація. Включає вимогу гарантій безпеки — використання засобів захисту [user guidance (AGD_USR.1)].

Р. ВГБ: керування версіями /р. ВГБ: управление версиями/ [Configuration Management CAPabilities (ACM_CAP)] — розділ ВГБ у класі ВГБ: керування проектом. Включає наступні вимоги гарантій безпеки: нумерація версій [version numbers (ACM_CAP.1)]; ідентифікація компонентів [configuration items (ACM_CAP.2)]; контроль цілісності версій [authorisation controls (ACM_CAP.3)]; авторизація розробників при поновленні версій [generation support and acceptance procedures (ACM_CAP.4)]; контроль цілісності й автентичності дистрибутива системи [advanced support (ACM_CAP.5)].

Р. ВГБ: конфігурація проекта /р. ТГБ: конфигурация проекта/ [Configuration Management SCoPe (ACM_SCP)] — розділ ВГБ у класі ВГБ: керування проектом. Включає наступні вимоги гарантій безпеки: основні компоненти проекту (алгоритми, вихідні тексти, тексти, документація)[TOE management automati-

on coverage (ASM_SCP.1)]; включення до складу конфігурації об'єкта виявлених помилок і уразливостей [problem tracking management automation coverage (ASM_SCP.2)]; включення до складу конфігурації проекту інструментальних засобів розробки [development tools management automation coverage (ASM_SCP.3)].

Р. ВГБ: методика тестування /р. ТГБ: методика тестирования/ [FUNctional tests (ATE_FUN)] — розділ ВГБ у класі ВГБ: тестування. Включає наступні вимоги гарантій безпеки: функціональне тестування й протоколювання результатів тестів [functional testing (ALC_FUN.1)]; тестування у відповідності з певною методикою [ordered functional testing (ALC_FUN.2)].

Р. ВГБ: незалежне тестування /р. ТГБ: независимое тестирования/ [INDependent testing (ATE_IND)] — розділ ВГБ у класі ВГБ: тестування. Включає наступні вимоги гарантій безпеки: готовність продукту до незалежного тестування [independent testing - conformance (ALC_IND.1)]; вибіркове незалежне тестування [independent testing - sample (ALC_IND.2)]; повне незалежне тестування [independent testing - complete (ALC_IND.3)].

Р. ВГБ: повнота тестування /р. ТГБ: полнота тестирования/ [COVerage (ATE_COV)] — розділ ВГБ у класі ВГБ: тестування. Включає наступні вимоги гарантій безпеки: обґрунтування повноти тестування [evidence of coverage (ATE_COV.1)]; аналіз повноти тестування [analysis of coverage (ATE_COV.2)]; строгий аналіз повноти тестування [rigorous analysis of coverage (ATE_COV.3)].

Р. ВГБ: політика безпеки /р. ТГБ: политика безопасности/ [Security Policy Modeling (ADV_SPM)] — розділ ВГБ у класі ВГБ: розробка. Включає наступні вимоги гарантій безпеки: неформальний опис політики безпеки [informal TOE security policy model (ADV_SPM.1)]; напівформальний опис політики безпеки [semiformal TOE security policy model (ADV_SPM.2)]; формальна модель політики безпеки [formal TOE security policy model (ADV_SPM.3)]

Р. ВГБ: поставка /р. ТГБ: поставка/ [DELivery (ADO_DEL)] — розділ ВГБ у класі ВГБ: дистрибуція. Включає наступні вимоги гарантій безпеки: регламентована процедура поставки [delivery procedures (ADO_DEL.1)]; виявлення спотворень у процесі поставки [detection of modification (ADO_DEL.2)]; захист

від спотворень у процесі поставки [prevention of modification (ADO_DEL.3)].

Р. ВГБ: структура засобів захисту /р. ТГБ: структура средств защиты/ [TSF INTernals (ADV_INT)] — розділ ВГБ у класі ВГБ: розробка. Включає наступні вимоги гарантій безпеки: модульність [modularity (ADV_INT.1)]; ієрархічність [reduction of complexity (ADV_INT.2)]; мінімізація складності [minimisation of complexity (ADV_INT.3)].

Р. ВГБ: технологія розробки /р. ТГБ: технология разработки/ [Life Cycle Definition (ALC_LCD)] — розділ ВГБ у класі ВГБ: процес розробки. Включає наступні вимоги гарантій безпеки: визначена розробником технологія розробки [developer defined life-cycle model (ALC_LCD.1)]; стандартизована технологія розробки [standardised life-cycle model (ALC_LCD.2)]; технологія розробки, що дозволяє оцінювати продукт, що розроблюється [measurable life-cycle model (ALC_LCD.3)].

Р. ВГБ: установка, настройка, запуск /р. ТГБ: установка, настройка, запуск/ [Installation, Generation, and Start-up (ADO_IGS)] — розділ ВГБ у класі ВГБ: дистрибуція. Включає наступні вимоги гарантій безпеки: регламентовані процедури установки, настройки, запуску [installation, generation, and start-up procedures (ADO_IGS.1)]; протоколювання процесу установки, настройки, запуску [generation log (ADO_IGS.2)].

Р. ВГБ: форма надання продукту на сертифікацію /р. ТГБ: форма представления продукта на сертификацию/ [IMPlementation representation (ADV_IMP)] — розділ ВГБ у класі ВГБ: розробка. Включає наступні вимоги гарантій безпеки: опис реалізації обмеженої підмножини засобів захисту [subset of the implementation of the TSF (ADV_IMP.1)]; повний опис реалізації усіх засобів захисту [implementation of the TSF (ADV_IMP.2)]; структурований опис реалізації усіх засобів захисту [structured implementation of the TSF (ADV_IMP.3)].

Р. ВГБ: часткові специфікації засобів захисту /р. ТГБ: частные спецификации средств защиты/ [Low-Level Design (ADV_LLD)] — розділ ВГБ у класі ВГБ: розробка. Включає наступні вимоги гарантій безпеки: неформальні часткові специфікації засобів захисту [descriptive low-level design (ADV_LLD.1)] ; на-

півформальні часткові специфікації засобів захисту [semiformal low-level design (ADV_LLD.2)] ; формальні часткові специфікації засобів захисту [formal low-level design (ADV_LLD.3)].

Р. ФВБ /р. ФТБ/ [assurance family] — складова частина класу ФВБ. Структура розділу містить наступні елементи: назва й позначення розділу [family name]; опис розділу [family behaviour]; ранжирування вимог [component levelling]; керовані параметри [management]; об'єкти реєстрації й обліку [audit]; вимоги [components]. Кожний розділ має свою унікальну назву і семисимвольний ідентифікатор, який складається з трибуквеного ідентифікатора класу, знаку підкреслення і трибуквеного позначення розділу. Набір вимог представляє собою ієрархічну структуру, в якій підсилення вимог здійснюється монотонно, але при цьому не є лінійним упорядкованим списком. Вимоги, які стоять в ієрархії вище інших включають в себе нижчестоящі вимоги. Це означає, що у профілі захисту необхідно використати тільки одну з таких вимог. Вимоги, які не зв'язані відносинами ієрархічності є незалежними і можуть використовуватися одночасно.

Р. ФВБ: автентифікаційні параметри /р. ФТБ: аутентификационные параметры/ [Specification Of Secrets (FIA_SOS)] — розділ ФВБ у класі ФВБ: ідентифікація й автентифікація. Включає незалежні вимоги безпеки функціональні: перевірка якості автентифікаційних параметрів відповідно до заданих критеріїв [verification of secrets (FIA_SOS.1)]; автоматична генерація автентифікаційних параметрів і перевірка їхньої якості відповідно до заданих критеріїв [TSF generation of secrets (FIA_SOS.2)].

Р. ФВБ: автентифікація інформації /р. ФТБ: аутентификации информации/ [Data AUtentification (FDP_DAU)] — розділ ФВБ у класі ФВБ: захист інформації. Включає ієрархічно залежні вимоги безпеки функціональні: автентифікація інформації, що міститься в об'єкті доступу [basic data authentication (FDP_DAU.1)]; автентифікація інформації, що міститься в об'єкті доступу з ідентифікацією суб'єкта, що здійснює автентифікацію [data authentication with identity of guarantor (FDP_DAU.2)].

Р. ФВБ: автентифікація користувачів /р. ФТБ: аутентификация пользователей/ [User AUthentication (FIA_UAU)] — розділ ФВБ у класі ФВБ: ідентифікація й автентифікація. Включає незалежні вимоги безпеки функціональні: обов'язковість автентифікації користувачів [timing of authentication (FIA_UAU.1)];

механізм автентифікації повинен розпізнавати і попереджувати використання підроблених автентифікаційних параметрів або їхніх дублікатів [unforgeable authentication (FIA_UAU.3)]; використання одноразових автентифікаційних параметрів [single-use authentication mechanisms (FIA_UAU.4)]; використання множини механізмів автентифікації, що використовується залежно від ситуації [multiple authentication mechanisms (FIA_UAU.5)]; застосування механізмів повторної автентифікації для виконання встановленої множини операцій [re-authenticating (FIA_UAU.6)]; мінімізація інформації, що надається користувачеві в процесі проходження процедури автентифікації [protected authentication feedback (FIA_UAU.7)]. Вимога FIA_UAU.1 підсилюється вимогою — неможливість здійснення дій, що контролюються засобами захисту, без успішного проходження процедури автентифікації [user authentication before any action (FIA_UAU.2)];

Р. ФВБ: автоматичне реагування на спроби порушення безпеки /р. ФТБ: автоматическое реагирование на попытки нарушения безопасности/ [security audit Automatic ResPonse (FAU_ARP)] — розділ ФВБ у класі ФВБ: аудит. Включає вимогу безпеки функціональну — засоби захисту повинні реагувати на спроби порушення безпеки [security alarms (FAU_ARP.1)].

Р. ФВБ: адміністративні ролі /р. ФТБ: административные роли/ [Security Management Roles (FMT_SMR)] — розділ ФВБ у класі ФВБ: керування безпекою. Включає наступні вимоги безпеки функціональні: використання адміністративних ролей для керування безпекою [security roles (FMT_SMR.1)]; надання ролевих повноважень за запитом користувача [assuming roles (FMT_SMR.3)]. Вимога FMT_SMR.1 підсилюється вимогою — використання упорядкованого набору адміністративних ролей для керування безпекою [restrictions on security roles (FMT_SMR.2)].

Р. ФВБ: аналіз протоколу аудита /р. ФТБ: анализ протокола аудита/ [Security Audit Analysis (FAU_SAA)] — розділ ФВБ у класі ФВБ: аудит. Включає вимогу безпеки функціональну — виявлення потенційно небезпечних подій на основі контролю за діапазонами параметрів обліку на основі фіксованої множини правил [potential violation analysis (FAU_SAA.1)], яка підсилюється двома незалежними вимогами — статистичне розпізнавання вторгнень на основі аналізу профілів роботи користувачів [profile based

anomaly detection (FAU_SAA.2)] і динамічне розпізнавання сигнатур елементарних атак на основі простих евристик [simple attack heuristics (FAU_SAA.3)]. Вимога FAU_SAA.3 підсилюється вимогою — розпізнавання комплексних атак на основі складних евристик [complex attack heuristics (FAU_SAA.4)].

Р. ФВБ: анонімність користувачів /р. ФТБ: анонимность пользователей/ [ANOnymity (FPR_ANO)] — розділ ФВБ у класі ФВБ: конфіденційність роботи в системі. Включає ієрархічно залежні вимоги безпеки функціональні: анонімність суб'єктів, які представляють інтереси користувачів [anonymity (FPR_ANO.1)]; анонімність ідентифікаторів користувачів для середовища захисту [anonymity without soliciting information (FPR_ANO.2)].

Р. ФВБ: анонімність сеансів роботи із системою /р. ФТБ: анонимность сеансов работы в системе/ [UNLinkability (FPR_UNL)] — розділ ФВБ у класі ФВБ: конфіденційність роботи в системі. Включає вимогу безпеки функціональну — неможливість встановлення ініціатора операцій, що здійснюються в системі [unlinkability (FPR_UNL.1)].

Р. ФВБ: атрибути безпеки користувачів /р. ФТБ: атрибуты безопасности пользователей/ [user ATtribute Definition (FIA_ATD)] — розділ ФВБ у класі ФВБ: ідентифікація й автентифікація. Включає вимогу безпеки функціональну — індивідуальне призначення атрибутів безпеки користувачів [user attribute definition (FIA_ATD.1)].

Р. ФВБ: безпечне відновлення після збоїв /р. ФТБ: безопасное восстановление после сбоев/ [trusted ReCoVery (FPT_RCV)] — розділ ФВБ у класі ФВБ: надійність засобів захисту. Включає незалежні вимоги безпеки функціональні: ручне відновлення після збоїв [manual recovery (FPT_RCV.1)]; відновлення після збоїв шляхом здійсненні відкоту в безпечний стан [function recovery (FPT_RCV.4)]. Вимога FPT_RCV.1 підсилюється ієрархічно залежними вимогами: автоматичне відновлення після збоїв [automated recovery (FPT_RCV.2)]; автоматичне відновлення після збоїв з мінімізацією втрат інформації [automated recovery without undue loss (FPT_RCV.3)].

Р. ФВБ: блокування сеансу роботи із системою /р. ФТБ: блокирование сеанса работы с систе-

мой/ [SeSsion Locking (FTA_SSL)] — розділ ФВБ у класі ФВБ: контроль доступу до системи. Включає незалежні вимоги безпеки функціональні: автоматичне блокування сеансу роботи після вказаного періоду неактивності [TSF-initiated session locking (FTA_SSL.1)]; блокування сеансу користувачем [user-initiated locking (FTA_SSL.2)]; автоматичне завершення сеансу роботи після закінчення заданого періоду неактивності [TSF-initiated termination (FTA_SSL.3)].

Р. ФВБ: використання псевдонімів /р. ФТБ: использование псевдонимов/ [PSEudonymity (FPR_PSE)] — розділ ФВБ у класі ФВБ: конфіденційність роботи в системі. Включає вимоги безпеки функціональні — контроль дій анонімних користувачів за допомогою псевдонімів [pseudonymity (FPR_PSE.1)], яка підсилюється незалежними вимогами —- встановлення особистості користувача за псевдонімом [reversible pseudonymity (FPR_PSE.2)] і призначення псевдонімів відповідно до заданих правил [alias pseudonymity (FPR_PSE.3)].

Р. ФВБ: відбір подій для реєстрації й обліку /р. ФТБ: отбор событий для регистрации и учета/ [security audit event SELection (FAU_SEL)] — розділ ФВБ у класі ФВБ: аудит. Включає вимогу безпеки функціональну — визначення множини властивих аудитові подій на основі заданого набору атрибутів [selective audit (FAU_SEL.1)].

Р. ФВБ: відкіт /р. ФТБ: откат/ [ROLlback (FDP_ROL)] — розділ ФВБ у класі ФВБ: захист інформації. Включає незалежні вимоги безпеки функціональні: обмеження можливості здійснення відкоту для певної підмножини операцій на задане число кроків [basic rollback (FDP_ROL.1)]; розширення можливостей здійснення відкоту для всіх операцій на задане число кроків [advanced rollback (FDP_ROl.2)].

Р. ФВБ: відкликання атрибутів безпеки /р. ФТБ: отзыв атрибутов безопасности/ [REVolocation (FMT_REV)] — розділ ФВБ у класі ФВБ: керування безпекою. Включає вимогу безпеки функціональну — відкликання атрибутів безпеки відповідно до встановлених правил [revocation (FMT_REV.1)].

Р. ФВБ: відповідність користувачів і суб'єктів /р. ФТБ: соответствие пользователей и субъектов/ [User-Subject Binding (FIA_USB)] — розділ ФВБ у класі ФВБ: ідентифікація і автентифікація. Включає

вимогу безпеки функціональну — присвоєння суб'єктам, що діють від імені користувача, його атрибутів безпеки [user-subject binding (FIA_USB.1)].

Р. ФВБ: готовність засобів захисту до обслуговування віддалених клієнтів /р. ФТБ: готовность средств защиты к обслуживанию удаленных клиентов/ [availability of exported TSF data (FPT_ITA)] — розділ ФВБ у класі ФВБ: надійність засобів захисту. Включає вимогу безпеки функціональну — забезпечення готовності засобів захисту до обслуговування віддалених клієнтів із заданою ймовірністю [inter-TSF availability within a defined availability metric (FPT_ITA.1)].

Р. ФВБ: доступ до протоколу аудита /р. ФТБ: доступ до протокола аудита/ [Security Audit Review (FAU_SAR)] — розділ ФВБ у класі ФВБ: аудит. Включає незалежні вимоги безпеки функціональні: надання доступу до протоколу аудита для обмеженого набору авторизованих користувачів [audit review (FAU_SAR.1)]; захист протоколу аудита від неавторизованих користувачів [restricted audit review (FAU_SAR.2)]; вибіркове керування доступом до протоколу аудита [selectable audit review (FAU_SAR.3)].

Р. ФВБ: експорт інформації із системи /р. ФТБ: экспорт информации из системы/ [Export to outside TSF Control (FDP_ETC)] — розділ ФВБ у класі ФВБ: захист інформації. Включає незалежні вимоги безпеки функціональні: експорт інформації без атрибутів безпеки [export of user data without security attributes (FDP_ETC.1)]; експорт інформації разом з атрибутами безпеки [export of user data with security attributes (FDP_ETC.2)].

Р. ФВБ: засоби керування доступом /р. ФТБ: средства управления доступом/ [Access Control Functions (FDP_ACF)] — розділ ФВБ у класі ФВБ: захист інформації. Включає вимогу безпеки функціональну — керування доступом на основі атрибутів безпеки або іменованих груп атрибутів з явним дозволом або відмовою в доступі [security attribute based access control (FDP_ACF.1)].

Р. ФВБ: засоби керування інформаційними потоками /р. ФТБ: средства управления информационными потоками/ [Information Flow control Functions (FDP_IFF)] — розділ ФВБ у класі ФВБ: захист інформації. Включає незалежні вимоги безпеки функціональні: керування інформаційними потоками

на основі атрибутів безпеки інформації й суб'єктів, між якими здійснюється обмін інформацією [simple security attributes (FDP_IFF.1)]; контроль схованих інформаційних потоків [limited illicit information flows (FDP_IFF.3)]; моніторинг схованих інформаційних потоків і обмеження їхньої пропускної здатності [illicit information flow monitoring (FDP_IFF.6)]. Вимога FDP_IFF.1 підсилюється вимогою — керування інформаційними потоками на основі ієрархічно впорядкованих атрибутів безпеки, присвоєних усім інформаційним потокам і утворюючих грати [hierarchical security attributes (FDP_IFF.2)]. Вимога FDP_IFF.3 підсилюється ієрархічно залежними вимогами: часткова заборона схованих інформаційних потоків [partial elimination of illicit information flows (FDP_IFF.4)]; повна заборона схованих інформаційних потоків [no illicit information flows (FDP_IFF.5)].

Р. ФВБ: захист від збоїв /р. ФТБ: защита от сбоев/ [FaiL Secure (FPT_FLS)] — розділ ФВБ у класі ФВБ: надійність засобів захисту. Включає вимогу безпеки функціональну — збереження безпечного стану у випадку виникнення збоїв [failure with preservation of secure state (FPT_FLS.1)].

Р. ФВБ: захист від моніторингу сеансів роботи із системою /р. ФТБ: защита от мониторинга сеансов работы с системой/ [UNObservability (FPR_UNO)] — розділ ФВБ у класі ФВБ: конфіденційність роботи в системі. Включає незалежні вимоги безпеки функціональні: захист операцій, що відбуваються в системі, від моніторингу [unobservability (FPR_UNO.1)]; заборона засобам захисту запитувати у користувача конфіденційну інформацію [unobservability without soliciting information (FPR_UNO.3)]; моніторинг роботи системи і використання ресурсів тільки авторизованими користувачами [authorised user observability (FPR_UNO.4)]. Вимога FPR_UNO.1 підсилюється вимогою — розосередження критичної інформації між різними компонентами засобів захисту [allocation of information impacting unobservability (FPR_UNO.2)].

Р. ФВБ: захист внутрішніх каналів інформаційного обміну між засобами захисту /р. ФТБ: защита внутренних каналов информационного обмена между средствами защиты/ [Internal TOE TSF data transfer (FPT_ITT)] — розділ ФВБ у класі ФВБ: надійність засобів захисту. Включає вимогу безпеки функціональну — базові засоби захисту інформаційного обміну між засобами захисту [basic internal TSF data

transfer protection (FPT_ITT.1)], яка підсилюється незалежними вимогами — розподіл трафіка інформаційного обміну між засобами захисту і трафіка прикладних засобів [TSF data transfer separation (FPT_ITT.2)] і контроль цілісності інформації при взаємодії засобів захисту [TSF data integrity monitoring (FPT_ITT.3)].

Р. ФВБ: захист внутрішньосистемного передавання інформації при використанні зовнішніх каналів /р. ФТБ: защита внутрисистемной передачи информации при использовании внешних каналов/ [inter-TSF User data Confidentiality Transfer protection (FDP_UCT)] — розділ ФВБ у класі ФВБ: захист інформації. Включає вимогу безпеки функціональну — захист інформації при спрямуванні її у зовнішній канал [basic data exchange confidentiality (FDP_UCT.1)].

Р. ФВБ: захист інформації при передаванні внутрішніми каналами /р. ФТБ: защита информации при передаче внутренними каналами/ [Internal TOE Transfer (FDP_ITT)] — розділ ФВБ у класі ФВБ: захист інформації. Включає незалежні вимоги безпеки функціональні — базові засоби захисту інформації, що передається [basic internal transfer protection (FDP_ITT.1)] і контроль цілісності інформації, що передається [integrity monitoring (FDP_ITT.3)], які відповідно підсилюються вимогами — передавання даних з різними атрибутами безпеки окремими каналами [transmission separation by attribute (FDP_ITT.2)] і застосування різноманітних методів контролю цілісності в залежності від атрибутів безпеки [attribute-based integrity monitoring (FDP_ITT.4)].

Р. ФВБ: знищення залишкової інформації /р. ФТБ: уничтожение остаточной информации/ [Residual Information Protection (FDP_RIP)] — розділ ФВБ у класі ФВБ: захист інформації. Включає ієрархічно залежні вимоги безпеки функціональні: знищення залишкової інформації для певної підмножини об'єктів при їхньому створенні й вилученні [subset residual information protection (FDP_RIP.1)]; знищення залишкової інформації для всіх об'єктів при їх створенні або вилученні [full residual information protection (FDP_RIP.2)].

Р. ФВБ: ідентифікація користувачів /р. ФТБ: идентификация пользователей/ [User IDentification (FIA_UID)] — розділ ФВБ у класі ФВБ: ідентифікація й автентифікація. Включає ієрархічно залежні вимо-

ги безпеки функціональні: обов'язковість ідентифікації користувачів [timing of identification (FIA_UID.1)]; неможливість здійсненні дій, що контролюються засобами захисту, без успішного проходження процедури ідентифікації [user identification before any action (FIA_UID.2)].

Р. ФВБ: імпорт інформації /р. ФТБ: импорт информации/ [Import from outside TSF Control (FDP_ITC)] — розділ ФВБ у класі ФВБ: захист інформації. Включає незалежні вимоги безпеки функціональні: імпорт інформації без атрибутів безпеки [import of user data without security attributes (FDP_ITC.1)]; імпорт інформації разом з атрибутами безпеки [import of user data with security attributes (FDP_ITC.2)].

Р. ФВБ: квотування ресурсів /р. ФТБ: квотирование ресурсов/ [ReSource Allocation (FRU_RSA)] — розділ ФВБ у класі ФВБ: контроль за використанням ресурсів. Включає ієрархічно залежні вимоги безпеки функціональні: обмеження на споживання користувачами ресурсів системи за допомогою квот [maximum quotas (FRU_RSA.1)]; обмеження на споживання користувачами ресурсів системи за допомогою квот і резервування для споживача гарантованої множини ресурсів [minimum and maximum quotas (FRU_RSA.2)].

Р. ФВБ: керування атрибутами безпеки /р. ФТБ: управление атрибутами безопасности/ [Management of Security Attributes (FMT_MSA)] — розділ ФВБ у класі ФВБ: керування безпекою. Включає незалежні вимоги безпеки функціональні: керування авторизованими користувачами атрибутами безпеки [management of security attributes (FMT_MSA.1)]; контроль коректності значень атрибутів безпеки [secure security attributes (FMT_MSF.2)]; коректна ініціалізація атрибутів безпеки визначеними значеннями [static attribute initialization (FMT_MSA.3)].

Р. ФВБ: керування засобами захисту /р. ФТБ: управление средствами защиты/ [Management Of Functions in TSF (FMT_MOF)] — розділ ФВБ у класі ФВБ: керування безпекою. Включає вимогу безпеки функціональну — керування авторизованими користувачами засобами захисту [management of security functions behaviour (FMT_MOF.1)].

Р. ФВБ: керування ключами /р. ФТБ: управление ключами/ [Cryptographic Key Management (FCO_CKM)] — розділ ФВБ у класі ФВБ: криптографія. Включає незалежні вимоги безпеки функціо-

нальні: генерація ключів заданого розміру за певними алгоритмами у відповідності до певних стандартів [cryptographic key generation (FCO_CKM.1)]; розподіл ключів способами, визначеними в спеціальних стандартах [cryptographic key distribution (FCO_CKM.2)]; здійснення доступу до ключів з використанням методів, визначених у спеціальних стандартах [(FCO_CKM.3)]; знищення ключів з використанням методів, визначених у спеціальних стандартах [cryptographic key destruction (FCO_CKM.4)].

Р. ФВБ: керування параметрами й конфігурацією засобів захисту /р. ФТБ: управление параметрами и конфигурацией средств защиты/ [Management of TSF Data (FMT_MTD)] — розділ ФВБ у класі ФВБ: керування безпекою. Включає незалежні вимоги безпеки функціональні: керування параметрами й конфігурацією засобів захисту авторизованими користувачами [management of TSF data (FMT_MTD.1)]; виконання заданих дій у випадку виходу параметрів функціонування засобів захисту за встановлені межі [management of limits on TSF data (FMT_MTD.2)]; автоматичний контроль коректності конфігурації й параметрів засобів захисту [secure TSF data (FMT_MTD.3)].

Р. ФВБ: керування сеансами роботи із системою /р. ФТБ: управление сеансами работы с системой/ [TOE Session Establishment (FTA_TSE)] — розділ ФВБ у класі ФВБ: контроль доступу до системи. Включає вимогу безпеки функціональну — заборона встановлення сеансу роботи із системою на основі заданої множини правил [TOE session establishment (FTA_TSE.1)].

Р. ФВБ: контроль цілісності інформації у процесі зберігання /р. ФТБ: контроль целостности информации в процессе хранения/ [Stored Data Integrity (FDP_SDI)] — розділ ФВБ у класі ФВБ: захист інформації. Включає ієрархічно залежні вимоги безпеки функціональні: виявлення порушень цілісності інформації у процесі зберігання [stored data integrity monitoring (FDP_SDI.1)]; виявлення порушень цілісності інформації у процесі зберігання і визначення реакції на виявлені помилки [stored data integrity monitoring and action (FDP_SDI.2)].

Р. ФВБ: конфіденційність інформації, що передається, при роботі з віддаленими клієнтами /р. ФТБ: конфиденциальность передаваемой информации при работе с удаленными клиентами/ [confidenti-

ality of exported TSF data (FPT_ITC)] — розділ ФВБ у класі ФВБ: надійність засобів захисту. Включає вимогу безпеки функціональну — забезпечення конфіденційності інформації, що передається між засобами захисту і віддаленими клієнтами [inter-TSF confidentiality during transmission (FPT_ITC.1)].

Р. ФВБ: криптографічні засоби /р. ФТБ: криптографические средства/ [Cryptographic OPeration (FCO_COP)] — розділ ФВБ у класі ФВБ: криптографія. Включає вимогу безпеки функціональну — виконання криптографічних операцій з використанням ключів заданого розміру і визначених алгоритмів у відповідності до спеціальних стандартів [cryptographic operation (FCO_COP.1)].

Р. ФВБ: моніторинг взаємодій /р. ФТБ: мониторинг взаимодействий/ [Reference Mediation (FPT_RVM)] — розділ ФВБ у класі ФВБ: надійність засобів захисту. Включає вимогу безпеки функціональну — моніторинг усіх взаємодій у системі [non-bypassability of the TSP (FPT_RVM.1)].

Р. ФВБ: об'яви, попередження, запрошення й підказки /р. ФТБ: объявления, предупреждения, приглашения и подсказки/ [TOE Assess Banners (FTA_TAB)] — розділ ФВБ у класі ФВБ: контроль доступу до системи. Включає функціональну вимогу безпеки — демонстрація об'яв, попереджень, запрошень і підказок перед початком сеансу роботи із системою [default TOE access banners (FTA_TAB.1)].

Р. ФВБ: обмеження на використання атрибутів безпеки /р. ФТБ: ограничения на использование атрибутов безопасности/ [Limitation on scope of Selectable Attributes (FTA_LSA)] — розділ ФВБ у класі ФВБ: контроль доступу до системи. Включає вимогу безпеки функціональну — обмеження множини атрибутів безпеки, які використовуються користувачем у межах однієї сесії [limitation on scope of selectable attributes (FTA_LSA.1)].

Р. ФВБ: обмеження терміну дії атрибутів безпеки /р. ФТБ: ограничение времени действия атрибутов безопасности/ [Security Attribute Expiration (FMT_SAE)] — розділ ФВБ у класі ФВБ: керування безпекою. Включає вимогу безпеки функціональну — призначення терміну дії атрибутів безпеки авторизованими користувачами [time-limited authorization (FMT_SAE.1)].

Р. ФВБ: обмеження числа одночасних сеансів /р. ФТБ: ограничение числа одновременных сеан-

сов/ [limitation on Multiple Concurrent Sessions (FTA_MCS)] — розділ ФВБ у класі ФВБ: контроль доступу до системи. Включає ієрархічно залежні вимоги безпеки функціональні: обмеження числа одночасних сеансів [basic limitation on multiple concurrent sessions (FTA_MCS.1)]; обмеження числа одночасних сеансів у залежності від атрибутів безпеки користувачів [per user attribute limitation on multiple concurrent sessions (FTA_MCS.2)].

Р. ФВБ: погодженість обміну інформацією між засобами захисту /р. ФТБ: согласованность обмена информацией между средствами защиты/ [inter-TSF TSF Data Consistency (FPT_TDC)] — розділ ФВБ у класі ФВБ: надійність засобів захисту. Включає вимогу безпеки функціональну — коректність перетворення інформації при передаванні між засобами захисту [inter-TSF basic TSF data consistency (FPT_TDC.1)].

Р. ФВБ: політики керування доступом /р. ФВБ: политики управления доступом/ [ACcess Control policy (FDP_ACC)] — розділ ФВБ у класі ФВБ: захист інформації. Включає ієрархічно залежні вимоги безпеки функціональні: керування доступом для обмеженої множини операцій і об'єктів [subset access control (FDP_ACC.1)]; керування доступом для повної множини об'єктів, суб'єктів і операцій. Будь-яка операція, яка здійснюється будь-яким об'єктом, повинна контролюватися принаймні одною політикою керування доступом [complete access control (FDP_ACC.2)].

Р. ФВБ: політики керування інформаційними потоками /р. ФТБ: политики управления информационными потоками/ [Information Flow Control policy (FDP_IFC)] — розділ ФВБ у класі ФВБ: захист інформації. Включає ієрархічно залежні вимоги безпеки функціональні: керування інформаційними потоками для обмеженої множини операцій і потоків [subset information flow control (FDP_IFC.1)]; керування доступом до повної множини потоків, суб'єктів і операцій. Будь-яка політика керування потоками повинна контролювати всі операції у системі. Усі потоки інформації в системі повинні контролюватися принаймні однією політикою керування інформаційними потоками [complete information flow control (FDP_IFC.2)].

Р. ФВБ: попередження відмови від факту передавання інформації /р. ФТБ: предотвраще-

ние отречения от факта передачи информации/ [Non-Repudiation of Origin (FCO_NRO)] — розділ ФВБ у класі ФВБ: причетність до приймання/передавання. Включає ієрархічно залежні вимоги безпеки функціональні: підтвердження факту передавання інформації за вимогою [selective proof of origin (FCO_NRO.1)]; автоматичне підтвердження факту передавання інформації [enforced proof of origin (FCO_NRO.2)].

Р. ФВБ: попередження відмови від факту приймання інформації /р. ФТБ: предотвращение отречения от факта передачи информации/ [Non-Repudiation of Receipt (FCO_NRR)] — розділ ФВБ у класі ФВБ: причетність до приймання/передавання. Включає ієрархічно залежні вимоги безпеки функціональні: підтвердження факту одержання інформації за вимогою [selective proof of receipt (FCO_NRR.1)]; автоматичне підтвердження факту одержання інформації [enforced proof of receipt (FCO_NRR.2)].

Р. ФВБ: протокол аудиту /р. ФТБ: протокол аудита/ [security audit event SToraGe (FAU_STG)] — розділ ФВБ у класі ФВБ: аудит. Включає дві незалежні вимоги безпеки функціональні — виділення ресурсів під протокол аудита, захист протоколів від неавторизованої модифікації або видалення [protected audit trail storage (FAU_STG.1)] і попередження втрати записів протоколу аудита у випадку зменшення об'єму ресурсів, які відведені під протокол аудита до певної межі [action in case of possible audit data loss (FAU_STG.3)], кожна з яких підсилюється відповідно вимогами — гарантована доступність протоколу аудита [guarantees of audit data availability (FAU_STG.2)] і попередження втрат записів аудита у випадку вичерпання ресурсів, які відведені під протокол аудита [prevention of audit data loss (FAU_STG.4)].

Р. ФВБ: протокол сеансів роботи із системою /р. ФТБ: протокол сеансов работы пользователей/ [TOE Assess History (FTA_TAH)] — розділ ФВБ у класі ФВБ: контроль доступу до системи. Включає вимогу безпеки функціональну — реєстрація й демонстрація користувачам протоколу сеансів їхньої роботи й спроб входу в систему [TOE access history (FTA_TAH.1)].

Р. ФВБ: пряма взаємодія між засобами захисту /р. ФТБ: прямое взаимодействие между средствами защиты/ [Inter-TSF Trusted Channel (FTP_ITS)] — розділ ФВБ у класі ФВБ: пряма взаємодія. Включає вимогу безпеки функціональну — пряма взаємодія між компонентами між засобами захисту рі-

зних продуктів [inter-TSF trusted channel (FTP_ITS.1)].

Р. ФВБ: пряма взаємодія між користувачами /р. ФТБ: прямое взаимодействие пользователями/ [TRusted Path (FTP_TRP)] — розділ ФВБ у класі ФВБ: пряма взаємодія. Включає вимогу безпеки функціональну — пряма взаємодія з користувачами для вказаного набору ситуацій або за бажанням користувача [trusted path (FTP_TRP.1)].

Р. ФВБ: реакція на невдалі спроби автентифікації /р. ФТБ: реакция на неудачные попытки аутентификации/ [Authentication FaiLures (FIA_AFL)] — розділ ФВБ у класі ФВБ: ідентифікація й автентифікація. Включає функціональну вимогу безпеки — засоби ідентифікації й автентифікації повинні припиняти спроби встановлення сеансів роботи з системою після встановленого числа невдалих спроб автентифікації і призупиняти обслуговування засобів, що задіяні в ході цих спроб [authentication failure handling (FIA_AFL.1)].

Р. ФВБ: реєстрація й облік подій /р. ФТБ: функциональных требований: регистрация и учет событий/ [security audit data GENeration (FAU_GEN)] — розділ ФВБ у класі ФТБ: аудит. Включає незалежні вимоги безпеки функціональні: реєстрація заданої множини подій і задавання облікової інформації для подій кожного типу [audit data generation (FAU_GEN.1)]; реєстрація і облік подій та реєстрація користувачів, які ініціювали події [user identity association (FAU_GEN.2)].

Р. ФВБ: реплікація інформації, що використовується засобами захисту /р. ФТБ: репликация информации, используемой средствами защиты/ [internal TOE TSF data Replication Consistency (FPT_TRC)] — розділ ФВБ у класі ФВБ: надійність засобів захисту. Включає вимогу безпеки функціональну — контроль узгодженості копій інформації, що використовується засобами захисту [internal TSF consistency (FPT_TRC.1)].

Р. ФВБ: розпізнавання повторного передавання інформації та імітація подій /р. ФТБ: распознавание повторных передач и имитация событий/ [RePLay detection (FPT_RPL)] — розділ ФВБ у класі ФВБ: надійність засобів захисту. Включає вимогу безпеки функціональну — забезпечення конфіденційності

інформації, що передається між засобами захисту і віддаленими клієнтами [replay detection (FPT_RPL.1)].

Р. ФВБ: розподіл доменів /р. ФТБ: распределение доменов/ [domain SEParation (FPT_SEP)] — розділ ФВБ у класі ФВБ: надійність засобів захисту. Включає ієрархічно залежні вимоги безпеки функціональні: виділення спеціального домена для засобів захисту [TSF domain separation (FPT_SEP.1)]; виділення окремих доменів для процедур, що здійснюють моніторинг взаємодії і реалізують вказані політики безпеки [SFP domain separation (FPT_SEP.2)]; виділення окремих доменів для процедур. що здійснюють моніторинг взаємодій і реалізують будь-які політики безпеки [complete reference monitor (FPT_SEP.3)].

Р. ФВБ: розподіл ресурсів на основі пріоритетів /р. ФТБ: распределение ресурсов на основе приоритетов/ [PRiority of Service(FRU_PRS)] — розділ ФВБ у класі ФВБ: контроль за використанням ресурсів. Включає ієрархічно залежні вимоги безпеки функціональні: розподіл обмеженої підмножини ресурсів системи на основі пріоритетів [limited priority of service (FRU_PRS.1)]; розподіл усіх ресурсів на основі пріоритетів [full priority of service (FRU_PRS.2)].

Р. ФВБ: самотестування засобів захисту /р. ФТБ: самотестирование средств защиты/ [TSF Self Test (FPT_TST)] — розділ ФВБ у класі ФВБ: надійність засобів захисту. Включає вимогу безпеки функціональну — самотестування засобів захисту за запитом, у процесі завантаження і функціонування. Перевірка цілісності коду і даних засобів захисту [TSF testing (FPT_TST.1)].

Р. ФВБ: синхронізація /р. ФТБ: синхронизация/ [State Synchrony Protocol (FPT_SSP)] — розділ ФВБ у класі ФВБ надійність засобів захисту. Включає ієрархічно залежні вимоги безпеки функціональні: підтвердження приймання інформації [simple trusted acknowledgement (FPT_SSP.1)]; синхронізація стану учасників взаємодії у ході обміну інформацією [mutual trusted acknowledgement (FPT_SSP.2)].

Р. ФВБ: стійкість до відмов /р. ФТБ: отказоустойчивость/ [FauLt Tolerance (FRU_FLT)] — розділ ФВБ у класі ФВБ: контроль за використанням ресурсів. Включає ієрархічно залежні вимоги безпеки функціональні: забезпечення працездатності системи на заданому рівні у випадку виникнення вказаних збоїв [degraded fault tolerance (FRU_FLT.1)]; забезпечення нормальної роботи системи у випадку виникнення

вказаних збоїв [limited fault tolerance (FRU_FLT.2)].

Р. ФВБ: тестування апаратно-програмної платформи /р. ФТБ: тестирование аппаратно-программной платформы/ [underlying Abstract Machine Test (FPT_AMT)] — розділ ФВБ у класі ФВБ: надійність засобів захисту. Включає вимогу безпеки функціональну — перевірка коректності функціонування апаратно-програмної платформи [abstract machine testing (FPT_AMT.1)].

Р. ФВБ: фізичний захист /р. ФТБ: физическая защита/ [TSF PHysical Protection (FPT_PHP)] — розділ ФВБ у класі ФВБ: надійність засобів захисту. Включає незалежні вимоги безпеки функціональні — пасивне виявлення атак на фізичному рівні [passive detection of physical attack (FPT_PHP.1)] і активна протидія атакам на фізичному рівні [resistance to physical attack (FPT_PHP.3)], кожна з яких підсилюється вимогою — оповіщення адміністратора при виявленні атак на фізичному рівні [notification of physical attack (FPT_PHP.2)].

Р. ФВБ: цілісність внутрішньосистемного передавання інформації при використанні зовнішніх каналів /р. ФВБ: целостность внутрисистемной передачи информации при использовании внешних каналов/ [inter-TSF User data integrity Transfer protection (FDP_UIT)] — розділ ФВБ у класі ФВБ: захист інформації. Включає незалежні вимоги безпеки функціональні — виявлення порушень цілісності при передаванні інформації [data exchange integrity (FDP_UIT.1)] і відновлення інформації одержувачем [source data exchange recovery (FDP_UIT.2)], яка підсилюється вимогою — повторне передавання інформації [destination data exchange recovery (FDP_UIT.3)].

Р. ФВБ: цілісність інформації, що передається, при роботі з віддаленими клієнтами /р. ФТБ: целостность передаваемой информации при работе с удаленными клиентами/ [integrity of exported TSF data (FPT_ITI)] — розділ ФВБ у класі ФВБ: надійність засобів захисту. Включає ієрархічно залежні вимоги безпеки функціональні: виявлення спотворень інформації, яка передається між засобами захисту і віддаленими клієнтами [inter-TSF detection of modification (FPT_ITI.1)]; виявлення спотворень інформації, яка передається між засобами захисту і віддаленими клієнтами, і їхнє виправлення [inter-TSF detection and

correction of modification (FPT_ITI.2)].

Р. ФВБ: час /р. ФТБ: время/ [time STaMps (FPT_STM)] — розділ ФВБ у класі ФВБ: надійність засобів захисту. Включає вимогу безпеки функціональну — використання засобами захисту надійного таймера [reliable time stamps (FPT_STM.1)].

РОЗКРИТТЯ /вскрытие/ — виявлення, в чому-небудь того, що раніше не було відомим.

Р. інформації /р. информации/ — див. розголошення інформації.

Р. шифрувальної системи (шифру) /в. шифровальной системы (шифра/ — успішне криптоаналітичне дослідження системи шифрувальної (шифру).

РОЗМЕЖУВАННЯ /разграничение/ [differentiation] — розділення на основі проведення, визначення і встановлення межі.

Р. доступу до інформації /р. доступа к информации/ — 1) Сукупність заходів, які здійснюють розділення інформації на частини і організацію доступу до неї посадових осіб у відповідності до їхніх функціональних обов'язків і повноважень. 2) Сукупність процедур, що реалізують перевірку запитів на доступ і оцінку на підставі правил розмежування доступу можливості надання доступу.

Р. повноважень користувачів /р. полномочий пользователей/ — процедура створення в захищеній ділянці пам'яті системи обчислювальної таблиць повноважень, які містять профілі повноважень кожного користувача, термінала, процедури, процесу і т.ін. Ці профілі встановлюються за допомогою спеціальної привілейованої програми розпізнавання і контролю доступу до інформації обмеженого користування, і, як правило, задаються у вигляді матриці встановлення повноважень.

РОЗПОВСЮДЖЕННЯ /распространение/ [distribution] — розширення обсягів дії чого-небудь.

Р. ключів (обмін ключами) /р. ключей/ [key establishment, key d.] — процес або протокол, за допомогою якого секретний ключ стає доступним двом або більшому числу законних абонентів, для подальшого його використання в процесі оброблення інформації криптографічного. Існують два методи встановлення ключів — методи перенесення (або транспортування ключів) та методи формування (погодження ключів).

Кожний з цих методів може використовуватися при створенні різних схем розповсюдження ключів.

РОЗПОДІЛ /распределение/ [distribution] — дія, спрямована на ділення чогось між ким-, чим-небудь, надання кожному окремої частки.

Р. інформації і функцій її оброблення /р. информации и функций ее обработки/ — розподілення інформації і функцій її оброблення за ознаками, що забезпечують звернення до інформації і її оброблення на основі дозволених повноважень. До числа таких ознак відносяться: ступінь важливості; ступінь секретності; виконувані функції користувачем, пристроєм; види документів; види даних; найменування томів, файлів, масивів, записів; ім'я користувача; функції оброблення інформації: читання, запис, виконання; ділянок оперативної і довготривалої пам'яті; години дня. Застосовується в системі розпізнавання і обмеження доступу до інформації.

Р. ключів /р. ключей/ [key d.] — передача відповідних ключів абонентам системи оброблення секретної інформації.

Р. ключів відкритий /р. ключей открытое/ — механізм розповсюдження ключів незахищеними каналами. Базується на використання дискретного логарифмування. Див. також проблема дискретного логарифма.

РОЗСЕКРЕЧЕННЯ /рассекречивание/ [declassification] — дія, спрямована на зняття заборони на розголошення будь-чого.

Р. відомостей і їхніх носіїв /р. ведомостей и их носителей/ — зняття раніше введених у передбаченому законом порядку обмежень на розповсюдження відомостей, що складають державну таємницю, і на доступ до їхніх носіїв. Основою для розсекреченню найчастіше є: узяття на себе державою міждержавних зобов'язань із відкритого обміну відомостями, що складають у даній державі державну таємницю; зміна об'єктивних обставин, внаслідок яких подальший захист відомостей, що складають державну таємницю, є недоцільним.

РОЗСІЧЕННЯ-РОЗНЕСЕННЯ /рассечение-разнесение/ [chafing-and-winnowing] — самостійний метод

захисту інформації, який полягає в розділенні повідомлення на частини таким чином, що по частині не можна відтворити цілого повідомлення. Потім частини повідомлення передаються отримувачеві різними шляхами (у різні проміжки часу). В залежності від алгоритму розсічення повідомлення розрізняють р.-р. за змістом та механічне р.-р. Цей метод, разом із стеганографією розглядається як альтернативний методам захисту криптографічним інформації у разі введення державою обмежень на використання останніх.

РОЗШИРЕННЯ /расширение/ [extension, enhancement] — 1) Удосконалення, добавлення можливостей. 2) В теорії кодування — процес одночасного кодування групи символів або результат цього процесу.

Р. ключа /р. ключа/ [key e.] — збільшення довжини ключа.

РОЗШИФРОВУВАННЯ /расшифровывание/ [decipherement, decryption] — процес перетворення шифртексту у текст відкритий при відомому ключі; процес, зворотний процесу зашифровування (див. також дешифрування). При застосуванні багаторазового зашифровування в процесі розшифровування можна отримати і шифртекст.

С

САБОТАЖ /саботаж/ [sabotage] (франц. sabotage, від saboter — стукати черевиками) — 1) Навмисний зрив роботи роботи шляхом прямої відмови від неї або свідомо недбалого її виконання. 2) Прихована, замаскована протидія будь-яким заходам.

САЙТ /сайт/ (з англ. site — участок) — сукупність Web-сторінок, що належать приватній особі або організації, розташованих на будь-якому Web-сервері.

САМОДУБЛЮВАННЯ /самодублирование/ [self-doubling] — процес самовідтворення чого-небудь у двох екземплярах, самоповторення. Див. також дублювання.

С. програми з потенційно небезпечними наслідками /с. программы с потенциально опасными последствиями/ — процес відтворення програмою з потенційно небезпечними наслідками свого власного коду в оперативній або зовнішній пам'яті персональної ЕОМ.

САНГВІНІК /сангвиник/ [sanguine person] (від лат. sanguis [sanguinis] — кров, життєва сила) — людина із сильним рухливим, урівноваженим типом нервової системи. Див. темперамент.

СВІДОМІСТЬ /сознание/ [consciousness] — вищий рівень психічного відображення дійсності; обізнаність про події й стимули навколишнього світу та про пізнавальні явища, такі як спогади, думки і тілесні відчуття.

СВІТЛОСИЛА /светосила/ [light gathering power] — величина, яка характеризує здатність об'єктива створювати освітленість у полі зображення у відповідності до яскравості об'єкта. На с. об'єктива впливають наступні фактори: відносний отвір об'єктива; прозорість (коефіцієнти пропускання, поглинання, відбиття) лінз; коефіцієнт збільшення (масштаб зображення, що одержується); коефіцієнта зменшення освітленості до країв зображення. С. без врахування реальних утрат світла в лінзах оцінюється величиною геометричного відносного отвору $1 : k = 1 : f/D$, де D — діаметр вхідного отвору об'єктива (апертура); f — фокусна відстань об'єктива, або фокальним числом $F = f/D$. Чим більша с., тим вища чутливість засобу спостереження. Але при цьому ростуть спотворення зображення і для їхнього зменшення ускладнюють конструкцію світлосильних об'єктивів, що приводить до їхнього подорожчання. Утрати світла в об'єктиві зменшують шляхом просвітлення лінз, тобто нанесенням на поверхню скла тонкої плівки з коефіцієнтом переломлення, меншим переломлення скла лінзи.

СВОЄЧАСНІСТЬ /своевременность/ [timeliness] — термін, що означає здійснення в необхідний момент, у свій час.

С. добутої інформації /с. добытой информации/ — забезпечення подання добутої інформації керівництву у встановлені строки, протягом яких вона повністю відповідає реальній обстановці. Своєчасність є важливим показником її якості, так як вона впливає на ціну інформації. С. д. і. слід оцінювати відносно тривалості її життєвого циклу. Якщо час старіння інформації значно більший за час її використання після добування, то вона своєчасна, у протилежному випадку — вона застаріла.

СЕЙФ /сейф/ [safe] (англ. safe, букв. надійний, безпечний) — інженерна конструкція захисту об'єктів, призначена для зберігання особливо цінних документів, речей, великих сум грошей. С. являють собою дво-

стінні шафи металеві з важкими наповнювачами простору між стінками (найчастіше застосовують армовані бетонні суміші, композити, багатошарові заповнювачі з різноманітних матеріалів). Характеризуються стійкістю до зламу, стійкістю до температури, стійкістю до вологості навколишнього середовища. С. високого класу мають велику вагу, яку треба враховувати при виборі місця їхньої установки, особливо для міжповерхових перекриттів. Для утруднення виносу легких с. разом із умістом вони прикріплюються до підлоги або вбудовуються у стіну. При виборі с. слід враховувати: об'єм і тип вкладення (гроші, документи, машинні носії, матеріальні цінності); вид впливу (злам, вогонь, вода); кількість і типи замків с.; масо-габаритні характеристики, що впливають на спосіб установки с. (на підлозі без кріплення, із кріпленням до підлоги, у стіні); максимальна сума страхового покриття на випадок зламу с., яка змінюється значних межах у залежності від класу с.

СЕКРЕТ /секрет/ [secret] (франц. secret, від лат. secretum — таємниця) — 1) Таємниця (у тому числі державна); те, що старанно охороняється і приховується (інформація, винаходи, прилади і т. ін.). 2) Потайний пристрій в механізмі.

СЕКРЕТНІСТЬ /секретность/ [secrecy, confidentiality, privacy] — див. конфіденційність.

С. інформації /с. информации/ [information p.] — обмеження, що накладаються автором на доступ до його інформації інших осіб. Оформлюється присвоєнням інформації певного грифа секретності і досягається закриттям її паролем, шифруванням та іншими методами захисту інформації.

СЕЛЕКЦІЯ /селекция/ [selection] (від лат. selectio — добір) — виділення кого-, чого-небудь із загальної маси за певною ознакою; відбір.

С. інформації /с. информации/ — процес визначення належності поточної інформації до кадастру інформаційного.

СЕРВЕР /сервер/ [server] (англ. server, від serve — служити) — 1) Службовий пристрій. 2) ЕОМ, що виконує певні функції обслуговування користувачів; спеціальна віртуальна ЕОМ. В мережах обчислювальних вона управляє використанням ресурсів, що розподіляються — принтерів, пам'яті зовнішньої, баз даних.

3) Комп'ютер, що дає свої ресурси (послуги, інформацію, файли, диски, принтери і т. ін.) для спільного використання в мережі. Один комп'ютер може виконувати одночасно функції декількох серверів, наприклад, сервера Web, сервера FTP, сервера DNS і сервера проксі. Інші типи серверів: сервер файловий, сервер преси, сервер факс, поштовий сервер і т. ін.

С. DNS /с. DNS/ [DNS-s.] — сервер служби каталогів, що містить базу даних доменів.

С. FTP /с. FTP/ [FTP-s.] — сервер, що забезпечує доступ до файлів для копіювання і передачі файлів по протоколу FTP (file transfer protocol). Може містити файлові архіви від десятків мегабайт до десятків гігабайтів. Для організації FTP-сервера в найпростішому випадку необхідний персональний комп'ютер та серверне програмне забезпечення (WinNT / Win95 OSR2 / Win95-WarFTP + підключення до Internet).

С. NEWS /с. NEWS/ [NEWS-s.] — сервер, що забезпечує прийом-передачу листів у тематичні конференції, а також їхню маршрутизацію. Для організації поштового сервера необхідно установити на персональний комп'ютер відповідне програмне забезпечення (наприклад, Ndaemon).

С. Web /с. Web/ [Web-s.] — див. павутина всесвітня та сервер WWW.

С. WWW /с. WWW/ [WWW-s.] — сервер, що забезпечує доступ до сторінок Web за протоколом HTTP. Може містити від декількох до тисяч Web-сторінок, що посилаються з одного до іншого та на інші типи серверів. Сервіс WWW — найпопулярніший в Internet (80 % трафіка). До WWW-с. відносяться HTTP-сервери, WEB-сервери, WEB-сайти.

С. бази даних /с. базы данных/ [database s.] — система управління даними для великої кількості користувачів, яка централізовано здійснює пошук і оброблення даних, що запитуються прикладними програмами, які виконуються в вузлах обчислювальної мережі (на станціях робочих).

С. комунікаційний (поштовий) /с. коммуникационный (почтовый)/ [communications s. (host)] — одна з ЕОМ в мережах обчислювальних локальних, що забезпечує всім станціям робочим мережі доступ

до її ресурсів: міні- або великих ЕОМ, модемів, факс-модемів та інших пристроїв.

С. поштовий /с. почтовый/ — сервер пошти електронної Інтернету.

С. проксі з функціями кешування /с. прокси с функциями кеширования/ — сервер, що запам'ятовує відповіді з Інтернету на запити користувача, і видає інформацію, що запам'ятовується, при повторі користувачем запиту (кешування). Його використання дозволяє знизити трафік у каналі підключення до Інтернету від 2 до 10 разів. Сервер дозволяє приєднати до Інтернету персональні комп'ютери, що не мають адреси IP (наприклад, у випадку їхнього дефіциту) або взагалі IP-протоколів, а також обліку роботи в Інтернеті. За допомогою програми WinGate можна організувати комп'ютерний Інтернет-клас із використанням єдиної IP-адреси.

С. проксі прикладний /с. прокси прикладной/ [proxy application s.] — див. фільтри прикладного рівня.

С. файловий (файлова станція, файловий процесор) /с. файловый (файловая станция, файловый процессор/ [file s.] — 1) Система керування даними для великої кількості користувачів, в якій дані розташовані централізовано, в одному вузлі обчислювальної мережі, під управлінням сервера, а СКБД — в кожному вузлі (на станціях робочих). При цьому СКБД веде оброблення даних, а сервер відіграє роль драйвера диска. 2) Спеціалізований вузол обчислювальної мережі, який керує зовнішніми пристроями запам'ятовуючими великої ємності і забезпечує зберігання загальних файлів і доступ до них з інших вузлів мережі.

СЕРЕДОВИЩЕ /среда/ [environment, medium] — 1) Носій інформації (medium), тобто матеріал, на який записуються дані і на якому вони зберігаються. 2) Оточення (environment), в якому функціонує об'єкт. С. виконання програми прикладної є ЕОМ, операційна система, запам'ятовуючі пристрої, набори даних.

С. автоматизованої системи інформаційне /с. автоматизированной системы информационная/ — уся інформація, що оброблюється в автоматизованій системі. Інформація розташовується на різноманітних носіях даних і характеризується своєю належністю певному власникові, ступенем конфіденційності,

достовірності і новизни. Оцінкою і. с. є множина $I = \{i_1, i_2, .., i_n\}$, елементами якої є показники, що характеризують окремі параметри с. а. с. і. Якщо i_1 — показник, що характеризує конфіденційність інформації, тоді i_1 може приймати значення: “цілком секретна”, “секретна”, “для службового користування”, “відкрита”, “некласифікована". Решту елементів I будуть визначати інші характеристики інформації: чутливість до порушення цілісності, важливість доступності, відомча належність і т. ін.

С. автоматизованої системи робоче /с. автоматизированной системы рабочая/ — приміщення і територія, в яких розташована система автоматизована, технічне обладнання, що не зв’язане з обробленням інформації, і правила функціонування автоматизованої системи. Оцінкою даного середовища є множина $P = \{p_1, p_2, ..p_n\}$, елементами якої є показники, що характеризують окремі параметри р. с.

С. автоматизованої системи технологічне /с. автоматизированной системы технологическая/ — програмні й апаратні засоби системи автоматизованої, за допомогою яких здійснюються усі операції над інформацією в автоматизованій системі. До с. а. с. т. також відносять комплекс засобів захисту. Оцінкою с. а. с. т. є множина $T = \{t_1, t,_2 ..t_n\}$, елементами якої є показники, що характеризують його окремі параметри.

С. апаратне /с. аппаратная/ [hardware e.] — засоби технічні, що використовуються при виконанні програми.

С. гипертекстове /с. гипертекстовая/ [hypertext e.] — комплекс прийомів створення комп’ютерним шляхом багатошарових гіпертекстів, що дозволяють користувачам без утрати змісту початкового запиту встановлювати різноманітні зв’язки з додатковими даними і тим самим створювати враження розширення інформаційного простору цих даних.

С. запам’ятовуюче /с. запоминающая/ [storage m.] — див. середовище.

С. інструментальне /с. инструментальная/ [source e.] — сукупність інструментальних засобів, що охоплюють весь цикл розробки програми або системи.

С. інформаційне /с. информационная/ [information e.] — сфера діяльності суб’єктів, зв’язана із ство-

ренням, перетворенням і споживанням інформації.

С. комунікаційне /с. коммуникационная/ [communication e.] — сукупність технічних і програмних засобів системи передавання даних.

С. користувачів автоматизованої системи /с. пользователей автоматизированной системы/ — сукупність користувачів, які можуть одержати доступ до середовища автоматизованої системи інформаційного. Множина $K = \{k_1, k_2, .., k_n\}$, елементами якої є показники, що характеризують користувачів, вважається оцінкою к. с. Користувачів автоматизованої системи можна характеризувати за службовим станом (керівник, користувач, допоміжний персонал, користувач, що не входить до штату автоматизованої системи), допуском до інформації, рівнем компетентності і т. ін.

С. обчислювальне (операційне, системне) /с. вычислительная (операционная, системная)/ [compute (operational) e.] — засоби апаратні, забезпечення програмне і набори даних (файлів).

С. операційне /с. операционная/ [operational e.] — середовище, яке створюється засобами системи операційної.

С. програмне /с. программная/ [software e.] — програмні засоби, з якими взаємодіє програма або система.

С. розповсюдження носія інформації /с. распространения носителя информации/ — частина простору, в якій передається носій інформації. Характеризується набором параметрів, що визначають умови переміщення носія. Основними параметрами, які необхідно враховувати для опису середовища розповсюдження, є: фізичні перепони для суб'єктів і матеріальних тіл; міра ослаблення (або пропускання) сигналу на одиницю довжини; частотна характеристика (нерівномірність ослаблення частотних складових спектра сигналу); вид і потужність завад для сигналу.

С. фізичне /с. физическая/ [physical m.] — див. середовище.

СЕРТИФІКАТ /сертификат/ [certificate] (франц. certificat, від лат. certus — вірний і fasio — роблю) — 1) Документ, який підтверджує, що належним чином ідентифіковані продукт або послуга відповідають

вимогам нормативних документів. 2) Електронний документ, який зв'язує ідентифікатор власника сертифіката з його ключами відкритими. Звичайно, цей зв'язок реалізується за допомогою механізму підпису цифрового, а у с. містяться і самі значення відкритих ключів. 3) В законодавстві про цифровий підпис — електронне посвідчення, яке зв'язує дані, необхідні для верифікації підпису з особою та підтверджує ідентичність цієї особи.

С. відкритого ключа /с. открытого ключа/ [public key c.] — див. сертифікат.

С. відповідності /с. соответствия/ [c. of conformity] — документ, виданий згідно з правилами системи сертифікації, який указує, що забезпечується необхідна впевненість у тому, що потрібним чином ідентифікована продукція, процес чи послуга відповідають конкретному стандартові чи іншому нормативному документові.

С. захисту /с. защиты/ [protection c.] — документ, що засвідчує відповідність засобів обчислювальної техніки або автоматизованої системи набору вимог по захисту від несанкціонованого доступу до інформації і дає право розробникові використовувати або розповсюджувати їх як захищених.

С. користувача /с. пользователя/ [user c.] — див. сертифікат.

С. об'єкта (суб'єкта) доступу /с. объекта (субъекта) доступа/ — загальнодоступна ключова та службова інформація, що використовується в процесі автентифікації.

СЕРТИФІКАЦІЯ /сертификация/ [certification] — 1) Діяльність, спрямована на підтвердження відповідності продукції встановленим вимогам. 2) В галузі безпеки інформації — офіційна атестація, що включає процедуру всебічної оцінки системи обробки даних, після завершення якої третя сторона, уповноважена на це органом сертифікації, дає гарантії, що частина або система оброблення даних в цілому задовольняє певним вимогам по безпеці інформації, що обробляється нею.

С. добровільна /с. добровольная/ — сертифікація на відповідність вимогам, не віднесеним нормативними документами до обов'язкових, яка проводиться на добровільних засадах за ініціативою виробника,

постачальника чи споживача продукції.

С. засобів захисту інформації /с. средств защиты информации/ [security s.] — процес встановлення відповідності засобів захисту інформації до вимог захисту відомостей відповідного ступеня секретності.

С. обов'язкова /с. обязательная/ — сертифікація на відповідність вимогам, які віднесені нормативними документами до обов'язкових для виконання.

С. рівня захисту /с. уровня защиты/ [protection level s.] — процес установлення відповідності засобу обчислювальної техніки або автоматизованої системи набору певних вимог по захисту.

СИГНАЛ /сигнал/ [signal] (франц. signal, нім. Signal, від лат. sidnum — знак) — 1) Фізична величина, зміна якої відображає повідомлення. 2) В безпеці інформаційній — розповсюджуваний у просторі носій з інформацією, яка міститься у значеннях його фізичних параметрів. За формою с. можуть бути аналоговими або дискретними. За фізичною природою с. можуть бути акустичними, електричними, магнітними, електромагнітними (в радіодіапазоні — радіосигнали), корпускулярними і матеріально-речовими. С. за видом інформації, що передається, поділяються на мовні, телеграфні, телекодові, факсимільні, телевізійні, про радіоактивне випромінювання і умовні. За часом прояву с. можуть бути регулярними та випадковими.

С. адитивний /с. аддитивный/ [additivity s.] (від лат. additivus — придатковий, пов'язаний з додаванням) — сигнал, миттєві значення якого є сумою миттєвих значень двох або більше сигналів, взятих в один і той же момент часу. Якщо один з сигналів, що створює с. а., вважається корисним, а інші заважаючими, то заважаючі сигнали іноді називають завадою або шумом.

С. акустичний /с. акустический/ [acoustic s.] — сигнал, носієм інформації якого є хвилі акустичні.

С. аналоговий (безперервний) /с. аналоговый (непрерывный)/ [analog (continuous) s.] — сигнал, що характеризується нескінченною множиною значень змінної величини і за скінченний період часу може створювати нескінченну множину повідомлень. До с. а. відносяться сигнали, рівень (амплітуда) яких може приймати довільні значення в певному для сигналу інтервалі. С. а. описуються певним набором параметрів, які є його ознаками. До них відносяться: частота або діапазон частот; фаза сигналу; тривалість сигналу;

амплітуда або потужність сигналу; ширина спектра сигналу; діапазон динамічний сигналу.

С. випадковий /с. случайный/ [random s.] — сигнал, час прояву якого заздалегідь не відомий. Статистичні характеристики прояву с. в. у часі можуть являти собою достатні ознаки демаскуючі джерела (об'єкта), насамперед, його належність і режими функціонування. С. в., будь-яка характеристика якого, одержана усереднюванням по множині можливих реалізацій з імовірністю, близькою до одиниці, дорівнює часовому середньому, одержаному усереднюванням за достатньо великий проміжок часу однієї реалізації, називається ергодичним.

С. випадковий нестаціонарний /с. случайный нестационарный/ [nonstationary random s.] — сигнал випадковий, у якого густина ймовірності деякої сукупності миттєвих значень змінюється при деякому зсуві цієї сукупності в часі.

С. випадковий стаціонарний /с. случайный стационарный/ [stationary random s.] — сигнал випадковий, у якого густина ймовірності будь-якої сукупності миттєвих значень не змінюється при будь-якому зсуві цієї сукупності в часі. Випадковий сигнал, у якого середнє значення і дисперсія не залежать від часу, а кореляційна функція залежить тільки від часу запізнення, називається стаціонарним в широкому розумінні.

С. гідроакустичний /с. гидроакустический/ [hydroacoustoc s.] — пружні хвилі акустичні у водному середовищі від джерела збудження.

С. груповий /с. групповой/ [baseband s.] — в багатоканальних системах зв'язку — сигнал, в який об'єднуються індивідуальні сигнали окремих каналів (канальні сигнали).

С. демаскуючий /с. демаскирующий/ — сигнал, факт виявлення якого може служити інформативною ознакою об'єкта, що потребує захисту.

С. детермінований /с. детерминированный/ [deterministic s.] — сигнал, миттєві значення якого в будь-який момент часу відомі. Загальні характеристики с. д. можуть бути знайдені розрахунковим способом.

С. дискретний /с. дискретный/ [discrete s.] — сигнал, що характеризується скінченною множиною

значень змінної величини і за скінченний період часу може створювати скінченну множину повідомлень. С. д. створюється безперервним квантуванням у часі, за рівнем (амплітудою) або одночасно в часі і за рівнем. С. д. описуються певним набором параметрів, які є його ознаками. Наприклад, дискретний періодичний сигнал характеризується наступними ознаками: амплітудою і потужністю, тривалістю імпульсу, періодом, або частотою повторення імпульсів, шириною спектра сигналу, відношенням періоду повторення імпульсів до їхньої тривалості.

С. електричний /с. электрический/ [electrical s.] — величина струму, напруги, напруженості електромагнітного поля, зміна якої відображає повідомлення.

С. електрозв'язку /с. электросвязи/ — сигнали електричні, що використовуються в системах електрозв'язку. Поділяються на телефонні, телеграфні, телевізійні, передавання даних і т. ін.

С. імпульсний /с. импульсный/ [(im)pulse s.] — сигнал детермінований скінченної енергії, суттєво відмінний від нуля протягом обмеженого інтервалу часу, сумірний з часом установлення перехідного процесу в системі, для впливу на яку цей сигнал призначений. Сигнал, що являє собою послідовність скінченного відомого числа імпульсів однакової форми, які слідують один за одним через однакові інтервали часу, називають пачкою імпульсів. Сигнал, що складається з імпульсів, число, форма і значення параметрів яких відомі, називається кодовою групою імпульсів.

С. корпускулярний /с. корпускулярный/ [corpuscular s.] — сигнал у вигляді потоку елементарних часток.

С. матеріально-речовинний /с. материально-вещественный/ — матеріал або речовина, що несуть певне повідомлення. Наприклад, пахуча добавка до газу подає повідомлення про його витік.

С. мовний (телефонний) /с. речевой (телефонный)/ [speech (voice) s.] — електричний сигнал, що відображає мову природну. Так як мова є нестаціонарним випадковим процесом, то і с. м., який формується електроакустичними перетворювачами (мікрофонами), являє собою реалізацію цього нестаціонарного процесу. Статистичні характеристики цього сигналу одержують усередненням результатів вимірювань як

в часі, так і по множині. Особливістю с. м. є те, що вони поступають в канал зв'язку не безперервно — окремі слова і фрази розділяються паузами різноманітної тривалості. Мова являє собою широкосмуговий процес, частотний спектр якого простягається від 50–100 до 8000–10000 Гц. Проте якість мови задовільна при обмеженні спектра частотами 300 і 3400 Гц.

С. модульований /с. модулированный/ [modulated s.] — сигнал, який є результатом взаємодії двох або більше сигналів, що називається модуляцією. Модуляція — процес отримання сигналу, математичний опис якого може бути одержаний заміною параметра в математичному описі модульованого сигналу на функцію від модулюючого сигналу. В більшості випадків ця функція (закон модуляції) є лінійною. При цьому закон модуляції характеризується такими ж параметрами і функціоналами, як і модулюючий сигнал. Як сигнал, що модулюється, використовується гармонічний сигнал або періодична послідовність прямокутних імпульсів. Якщо сигнал, що модулюється, є гармонічним, в залежності від параметра, що піддається впливу з боку модулюючого сигналу (амплітуди, частоти, початкової фази) розрізняють відповідно амплітудну (АМ), частотну (ЧМ) і фазову (ФМ) модуляції. Відповідні с. м. називаються амплітудно-модульованим (АМ-сигнал), частотно-модульованим (ЧМ-сигнал) і фазо-модульованим (ФМ-сигнал). Часто частотна і фазова модуляція іменуються загальним терміном модуляція кутова. Якщо сигнал, що модулюється, є періодичною послідовністю прямокутних імпульсів, в залежності від параметра, що піддається впливу з боку модулюючого сигналу (амплітуди, тривалості, положення імпульсу на інтервалі, частоти надходження імпульсів, періоду імпульсів) розрізняють відповідно модуляцію амплітудно-імпульсну (АІМ), модуляцію широтно-імпульсну (ШІМ), часову або модуляцію фазово-імпульсну (ФІМ), модуляцію частотно-імпульсну (ЧІМ) та періодно-імпульсну модуляцію (ПІМ). Відповідно розрізняють сигнал з АІМ, сигнал з ШІМ, сигнал з ФІМ, сигнал з ЧІМ і сигнал з ПІМ.

С. модулюючий /с. модулирующий/ [modulating s.] — сигнал, який викликає зміни певного параметра або параметрів несучої або піднесучої при модуляції.

С. мультиплікативний /с. мультипликативный/ [multiplicative s.] (від лат. multiplico — помножую)

— сигнал, миттєві значення якого пропорційні добутку миттєвих значень двох або більше сигналів, взятих в один і той же момент часу.

С. оптичний /с. оптический/ [optical s.] — величина електромагнітних коливань оптичного діапазону хвиль, зміна якої відображає повідомлення.

С. передавання даних /с. передачи данных/ — сигнал електричний у вигляді двополярних або однополярних прямокутних імпульсів.

С. періодичний /с. периодический/ [periodic s.] — сигнал детермінований, миттєві значення якого повторюються через рівні проміжки часу.

С. радіочастотний /с. радиочастотный/ [radio-frequency signal] — те ж, що радіосигнал.

С. регулярний /с. регулярный/ [regular s.] — сигнал, час прояву якого заздалегідь відомий одержувачу інформації.

С. скрембльований /с. скремблированный/ [scrambled s.] — сигнал, одержаний внаслідок застосування операції скреблювання. Властивості с. с. тим кращі, чим ближче параметри перетворюваного скремблером сигналу до параметрів випадкового двійкового сигналу.

С. телевізійний /с. телевизионный/ [television s.] — складний сигнал електричний, що включає в себе сигнал зображення і керуючі імпульси. Сигнал зображення формується методом розгортки з формуванням сигналів ліній, що об'єднуються в кадри (півкадри). Керуючі імпульси (гасячі і синхронізуючі) служать для погашення променя приймальної телевізійної трубки та синхронізації променів передавальної і приймальної трубок.

С. телеграфний /с. телеграфный/ [telegraph s.] — сигнал електричний у вигляді двополярних або однополярних прямокутних імпульсів, який використовується для передавання букво-цифрової інформації з низькою швидкістю.

С. телекодовий /с. телекодовый/ — сигнал електричний у вигляді імпульсів, який використовується

для передавання букво-цифрової інформації з великою швидкістю.

С. телефонний /с. телефонный/ [telephone s.] — див. сигнал мовний.

С. умовний /с. условный/ [prearranger s.] — сигнал, що несе інформацію, зміст якої заздалегідь визначений між її джерелом і одержувачем. Найчастіше с. у. здійснюється передаванням коротких повідомлень. С. у. можуть бути будь-які об'єкти спостереження і джерела випромінювання.

С. факсимільний /с. факсимильный/ [facsimile s.] — сигнал електричний, одержаний шляхом електрооптичного аналізу, що полягає в перетворенні світлового потоку, відбитого елементарними ділянками зображення. Ці ділянки створюються фокусуванням невеликої світлової плями, яка переміщується по поверхні зображення. У приймачі одержаний електричний сигнал збуджує будь-який фізичний вплив, що забарвлює елементарні ділянки носія запису, в результаті чого одержують копію зображення, що передається. Використовується для передавання нерухомих зображень.

С. цифровий /с. цифровой/ [digital s.] — сигнал, дискретизований у часі та квантований за рівнем, причому кожний з рівнів подається числом, як правило, двійковим. Цифровий сигнал описується квантованою решітчастою функцією.

СИГНАЛІЗАТОР /сигнализатор/ [event alerts (signaling device/indicator)] — технічний пристрій, який формує електричний сигнал тривоги при дії на нього або на створювані ним поля зовнішніх сил або об'єктів. С. бувають охоронні, охоронно-пожежні або пожежні. Різноманітність видів зон, що охороняються, і їхніх характеристик викликало появу різноманітних видів і типів с. За призначенням с. поділяються на засоби для блокування окремих предметів, виявлення зловмисника і пожежі в закритих приміщеннях, виявлення порушника на відкритих площадках і блокування периметрів території, будівлі, коридору. За видом зони, що охороняється с. поділяються на точкові, лінійні, поверхневі, об'ємні. За принципом виявлення зловмисника і пожежі с. поділяються на: контактні; акустичні; оптико-електронні; мікрохвильові (радіохвильові); вібраційні; ємнісні; теплові (пожежні); іонізаційні (пожежні); комбіновані.

С. акустичні /с. акустические/ — сигналізатори, що використовують для виявлення зловмисників

акустичні хвилі у звуковому і ультразвуковому діапазонах, які виникають при руйнуванні ним механічних перепон або відбиваються від порушника при проникненні його в приміщення, що охороняється. С. а. поділяються на активні і пасивні.

С. акустичні активні /с. акустические активные/ — сигналізатори акустичні, що випромінюють акустичні хвилі в ультразвуковому діапазоні. С. а. а. складається з електроакустичного випромінювача, приймача (акустоелектричного перетворювача і електронного блока). Випромінювач посилає в приміщення, що охороняється, акустичну хвилю з частотою вище 23 кГц. В результаті інтерференції прямих і відбитих хвиль у приміщенні виникають "стоячі хвилі". З появою у приміщенні людини, а також відкритого полум'я пожежі, характер "стоячих хвиль", а також відповідно і рівень акустичного сигналу на вході приймача змінюються, що приводить до появи сигналу тривоги на виході електронного блока. Пониження впливу завад досягається регулюванням чутливості приймача. З метою подальшого пониження впливу акустичних завад в сучасних с. а. а. передбачена селекція акустичного сигналу за величиною зміни його частоти внаслідок ефекту Допплера.

С. акустичні пасивні /акустические пассивные с./ — сигналізатори акустичні, що реагують на акустичні сигнали, які утворюються при руйнуванні зловмисником поверхні, що блокується. С. а. п. застосовуються для захисту будівельних конструкцій (вікон, вітрин, стін, стель, підлог, сейфів та ін.). У сигналізаторі акустичний сигнал перетворюється в електричний, при відповідності поточних параметрів якого еталонним формується сигнал тривоги. Для перетворення акустичних сигналів застосовують п'єзоелектричні і електромагнітні датчики. З метою зменшення ймовірності фальшивих тривог від акустичних завад збільшується кількість використовуваних для ідентифікації демаскуючих ознак і ускладнюються алгоритми їхнього оброблення.

С. вібраційні /с. вибрационные/ — сигналізатори, що виявляють зловмисника за створюваними ним вібраціями в ґрунті при пересуванні, в легкій огорожі при спробі подолання її порушником, при відкриванні дверей, вікон, люків і інших конструкцій. На відміну від акустичних сигналізаторів с. в. сприймають коли-

вання поверхні в інфразвуковому діапазоні. В залежності від фізичної природи перетворення механічного тиску в електричний сигнал с. в. бувають електретні, магнітні, волоконно-оптичні, трибоелектричні. Якщо датчики сигналізатора розташовуються в ґрунті, то в. с. називаються також сейсмічними.

С. електроконтактні /с. электроконтактные/ — сигналізатори контактні у вигляді кнопкових вимикачів, які замикають або розмикають електричні кола, що з'єднують сигналізатори з приймально-контрольним приладом, внаслідок дії зловмисника, наприклад, при відкриванні ними дверей, віконних рам, шафи і т.ін. До с. е. відносяться також датчики, виконані у вигляді контактних килимків, що розташовуються на можливому шляху пересування зловмисника, наприклад, перед дверима.

С. ємнісні /с. емкостные/ — сигналізатори, що утворюють сигнали тривоги при наближенні зловмисника до антени. Антеною може бути сам об'єкт охорони (наприклад, сейф) або електричний дріт, що закріплюється у віконних або дверних проймах, шафах, на стінах складів і т. ін. Принцип роботи с. є. заснований на зміні еквівалентної ємності в контурі генератора сигналів сигналізатора, що викликається збільшенням розподіленої ємності порушником, що наближається, і антеною. Зміна ємності приводить до зміни частоти сигналу генератора і зменшення його амплітуди, при пониження якої нижче заданого порога подається сигнал тривоги. Чутливість с. є. оцінюється максимальною відстанню наближення до антени, яка складає 10–30 см.

С. іонізаційні /с. ионизационные/ — сигналізатори для виявлення пожежі. С. і. реагують на дим пожежі, що погіршує прозорість середовища між розташованими в одному корпусі джерелом радіоактивного випромінювання і детектором.

С. комбіновані /с. комбинированные/ — сукупність сигналізаторів з різноманітними принципами виявлення зловмисника або пожежі. В результаті оброблення сигналів від різних датчиків на основі спеціальних алгоритмів підвищується ймовірність виявлення зловмисника або пожежі при забезпеченні малих значень ймовірності фальшивої тривоги.

С. контактні /с. контактные/ — сигналізатори, які реагують на дії зловмисника, що призводять до

замикання або розмикання контактів с., а також до обриву тонкого проводу або смужки фольги. Вони бувають електроконтактними, магнітоконтактними, удароконтактними і обривними.

С. лінійні /с. линейные/ — сигналізатори, призначені для охорони периметрів об'єктів.

С. магнітоконтактні /с. магнитоконтактные/ — сигналізатори контактні, що складаються з геркона (герметичної скляної трубки з контактами, що управляються за допомогою магніту) і постійного магніту, розташованих в однакових пластмасових корпусах прямокутної або циліндричної форми. С. м. призначені для блокування поверхонь, що відкриваються (дверей, вікон, люків і т. ін.), а також предметів, які можна переносити (експонатів музеїв, виставок). Магніт закріплюється на рухомій частині поверхні, що блокується або на експонаті, а геркон — на нерухомій частині або на підставці експоната паралельно магніту на відстані не більш 6–8 мм.

С. мікрохвильові (радіохвильові) /с. микроволновые (радиоволновые)/ — сигналізатори, що використовують для виявлення зловмисника електромагнітні хвилі в діапазоні надвисоких частот (9–11 ГГц). Вони містять НВЧ генератор, приймач і антени. Так як на електромагнітне поле в НВЧ діапазоні не впливають акустичні завади, світло і в значно меншій мірі атмосферні осадки, то ці с. все більш широко застосовуються для охорони приміщень, відкритих просторів і периметрів. До складу с. м. відносяться також радіопроменеві і радіотехнічні сигналізатори.

С. мікрохвильові об'ємні /микроволновые объемные с./ — сигналізатори мікрохвильові, що створюють об'ємну зону виявлення, яка заповнює електромагнітним полем весь об'єм приміщення. Для пониження потужності випромінювання, що важливо для безпеки обслуговуючого персоналу і підвищення завадостійкості, в сигналізаторах передбачається імпульсний режим роботи. Для зменшення фальшивих тривог в схемі м. с. о. реалізується принцип селекції на основі ефекту Допплера.

С. об'ємні /с. объемные/ — сигналізатори, призначені для охорони об'ємів приміщень або відкритих площадок.

С. обривні /с. обрывные/ — сигналізатори контактні, основу яких складають тонкий дріт, алюмінієва

фольга і струмопровідні шари скла або плівки, при обриванні яких порушується зв'язок між сигналізатором і приладом приймально-контрольним. С. о. мають високу завадостійкість і широко застосовуються для блокування поверхонь і периметрів.

С. оптико-електронні /с. оптико-электронные/ — сигналізатори, призначені для виявлення зловмисника або пожежі за допомогою інфрачервоних променів. За принципом дії поділяються на активні і пасивні.

С. оптико-електронні активні /оптико-электронные активные с./ — сигналізатори оптико-електронні, що складаються з однієї або декількох пар випромінювача інфрачервоних променів і фотоприймача. Випромінювач такого сигналізатора створює вузький промінь електромагнітного випромінювання у інфрачервоному діапазоні, який у черговому режимі попадає на фотоприймач. При перетинанні променя зловмисником або при появі на шляху його розповсюдження диму рівень сигналу на виході фотоприймача різко зменшується, що приводить до формування сигналу тривоги.

С. оптико-електронні пасивні /с. оптико-электронные пассивные/ — сигналізатори оптико-електронні, що формують сигнал тривоги при попаданні на вхід термочутливого елемента інфрачервоного випромінювання від зловмисника або від осередку пожежі.

С. поверхневі /с. поверхностные/ — сигналізатори, призначені для охорони поверхонь (стін, стель, вікон, вітрин і т. ін.).

С. радіопроменеві /с. радиолучевые/ — сигналізатори мікрохвильові, антени випромінювачів яких формують вузьку діаграму спрямованості у вигляді витягнутого еліпсоїда з висотою і шириною в зоні виявлення 2–10 м. Довжина однієї ділянки виявлення сягає 300 м. При перетинанні людиною електромагнітного променя, що випромінюється передавачем в сторону приймача, із-за екрануючих властивостей людини зменшується напруженість поля в точці прийому, в результаті чого подається сигнал тривоги.

С. радіотехнічні /радиотехнические с./ — сигналізатори мікрохвильові, що виявляють зловмисника за змінами ним характеристик надвисокочастотного електромагнітного поля. Електромагнітне поле ство-

рюється одним або декількома передавачами. Передавальною антеною може слугувати спеціальний радіочастотний кабель, що прокладається вздовж периметра території, що охороняється. Антена приймача розташовується у центрі території або у вигляді кабелю, паралельного передавальному. При вторгненні зловмисника в зону чутливості сигналізатора характеристики сигналу на вході приймача змінюються, що викликає сигнал тривоги.

С. сейсмічні /с. сейсмические/ — див. сигналізатори вібраційні.

С. теплові /с. тепловые/ — сигналізатори для виявлення пожежі. Чутливими до температури елементами в таких сигналізаторах служать: терморезистори, що змінюють свій опір від температури; термобіметалеві пластини з різними коефіцієнтами теплового розширення; легкоплавкі сплави (Вуда з температурою плавлення 60,5°С, д'Арсе — 79°С), що замикають при нормальній температурі контакти сигналізатора; термоферіти з магнітною проникливістю, що зменшується при підвищення температури, які використовуються як сердечники електромагнітних реле, що замикають контакти при пониженні магнітного поля менше рівня спрацьовування реле. С. т. мають високу завадостійкість та значну інерційність, зумовлену часом нагрівання чутливого елемента до температури спрацьовування с. т.

С. точкові /с. точечные/ — сигналізатори, призначені для охорони окремих об'єктів.

С. удароконтактні /с. ударноконтактные/ — сигналізатори контактні, принцип дії яких заснований на розмиканні нормально замкнутих контактів внаслідок дії сили інерції під час коливань корпусу датчика, приклеєного до скла. У. с. забезпечують блокування поверхонь, насамперед, віконного скла, що руйнуються від ударів.

С. ультразвукові /с. ультразвуковые/ — див. сигналізатори акустичні активні.

СИГНАЛІЗАЦІЯ /сигнализация/[signal(l)ing] — подавання сигналу попередження про будь-що, наприклад, застереження про небезпеку.

С. тривожна /с. тревожная/ [alarm s.] — сигналізація, призначена для психологічного впливу на порушника, який скрито проникає в зони, що охороняються, з метою примусити його відмовитися від наміру.

Засобами сигналізації служать, найчастіше разом, звукові і світлові сповіщувачі. В системі охорони об'єктів вони повинні мати відповідну потужність випромінювання звуку і світла, яка не тільки інформує зловмисника про те, що він виявлений, але і викликає у нього почуття страху. Найбільш сильний психологічний вплив в тихий нічний час здійснює звук сирени на межі больового відчуття (біля 120 дБ) і яскраве миготливе світло.

СИМВОЛ /символ/ [character, symbol] (від грец. *σύμβøλøν* — знак, прикмета, ознака) — 1) Умовне позначення будь-якого предмета, поняття або явища. С. бувають речові, графічні. 2) Знак, одиниця алфавіту. 3) Послідовність з одного або декількох знаків, що використовуються для позначення чого-небудь.

СИНЕРГЕТИКА /синергетика/ [synergetic] — галузь наукових досліджень, метою яких є виявлення загальних закономірностей в процесах утворення, стійкості й руйнування впорядкованих часових і просторових структур у складних системах різноманітної природи.

СИНЕРГИЗМ /синергизм/ [synergism] — взаємне підсилення впливу різних засобів інформації на масову аудиторію, об'єднану загальними іміджами, сюжетами, формами відображення реальних фактів, їхніх трактувань і оцінок.

СИСТЕМА /система/ [system] (від грец. *σύστημα* — утворення, складення) — сукупність об'єктів і відносин між ними, що створюють єдине ціле. Система задається (описується) наступними параметрами (характеристиками): метою і задачами (конкретизованою в просторі і часі метою); входами і виходами системи; обмеженнями, які необхідно враховувати при побудові (модернізації, оптимізації) системи; процесами всередині системи, які забезпечують перетворення входів у виходи.

С. автоматизована (АС) /с. автоматизированная (АС)/ [automated s.] — 1) Комплекс програмних і технічних засобів, призначених для автоматизації різноманітних процесів, зв'язаних з діяльністю людини. При цьому людина є ланкою цієї системи (на відміну від автоматичної системи, що функціонує без участі людини). 2) Організаційно-технічна система, що реалізує технологію інформаційну і об'єднує систему обчислювальну (див. середовище автоматизованої системи технологічне), середовище автоматизованої системи

робоче, персонал (див. середовище користувачів автоматизованої системи) і інформацію, яка оброблюється (див. середовище автоматизованої системи інформаційне). Сукупність заходів, що забезпечують захист інформації в автоматизованій системі утворюють комплексну систему захисту інформації. Частина проблем забезпечення захисту інформації в АС може бути вирішена заходами захисту інформації організаційними. Інші проблеми потребують застосування технічних засобів і заходів захисту В АС розрізняють два основних напрямки захисту інформації технічного — захист АС і інформації, що оброблюється, від несанкціонованого доступу і захист інформації від витоку каналами технічними. Реальна оцінка захищеності автоматизованої системи може бути одержана в результаті перевірки усіх чотирьох середовищ АС. Вважається, що захищеною є АС, в якій існує відповідність між даними середовищами, тобто безпека середовища користувачів, технологічного й робочого середовища відповідає чутливості інформаційного.

С. автоматична /с. автоматическая/ [automatic s.] — система, що функціонує самостійно, без участі людини (на відміну від системи автоматизованої).

С. безпеки /с. безопасности/ [security s.] — сукупність органів законодавчої, виконавчої і судової влади, державних, суспільних та інших організацій і об'єднань, громадян, що приймають участь в забезпеченні безпеки у відповідності до закону, а також законодавство, що регламентує відносини у сфері безпеки. Основними функціями с. б. можуть бути: виявлення і прогнозування внутрішніх і зовнішніх загроз життєво важливим інтересам об'єктів безпеки, здійснення комплексу оперативних і довготривалих заходів з їхнього попередження і нейтралізації; створення і підтримування в готовності сил і засобів забезпечення безпеки; управління силами і засобами забезпечення безпеки в повсякденних умовах і при надзвичайних ситуаціях; здійснення системи заходів з відновлення нормального функціонування об'єктів безпеки в регіонах, що постраждали в результаті виникнення надзвичайної ситуації; участь в заходах забезпечення безпеки за межами держави у відповідності до міжнародних договорів і угод, укладених або визнаних державою.

С. відеоконтролю /с. видеоконтроля/ — система замкнутого телебачення, створена на основі засобів спостереження телевізійних. Складає основу підсистеми спостереження системи охорони об'єктів. В най-

більш загальному випадку має у своєму складі наступні засоби телевізійної техніки: передавальні камери телевізійні; пристрої відображення інформації — монітори; пристрої оброблення відеоінформації (комутатори, квадратори, мильтиплексори); пристрої реєстрації (побутові і спеціальні відеомагнітофони); кабелі, що забезпечують електричні зв'язки елементів системи.

С. відкрита /с. открытая/ [open s.] — 1) Система, яка взаємодіє з навколишнім середовищем — людиною, джерелами інформації, іншими системами. 2) Система, здатна розширюватися за рахунок засобів середовища, в якому вона функціонує.

С. гасіння пожежі автоматична /с. тушения пожара автоматическая/ — сукупність засобів, що забезпечують гасіння пожежі шляхом заповнення приміщення з осередком загоряння газом за сигналом "Пожежа" від сигналізаторів, встановлених в цьому приміщенні. Типовий комплекс засобів с. г. п. а. включає: модуль газового гасіння пожежі з балонами газу об'ємом 40–100 л, засувно-пусковим пристроєм, манометром та піропатроном, розташованим в спеціальному приміщенні (станції газового гасіння пожежі); пожежо-охоронні і пожежні сигналізатори; прилад приймально-контрольний (пункт), до вхідних клем якого приєднуються шлейфи від сигналізаторів, а з вихідних клем знімаються сигнали керування підривом піропатрона, від'єднання вентиляції, включення табло оповіщення співробітників про подачу газу; газопроводи (труби) від газової станції до приміщень і газові розпилювачі в приміщеннях; кнопки ручного пуску та блокування газу. Через приймально-контрольний пункт комплекс газового гасіння пожежі приєднується до приймально-контрольного пункту автономної системи охорони і пункту спостереження централізованої системи. Найбільш безпечним і ефективним газом для гасіння пожежі є перфторбутан. Він не руйнує озоновий шар, не є токсичним, не залишає слідів після застосування.

С. експертні (ЕС) /с. экспертные (ЕС)/ [expert s.] — клас систем інформаційних автоматизованих, що мають бази даних і бази знань, здатні здійснювати аналіз і корекцію даних незалежно від санкцій користувача, аналізувати і приймати рішення як на основі запиту, так і незалежно від запиту користувача і виконувати ряд аналітично-класифікаційних задач. Можна виділити ЕС діагностики, планування та про-

гнозування. ЕС діагностики призначені для знаходження причин аномальності явищ, що спостерігаються. Основою для аналізу служать набори даних, за допомогою яких виявляються відхилення від еталонної поведінки і в результаті чого ставиться діагноз. ЕС планування призначені для вироблення програми дій, необхідних для досягнення певних цілей. ЕС прогнозування призначені для побудови сценарію майбутнього. Засновуючись на подіях минулого і сучасного, вони здатні виводити ймовірні наслідки із заданих ситуацій. Для цього в прогнозуючих ЕС використовуються динамічні параметричні моделі.

С. електрозв'язку /с. электросвязи/ [electric communication s.] — комплекс технічних засобів, що забезпечують передавання сигналів електрозв'язку. В основі с. е. лежить первинна мережа, яка включає в себе середовище розповсюдження і апаратуру передавання сигналу, що забезпечує створення типових каналів і трактів первинної мережі, які використовуються для передавання інформації. В сучасних с. е. таких середовищ три: електричний кабель, волоконно-оптичний кабель і радіоефір або радіочастотний ресурс. Типові канали і тракти первинної мережі використовуються різноманітними вторинними мережами: цифрової телефонії, цифровими з інтеграцією служб, на основі принципу асинхронного режиму передавання, передавання даних і т. ін., стільникового і транкового радіозв'язку, а також мережами спеціального призначення: мережами диспетчерського зв'язку, оперативного і технологічного управління, селекторних нарад і т.ін. Засоби с. е. утворюють найбільш численну і різноманітну групу джерел сигналів з семантичною інформацією. Перехоплення сигналів с. е. є одним з найбільш ефективних і широко розповсюджених методів добування інформації. Проте сигнали с. е. містять не тільки інформацію семантичну, але і інформацію про ознаки сигналів (див. інформація ознакова). Така інформація характеризує технічні рішення нових засобів і їхні можливості.

С. забезпечення безпеки даних /с. обеспечения безопасности данных/ — сукупність засобів і механізмів захисту даних.

С. замків і ключів /с. замков и ключей/ [locks and keys] — система захисту пам'яті, в якій сегментам пам'яті операційною системою присвоєні ідентифікаційні номери — замки, а зареєстрованим користува-

чам — числові коди — ключі. Ця дія здійснюється привілейованим процесом в деякій області пам'яті, що недоступна користувачеві.

С. захисту абсолютна /с. защиты абсолютная/ — система, яка має всі можливі способи захисту і здатна в будь-який момент свого існування спрогнозувати настання загрозливих подій за час, достатній для приведення в дію адекватних способів захисту.

С. захисту даних /с. защиты данных/ [security s. (s. of protection)] — комплекс апаратних, програмних та криптографічних засобів, а також заходів, що забезпечують захист даних від несанкціонованого доступу.

С. захисту державної таємниці /с. защиты государственной тайны/ — сукупність органів захисту таємниці державної, засобів і методів захисту відомостей, що складають державну таємницю, і їхніх носіїв, а також заходи, що проводяться з цією метою,

С. захисту з повним перекриттям /с. защиты с полным перекрытием/ — система, в якій є засоби захисту на кожний потенційно можливий шлях проникнення до закритих даних.

С. захисту інформації (СЗІ) /с. защиты информации (СЗИ)/ [information protection (protective) s., information safety s.] — сукупність взаємозв'язаних елементів, функціонування яких спрямоване на забезпечення безпеки інформації. Такими елементами є люди (керівництво і співробітники організації, насамперед, служби безпеки інформації), інженерні конструкції та технічні засоби, що забезпечують захист інформації. Метою створення системи є забезпечення необхідних рівнів безпеки інформації на об'єкті захисту. Завдання СЗІ конкретизуються стосовно до видів і категорій інформації, що підлягає захисту, а також елементів об'єкта захисту. Входами системи є дії з реалізації загроз, які в процесі реалізації заходів захисту інформації, вибраних на основі критерію ефективності СЗІ, визначають варіант системи захисту (вихід СЗІ). Обмеженнями системи є людські, матеріальні, фінансові ресурси, що виділяються на захист інформації, а також обмеження у вигляді вимог до системи, що передбачають прийняття таких заходів захисту інформації, які не знижують ефективність функціонування об'єкта, що підлягає захисту.

С. захисту інформації в автоматизованій системі оброблення інформації /с. защиты инфор-

мации в автоматизированной системе обработки информации/ — система, вбудована в структуру системи автоматизованої обробки інформації, і являє собою регульований цілісний механізм, що складається із системи взаємозв'язаних перешкод, які централізовано управляються з метою перекриття каналів несанкціонованого доступу до інформації. Система захисту інформації в АСОІ може включати в себе: СЗІ елементів АСОІ; систему розпізнавання і розмежування доступу до інформації; засоби захисту інформації в трактах передавання даних; засоби керування безпекою інформації в автоматизованій системі оброблення інформації; систему захисту інформації в мережі передавання даних.

С. захисту інформації в локальній обчислювальній мережі /с. защиты информации в локальной вычислительной сети/ — система, вбудована в структуру мережі обчислювальної локальної, і являє собою регульований цілісний механізм, що складається із системи взаємозв'язаних перешкод, які централізовано управляються з метою перекриття каналів несанкціонованого доступу до інформації ЛОМ. Система захисту включає в себе: засоби захисту інформації в локальній обчислювальній мережі від умисних несанкціонованих доступів, засоби захисту інформації в локальній обчислювальній мережі від випадкових впливів та засоби централізованого контролю і керування захистом інформації в локальній обчислювальній мережі.

С. захисту інформації в мережі передавання даних /с. защиты информации в сети передачи данных/ — сукупність засобів захисту інформації передавального середовища системи автоматизованої обробки інформації, що включає групу елементів АСОІ, які є одночасно елементами мережі передавання даних (МПД), та канали зв'язку. Структура системи захисту інформації в МПД може включати в себе: систему захисту інформації елементів МПД; систему розпізнавання і розмежування доступу до інформації в МПД; систему керування безпекою інформації в МПД; систему захисту інформації в каналах зв'язку; систему підвищення достовірності інформації.

С. захисту інформації в ПЕОМ /с. защиты информации в ПЭВМ/ — сукупність засобів, призначених для перекриття можливих несанкціонованих каналів доступу до ПЕОМ. Система захисту може включати в себе: окреме приміщення з контрольованим доступом; фізичні перепони з охоронної сигналізаці-

єю; блокування замком кожуха системного блока; блокування замком вмикання електроживлення і завантаження програмного забезпечення; спеціальний електронний ключ; програму контролю і розмежування доступу; операційну системну оболонку; пакет антивірусних програм; спеціальні перетворення інформації (компресія, шифрування даних); захист від програм налагодження; зменшення рівня сигналів побічного електромагнітного випромінювання і наведення інформації або зашумлення його; спеціальні засоби стирання залишків на магнітних носіях; спеціальні засоби знищення відходів носіїв інформації; організаційні заходи.

С. захисту інформації комплексна (КСЗІ) /с. защиты информации комплексная (КСЗИ)/ — сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в автоматизованій системі.

С. захищена /с. защищенная/ [s.] — система, яка була розроблена з урахуванням вимог до захисту інформації.

С. зв'язку /с. связи/ [communication s.] — сукупність вузлів і станцій зв'язку, з'єднаних між собою лініями зв'язку в порядку, відповідному до прийнятої організації системи управління та поставлених перед ними завданнями.

С. зв'язку автоматизована /с. связи автоматизированная/ — комплекс автоматизованих вузлів і ліній зв'язку, що забезпечує оперативний взаємообмін інформацією. В с. з. а. входять автоматизовані центри комутації і управління системою, вузли зв'язку пунктів управління, розгалужена мережа різних засобів зв'язку. Автоматизований обмін інформацією може здійснюватися як в аналоговій, так і в дискретній формі (цифровим кодом). В останньому випадку в с. з. а. широко використовується техніка обчислювальна, яка дозволяє одержати найбільшу пропускну здатність ліній зв'язку. В залежності від методів розподілу та передавання інформації с. з. а. поділяються на системи з комутацією каналів, комутацією повідомлень та комутацією каналів і повідомлень.

С. зору людини /с. зрения человека/ — найбільш досконалий засіб спостереження у видимій частині

оптичного діапазону електромагнітного випромінювання. Включає очі та частини мозку, що здійснюють оброблення сигналів, що поступають з сітківки ока. Характеризується наступними можливостями: сприймає світлові промені в діапазоні 0,4–0,76 мкм, причому максимум її спектральної чутливості у світлу пору доби приходиться на голубий колір (0,52 мкм), в темноті — на зелений (0,55 мкм); поріг кутових розмірів, які око розрізняє як дві роздільні точки на об'єкті спостереження, складає вдень — 0,5–1 кут. хв., вночі — 30 кут. хв.; поріг контрастності об'єкта по відношенню до фону складає вдень — 0,01–0,03, вночі — 0,6; діапазон освітленості об'єктів спостереження, до яких адаптується око, 60–70 дБ; при освітленості менше 0,1 лк (в безхмарну місячну ніч) око перестає розрізняти кольори.

С. інформаційна (ІС) /с. информационная (ИС)/ [Information S. (IS)] — 1) Система інформаційного обслуговування, що являє собою організаційно-упорядковану сукупність ресурсів інформаційних, технічних засобів, технологій, що реалізують процеси інформаційні в традиційному або автоматизованому режимі для задоволення інформаційних потреб користувачів. 2) Сукупність носіїв інформаційних і діячів інформаційних, об'єднаних доцільними відносинами інформаційними (див. також система інформаційних відносин). 3) Система, яка здійснює: одержання вхідних даних; оброблення цих даних і/або зміну власного внутрішнього стану (внутрішніх зв'язків/відносин); видачу результату або зміну свого зовнішнього стану (зовнішніх зв'язків/відносин).

С. інформаційна автоматизована (АІС) /с. информационная автоматизированная (АИС)/ [automatized information s.] — система інформаційна, що реалізується на базі технологій інформаційних з використанням засобів обчислювальної техніки, інформатики та зв'язку. До АІС відносяться: банки даних; бази даних; бази знань; системи експертні; системи керування автоматизовані; системи автоматизованого проектування; автоматизовані системи оброблення даних; автоматизовані системи науково-технічної інформації; інформаційно-обчислювальні системи; мережі інформаційні.

С. інформаційна із самонавчанням (ІСС) /с. информационная самообучающаяся (СИС)/ — система інформаційна, що змінює свій стан від впливу інформаційного. Класичними прикладами ІСС може бути

людина, суспільство, держава.

С. інформаційна стратегічна /с. информационная стратегическая/ — поняття, яке поряд з поняттям планування інформаційних систем стратегічного вживають при використанні інформаційно-телекомунікаційних технологій для досягнення і підтримування переваги над конкурентами. С. і. с. — система інформаційна, яка об'єднує процеси планування і полегшує складання стратегічного плану розвитку організації або просто змінює форми боротьби з конкурентами. Якщо інформаційні системи розглядаються як зброя в боротьбі з конкурентами, то їх поділяють на три групи: системи, які націлені на передові інформаційно-телекомунікаційні технології для досягнення переваги над конкурентами (інноваційна стратегія призначається для систем, які спроектовані для передбачення й задоволення майбутніх запитів споживачів); системи, які використовують інформацію для поліпшення фінансових і статистичних даних, забезпечення взаємодії клієнтів з фірмою; системи, які підвищують продуктивність, знижують витрати на виробництво, маркетинг і розповсюдження.

С. інформаційних відносин /с. информационных отношений/ [information retations s.] — упорядкована сукупність відносин зовнішніх і внутрішніх інформаційних (взаємодій) системи інформаційної.

С. інформаційно-обчислювальна /с. информационно-вычислительная/ [information calculation s.] — система автоматизована, призначена для вирішення як інформаційних, так і обчислювальних (розрахункових) задач. Являє собою поєднання АІС з АСОД.

С. інформаційно-телекомунікаційна /с. информационно-телекоммуникационная/ [information telecommunictions s.] — організаційно-технічна сукупність, до складу якої входять системи автоматизовані та мережі передавання даних.

С. інформаційної безпеки /с. информационной безопасности/ [information security s.] — сукупність взаємозв'язаних правничих та організаційних заходів, технічних та програмних засобів, що забезпечують певні умови для керування доступом до ресурсів інформаційних з урахуванням вимог до захисту даних і

для контролю за доступом до тих частин системи інформаційної, які охоплені засобами захисту.

С. інформаційної безпеки країни державна /с. информационной безопасности страны государственная/ [government system of national s.] — організаційне об'єднання державних органів, а також сил та засобів безпеки інформаційної, що виконують свої функції на основі закону під контролем і захистом судової влади. Державна система складає найважливішу ланку системи інформаційної безпеки особистості, суспільства і держави в правовій державі. Основними завданнями такої системи є: виявлення і прогнозування факторів дестабілізуючих і загроз інформаційних життєво важливим інтересам особистості, суспільства і держави; здійснення комплексу оперативних і довготривалих заходів з їхнього попередження і усунення; створення і підтримання в готовності сил та засобів забезпечення інформаційної безпеки. Органи (служби) інформаційної безпеки можуть створюватися (на законодавчих засадах) і в недержавних структурах для захисту своїх потреб в забезпеченні необхідною інформацією. Дані органи на основі укладення відповідних угод можуть бути приєднані до єдиної державної системи інформаційної безпеки.

С. керування автоматизована (АСК) /с. управления автоматизированная (АСУ)/ [automatized control s.] — людино-машинна система, що являє собою сукупність технічних засобів, забезпечення математичного та операторів і організована для вирішення завдань збирання, оброблення, відображення та документування інформації про склад об'єктів керування та середовища, математичного моделювання майбутніх дій об'єктів керування, вироблення рекомендацій для прийняття рішень керівником і передавання командної інформації на об'єкти керування. АСК дозволяє охопити функціонування всіх елементів складної системи єдиною моделлю математичною або комплексом взаємопов'язаних моделей. Найважливішими елементами АСК є: комплекси обчислювальні і мережі, засоби передавання даних, пристрої введення та виведення, зберігання і відображення інформації.

С. керування базами даних (СКБД) /с. управления базами данных (СУБД)/ [database management s. (DBMS)] — база даних в сукупності з керуючою програмою для оперування даними на фізичному рівні. Керуюча програма має наступний мінімальний набір функцій: мова опису і маніпулювання даними; під-

тримка логічних моделей даних; операції над даними (вибірка, вставка, поновлення, вилучення і т. ін.); забезпечення захисту і цілісності даних.

С. керування доступом до об'єктів /с. управления доступом к объектам/ — сукупність ЕОМ та засобів керування доступом людей і транспорту, об'єднаних з метою підвищення надійності ідентифікації шляхом вирішення завдання виявлення і впізнання на основі збільшення кількості інформативних ознак і автоматизації їхнього оброблення. Наявність ЕОМ надає також ряд додаткових можливостей: автоматичний облік робочого часу персоналу; облік присутності персоналу на робочому місці; виявлення місця знаходження співробітника і відвідувача на території організації; дистанційний контроль за станом дверей, турнікетів, шлагбаумів, воріт, датчиків охоронно-пожежної сигналізації; оперативна зміна режиму роботи організації або окремих співробітників.

С. керування ієрархічна /с. управления иерархическая/ [hierarchical control s.] (грец. *ἱεραρξία*, від *ἱερός* — священний і *ἀρξή* — влада) — системи різноманітного призначення, побудовані в функціональному або організаційному відношення у вигляді багаторівневих (багатоступінчастих) структур, в яких функції керування розподілені між співпідпорядкованими рівнями. Керуючі сигнали старших рівнів носять більш загальний характер і конкретизуються на нижчих рівнях.

С. керування корпорації автоматизована /с. управления корпорации автоматизированная/ [corporate automatized control s.] — взаємозв'язана загальними цілями й алгоритмами сукупність комплексів засобів автоматизації пунктів керування регіональними відділеннями корпорації, об'єднаних засобами зв'язку і передавання даних. Динамічність і оперативність процесів керування забезпечується одним з основних складових с. к. к. а. — мережею інформаційно-обчислювальною корпорації.

С. керування розподіленими базами даних (СКРБД) /с. управления распределенными базами данных (СУРБД)/ [distributed database management s.] — система керування базами даних, призначена для організації доступу користувачів до розподіленої бази даних, складові частини якої — локальні бази

даних — розташовані в різних вузлах мережі обчислювальної.

С. кодування /с. кодирования/ [coding s.] — сукупність правил, які визначають систему знаків і порядок їхнього використання до подання, передавання, оброблення і зберігання інформації. В с. к. застосовують алфавіт коду — знаки, які використовуються в с. к., і основу коду — кількість знаків в алфавіті коду.

С. колективного користування (доступу) /с. коллективного пользования (доступа)/ [multiple-access s.] — система, що забезпечує одночасну роботу багатьох користувачів за рахунок розподілу ресурсу.

С. комп'ютерна (КС) /с. компьютерная (КС)/ [computer s., target of evaluation] — сукупність програмно-апаратних засобів, яка подана для оцінки безпеки інформації. Як КС можуть виступати: ЕОМ загального користування або персональна ЕОМ; система операційна; прикладна або інструментальна програма (пакет програм); комплекс засобів захисту, що окремо поставляється, або підсистема захисту від доступу несанкціонованого, наприклад, мережа, яка являє собою надбудову над системою обчислювальною; мережа обчислювальна локальна, як сукупність апаратних засобів, програмного забезпечення, що реалізує протоколи взаємодій, мережної операційної системи і т. ін.; обчислювальна система системи автоматизованої, яка реально функціонує, в найбільш загальному випадкові — власне автоматизована система або її частина.

С. комп'ютерна захищена /с. компьютерная защищенная/ [trusted computer s., trusted computer product] — система комп'ютерна, яка здатна забезпечувати захист інформації, що оброблюється, від певних загроз.

С. контролю доступу /с. контроля доступа/ [access monitoring s.] — сукупність організаційних заходів і технічних засобів, призначених для ідентифікації і перевірки автентичності осіб, що допускаються на об'єкт захисту. Традиційно використовується система перепусток з фотографіями особи власника та відомостей про нього, системи з записами на носіях кодових значень паролів, а також перспективні системи з використанням біометричних методів, в яких як ідентифікатори використовуються відбитки пальців,

долоні, голосу, особистого підпису і т. ін.

С. криптографічна /с. криптографическая/ [cryptosystem] — сукупність засобів криптографічного захисту інформації, необхідної ключової, нормативної, експлуатаційної, а також іншої документації (у тому числі такої, що визначає заходи безпеки), використання яких забезпечує належний рівень захищеності інформації, що обробляється, зберігається та (або) передається. Див. також криптосистема, система шифрувальна.

С. криптографічного захисту даних (СКЗД) /с. криптографической защиты данных (СКЗД)/[cryptosystem] — сукупність програмних і апаратних засобів, що реалізують захист інформації за допомогою перетворення криптографічного.

С. криптографічного захисту інформації /с. криптографической защиты информации/ — сукупність органів, підрозділів, груп, діяльність яких спрямована на забезпечення захисту інформації криптографічного, та підприємств, установ і організацій, що розробляють, виготовляють, експлуатують та (або) розповсюджують криптосистеми і засоби криптографічного захисту інформації.

С. менеджменту інформаційної безпеки /с. менеджмента информационной безопасности/ [information security management s.] — див. стандарт ISO/IEC 17799.

С. моніторингу інформаційної безпеки /с. мониторинга информационной безопасности/ [information security monitoring s.] — ієрархічна структура, вищою ланкою якої є надвідомчий повноважний орган, куди з міністерств, відомств та власних джерел поступає інформація про стан безпеки об'єктів і систем. Аналіз цієї інформації дозволить оцінювати і прогнозувати ситуацію із забезпечення безпеки, здійснити координацію діяльності і сформувати плани розвитку системи безпеки в цілому.

С. оброблення даних (інформації) /с. обработки данных (информации)/ [data processing s.] — комплекс апаратних та інших засобів, призначених для механізації і автоматизації оброблення даних (інформації).

С. оброблення даних (інформації) автоматизована (АСОД, АСОІ) /с. обработки данных (ин-

формации) автоматизированная (АСОД, АСОИ)/ [automatized data processing s.] — комплекс програмних і технічних засобів, призначених для вирішення широкого кола обчислювальних задач. Забезпечує введення даних, оброблення їх за заданими алгоритмами (програмами) і виведення результатів рішення в заданій формі. АСОД можуть бути зосередженими і розподіленими. До зосереджених АСОД відносяться ЕОМ, комплекси обчислювальні, ПЕОМ та системи обчислювальні, а до розподілених — мережі обчислювальні, системи керування автоматизовані, системи телеоброблення даних.

С. оброблення інформації захищена /с. обработки информации защищенная/ [protected data processing s.] — система оброблення інформації, яка для певних умов експлуатації забезпечує безпеку (конфіденційність і цілісність) інформації, що оброблюється, і підтримує свою працездатність в умовах впливу на неї заданої множини загроз. С. о. і. з. повинна мати наступні властивості: здійснювати автоматизацію процесу оброблення конфіденційної інформації, що включає усі аспекти цього процесу зв'язані із забезпеченням безпеки інформації, що оброблюється; успішно протидіяти загрозам безпеці, що діють в певному середовищі; відповідати вимогам і критеріям стандартів інформаційної безпеки.

С. обчислювальна /с. вычислительная/ [computer s.] — 1) Сукупність ЕОМ та її забезпечення програмного, призначених для організації і виконання процесу обчислювального. 2) Сукупність програмно-апаратних засобів, призначених для оброблення інформації.

С. оманна /с. обманная/ [deception s.] — система захисту, принцип дії яких полягає в введенні порушника в оману про систему обробки інформації, яка захищається. Існує три типи методів, на яких будуються с. о.: приховування, камуфляж та дезінформація.

С. операційна безпечна /с. операционная безопасная/ [secure operating s.] —- операційна система, яка забезпечую таке керування апаратними та програмними засобами, що дозволяє забезпечувати належний рівень захисту, відповідний до цінності даних та ресурсів, які оброблюються за допомогою цієї системи операційної.

С. операційна (ОС) /с. операционная (ОС)/ [operating s.] — сукупність програмних засобів, які за-

безпечують керування апаратними ресурсами системи обчислювальної та взаємодію програмних процесів з апаратурою, іншими процесами та користувачами. Звичайно, ОС виконує наступні дії: керування пам'яттю, вводом/виводом, файловою системою, взаємодію та диспетчеризацію процесів, захист, облік використання ресурсів, обробка мови команд.

С. охорони об'єктів /с. охраны объектов/ — сукупність людей та засобів інженерного захисту і технічної охорони об'єктів, що створюють систему охорони джерел інформації (див. метод охорони джерел інформації. В найбільш загальному випадку структуру с. о. о. складають підсистеми: інженерного захисту; сповіщення; спостереження; нейтралізації загроз; керування. Ефективність системи оцінюють ймовірністю виявлення службою безпеки зловмисника або пожежі, а також часом пересування зловмисника на території організації до джерела інформації і назад. В залежності від структури с. о. о. поділяють на автономні і централізовані. В автономних с. о. о. всі завдання охорони вирішуються в межах однієї організації, в централізованих — підсистеми нейтралізації загроз і керування є загальними для декількох організацій.

С. охорони об'єктів інтегрована автоматизована /с. охраны объектов интегрированная автоматизированная/ — система автоматизована ієрархічної структури, реалізована на основі адресних панелей, що обслуговують сигналізатори (датчики) (охоронні, охоронно-пожежні, пожежні, зчитувачі електронних замків і т. ін.), і виконавчі пристрої (телевізійних камер, сповіщувачів сигналізації тривожної, виконавчих механізмів замків, піропатронів, модулів газового гасіння пожежі і т. ін.). Загальне керування системою здійснюється одною або декількома ЕОМ. Стан об'єктів охорони відображається у графічному вигляді на робочому місці оператора. На екрані монітора вимальовується план вибраної території із зазначенням стану кожної окремої зони у супроводі тексту, звукових і мовних сигналів. На екран у поліекранному режимі можуть виводитися зображення від відповідних телевізійних камер. Засоби реєстрації фіксують: події, що виникають у випадку тривожних або нештатних ситуацій; постановку і знімання з охорони зон об'єктів охорони; дії оператора, що визначаються як його втручання у роботу системи, так і його реакцією на тривожні події; несправності, викликані виходом з ладу апаратури, порушенням ліній комунікацій або несанкціоно-

ваного втручання в роботу системи. Закладається також можливість контролю роботи чергової зміни як на робочих місцях, так і на маршруті при обході зон, що охороняються.

С. охоронної сигналізації /с. охранной сигнализации/ — сукупність сигналізаторів (датчиків), об'єднаних в електронну систему для узгодженого функціонування, з центром керування і засобами відображення їхнього стану. С. о. с. створюють фізичну перепону захисного контуру об'єкта захисту і найчастіше розміщуються за периметром зони, що охороняється. В залежності від принципу дії с. о. с. класифікуються наступним чином: традиційні звичайні, засновані на використанні кіл сигналізації і індикації в комплексі з різноманітними контактами (датчиками); ультразвукові; з перериванням променя; телевізійні; радіолокаційні; мікрохвильові та інші.

С. підвищення достовірності інформації /с. повышения достоверности информации/ — сукупність засобів мережі передавання даних, що забезпечують захист інформації від випадкових впливів. Див. достовірність оброблення інформації та контроль достовірності.

С. пошукові /с. поисковые/ — спеціальні сервери, створені для полегшення пошуку інформації на WWW, FTP і т.ін. за запитом користувача на природній мові. П. с. видає сторінку (сторінки) із посиланнями на ресурси, що задовольняють умові пошуку. Найбільш популярні: Російські: yandex.ru, www.rambler.ru, www.online.ru. Міжнародні: www.yahoo.com, www.altavista.digital.com. Пошук файлів: ftpsearch.ntnu.no, www.filez.com, www.shareware.com. Інформація про вміст сервера буде внесена в базу даних пошукової системи тільки за умови реєстрації його покажчика URL.

С. радіозв'язку /с. радиосвязи/ [radio communication s.] — сукупність радіостанцій для здійснення радіообміну у порядку, відповідному до прийнятої організації системи управління та поставлених перед ними завданнями.

С. радіозв'язку секретного /с. радиосвязи секретной/ — система радіозв'язку із використанням засобів захисту від несанкціонованого доступу.

С. радіозв'язку стільникова /с. радиосвязи подвижной сотовая/ — система наземної рухомої ра-

діослужби, що складається із замкнутої системи базових радіостанцій, які покривають наземну поверхню зонами за принципом бджолиних стільників. В с. р. с. вирішена проблема економії спектра радіочастот шляхом багаторазового використання частотного ресурсу рознесенням у просторі прийомопередавачів, у яких частоти робочі співпадають. Стільникова топологія дозволила багатократно збільшити ємність телекомунікаційнихмереж по відношенню до мереж радіальної структури без погіршення якості зв'язку і розширення наданої смуги радіочастот. Для цього в с. р. с. реалізовані способи визначення поточного місцезнаходження рухомих абонентів і забезпечення безперервного зв'язку при переміщенні абонента з одного стільника в інший. Існують як аналогові, так і цифрові стандарти стільникового радіозв'язку.

С. радіозв'язку транкового /с. радиосвязи транкинговой/ — система наземної рухомої радіослужби, що надає послуги внутрішньовідомчого радіозв'язку (мережі корпоративної). Особливістю с. т. р. є використання напівдуплексного режиму роботи.

С. радіотехнічна (РТС) /с. радиотехническая (РТС)/ [radio engineering s.] — сукупність рознесених у просторі та взаємодіючих між собою радіотехнічних засобів, об'єднаних для вирішення певних завдань. Розрізняють радіолокаційні, радіонавігаційні, радіотелеметричні, радіотелекерування, радіопротидії (радіоелектронної боротьби) та інші РТС і засоби. Інформація ознакова, що міститься в сигналах РТС, використовується для оцінки їхніх технічних рішень та можливостей, а також може застосовуватися для порушення правильного функціонування цих систем.

С. розвідки /с. разведки/ [intelligence s.] — сукупність органів розвідки, що створюють багаторівневу ієрархічну структуру, призначену для добування, оброблення та доведення споживачам інформації, необхідної для прийняття рішень. Основним складовими с. р. є органи добування інформації, органи збирання і оброблення інформації та органи планування і управління. В органах планування і управління на основі завдань керівництва перед розвідкою формулюються конкретні завдання, плануються операції розвідувальні, залучаються необхідні сили і засоби та здійснюється управління ними. У відповідності з поставленими завданнями і планом проведення операції органи добування забезпечують контакт розвідувальний з дже-

релами інформації і одержують від них дані і відомості, які після збирання і оброблення у відповідному органі подаються споживачеві інформації.

С. розмежування доступу /с. разграничения доступа/ [security policy realization] — сукупність реалізованих правил розмежування доступу в засобах обчислювальної техніки або автоматизованих системах.

С. розпізнавання і розмежування доступу до інформації /с. распознавания и разграничения доступа к информации/ — сукупність засобів контролю і керування доступом, призначених для перекриття несанкціонованого доступу і контролю санкціонованого доступу до інформації, яка потребує захисту. Розмежування доступу здійснюється у відповідності до функціональних обов'язків і повноважень осіб-користувачів, обслуговуючого персоналу, просто користувачів, а допускаються і виконуються тільки ті звернення до інформації, в яких містяться відповідні ознаки дозволених повноважень. Основні завдання системи: ідентифікація й автентифікація користувачів, пристроїв, процесів і т. ін.; розподілення інформації і функцій її оброблення; установка і введення повноважень.

С. слухова людини /с. слуховая человека/ — природний засіб безпосереднього підслухування акустичних сигналів, що розповсюджуються від джерела звуку прямолінійно у повітрі, повітроводами або через різноманітні огорожі (двері, стіни, вікна і т. ін.). С. с. л. забезпечує приймання акустичних сигналів в діапазоні звукових (20–20000 Гц) частот, межі якого для різних людей коливаються в широких межах і змінюються з віком.

С. стеганографічна (стегосистема)/с. стеганографическая (стегосистема)/ [stegosystem] — сукупність засобів та методів, які використовуються для формування прихованого каналу передавання інформації.

С. телевізійна /с. телевизионная/ [television s.] — комплекс радіоелектронних, оптичних і механічних засобів, призначених для одержання телевізійних сигналів, передавання, приймання і вторинного перетворення їх в видиме зображення. С. т. поділяються: за якісними ознаками — на чорно-білі, кольорові, стереоскопічні, стереокольорові; за шириною спектра телевізійного сигналу — на широкосмугові та вузькосмугові;

за видом розгортки зображення — на одностроκові та багатострокові (малокадрові та багатокадрові); за способом передавання сигналу — на відкриті або розімкнені (з передаванням радіосигналу по радіоканалу) і замкнені (з передачею по кабелю), з використанням ліній зв'язку волоконно-оптичних та лазерів; за використанням — на космічні, авіаційні, підводні, диспетчерські і т. ін.

С. телеоброблення даних /с. телеобработки данных/ [teleprocessing s.] — взаємозв'язаний комплекс технічних, програмних засобів і процедур обміну даними, що реалізує телеоброблення даних.

С. технічного захисту інформації /с. технической защиты информации/ [s. of technical protection of information] — сукупність організаційних структур, нормативно-правових документів та засобів забезпечення захисту інформації технічного.

С. шифрувальна /с. шифровальная/ [cryptosystem] — сукупність правил, які повністю визначають процес зашифровування/розшифровування — підготовка відкритого тексту до шифрування, власне дії по виконанню перетворення відкритого тексту в шифрований і навпаки, спосіб передавання шифрованих повідомлень адресата. Див. також система криптографічна.

СИТО /сито/ [sieve, bolter] — пристрій у вигляді металевого листа з дрібними дірочками або сітка для просіювання та сортування сипких речовин.

С. Ератосфена /с. Эратосфена/ — те ж, що тест пробного ділення.

СИТУАЦІЯ /ситуация/ [situation] (франц. situation, від лат. situs — становище) — збіг умов і обставин, що створюють певне становище; обстановка.

С. індивідуальна /с. инивидуальная/ — ситуація інформування, що складається тоді, коли вплив переконуючий вдається здійснити на будь-яку конкретну аудиторію, з урахуванням її психологічних характеристик. Це може бути і мовлення усне на один з підрозділів військ противника, що знаходиться на передньому краю його оборони, і програма радіомовлення, призначена для певної соціально-психологічної групи населення. В с. і. простіше визначити прийнятний стиль надання інформації, простіше підібрати необхідну лексику і т. ін. Тому ефективність впливу на війська й населення противника у цьому випадку

значно вища, ніж в ситуації масовій.

С. інформування /с. информирования/ — сукупність умов, в яких здійснюється інформування, а також характер реакції об'єкта на зміст повідомлення. С. і. з метою переконуючого впливу поділяють на ситуацію індивідуальну і ситуацію масову.

С. масова /с. массовая/ — ситуація інформування, що складається тоді, коли інформування з метою переконування здійснюється одночасно на численну різноманітну аудиторію. В цьому випадку важко забезпечити належну адресність впливу і необхідно виходити із загальних психологічних закономірностей сприйняття: переконуючий вплив, що містить сильні аргументи проти будь-якої думки, якої притримується адресат, більш ефективний тоді, коли увага об'єкта будь-чим відвертається (ілюстраціями в листівці, музичним супроводом і різноманітними шумами в програмі радіомовлення, відеорядом в телевізійній програмі); ефект "контрастної оцінки віддалених позицій", суть якого в тому, що якщо зміст переконуючого впливу здається значно відмінним від позицій його об'єкта, то він оцінюється як неприпустимий; ефект "асимілятивної оцінки віддалених поглядів", в силу якого якщо зміст переконуючого впливу здається таким, що майже не відрізняється від поглядів адресата, то останній часто ототожнює власні погляди із змістом переконуючого впливу.

СКАНЕР /сканер/ [scanner] — 1) Пристрій вводу зображення в пам'ять ЕОМ. 2) В системах програмування — лексичний аналізатор.

С. сітківки ока /с. сетчатки глаза/ — пристрій, призначений для введення зображення сітківки ока користувача в пам'ять ЕОМ з метою подальшої його ідентифікації.

СКРЕМБЛЕР /скремблер/ [scrambler] — кодувальний пристрій, який видає випадкову послідовність бітів, забезпечуючи постійність спектральної густини модульованих сигналів незалежно від змісту інформації, що передається (див. скремблювання). В найбільш загальному випадку с. реалізує логічну операцію підсумовування за модулем два вихідного і перетворюючого випадкового двійкового сигналу. Обернена операція здійснюється пристроєм, що називаються дескремблером. С. і дескремблери реалізуються за до-

помогою регістрів зсуву.

С. аналоговий /с. аналоговый/ [analog s.] — засіб закриття мовної інформації технічного, що реалізує способи скремблювання аналогового. С. а. прості в технічній реалізації, мають низьку вартість і малі габарити. Можуть експлуатуватися практично на будь-яких каналах зв'язку, призначених для передавання мовних повідомлень. Основний недолік с. а. — відносно низька стійкість закриття інформації. Крім того, с. а. вносять спотворення у відновлений мовний сигнал.

С. з інверсією кадру /с. с инверсией кадра/ — скремблер аналоговий, що реалізує спосіб часового закриття. Інверсія кадру забезпечується шляхом попереднього запам'ятовування в пам'яті передавального скремблера відрізка мовного повідомлення (кадру) тривалістю T_k і зчитування його (з передаванням в телефонну лінію) з кінця кадру (інверсно). При прийманні кадр мовного повідомлення запам'ятовується і зчитується з пристрою пам'яті у зворотному порядку, що забезпечує відновлення повідомлення. Для досягнення нерозбірливості мови необхідно, щоб тривалість кадру була не менше 250 мс. В цьому випадку сумарна тривалість запам'ятовування і інверсного передавання кадру складає приблизно 500 мс, що може створити значні затримки сигналу при телефонній розмові.

С. з інверсією спектра /с. с инверсией спектра/ — скремблер аналоговий, в якому реалізоване перетворення спектру мовного сигналу шляхом обернення частотної смуги сигналу навкруги деякої середньої точки спектра f_0. В цьому випадку досягається ефект перетворення низьких частот в більш високі і навпаки. Такий скремблер забезпечує невисокий рівень закриття, так як при перехопленні достатньо легко визначається значення частоти f_0 інверсії спектру мовного сигналу.

С. з часовими перестановками /с. в временными перестановками/ — скремблер аналоговий, в якому кадр мовного повідомлення ділиться на відрізки (сегменти) тривалістю τ_c кожний. Послідовність передавання в лінію сегментів визначається ключем, який повинен бути відомий приймальній стороні. Змінюванням ключа в ході сеансу зв'язку в скремблерах (динамічним закриттям) можна суттєво підвищити рівень захисту мовної інформації. Залишкова розбірливість залежить від тривалості кадру і із збільшенням останньої

зменшується. Внаслідок накопичення інформації в блоці часового перетворення з'являється затримка між вхідним мовним сигналом і відновленим сигналом. Ця затримка неприємно сприймається на слух, якщо перевищує 1–2 с. Тому T_k вибирають рівною $(4–16)\tau_c$.

С. з частотними перестановками /с. с частотными перестановками/ — скремблер аналоговий, в якому спектр вхідного сигналу розділяється на декілька частотних смуг (до 10–15), що перемішуються (переставляються) відповідно до деякого алгоритму (ключа). При прийомі спектр сигналу відновлюється в результаті зворотних процедур. Зміна ключа в ході сеансу зв'язку в скремблерах (динамічне закриття) дозволяє підвищити ступінь закриття, але при цьому потрібна передача на приймальну сторону сигналів синхронізації, що відповідають моментам зміни ключа.

С. комбінований /с. комбинированный/ — скремблер аналоговий, в якому для підвищення ступеня закриття мови використовують комбінацію часового і частотного скремблювання. В с. к. вхідне повідомлення розділяється на кадри і сегменти, які запам'ятовуються в пам'яті скремблера. При формуванні повідомлення, що передається, здійснюються перестановки сегментів кадру і перестановки смуг спектра мовного сигналу кожного сегменту. Якщо при цьому забезпечити динамічну зміну ключа часової і частотної перестановки, то рівень захисту такого комбінованого технічного закриття може наближатися до рівня захисту при шифруванні мовної інформації. Проте складність реалізації такого скремблера і вимоги до якості передавання синхроімпульсів між скремблерами телефонних абонентів також високі.

СКРЕМБЛЮВАННЯ /скремблирование/ [scramble, scrambling] (від англ. scramble — зашифровувати) — 1) Перетворення інформаційного двійкового сигналу з будь-якими статистичними властивостями у двійковий сигнал, в якому послідовність одиниць і нулів змінюється по випадковому або псевдовипадковому закону. С. можна розглядати як вторинне кодування без внесення надмірності. Воно здійснюється на передавальній стороні за допомогою пристрою, що називається скремблером. На приймальній стороні здійснюється зворотна операція — дескремблювання — пристроями, що називаються дескремблерами. 2) Спрощений метод захисту інформації, заснований, як правило, на перестановці (змішуванні) окремих

елементів повідомлення без використання ключа.

С. аналогове /аналоговое с./ — перетворення аналогового сигналу з будь-якими статистичними властивостями в сигнал, що змінюється по випадковому або псевдовипадковому закону. С. а. застосовується для технічного закриття мовних сигналів. При с. а. характеристики вхідного мовного повідомлення змінюються таким чином, що перетворене повідомлення стає несприйнятим для слухової системи людини, але займає таку саму смугу частот. Це дозволяє передавати скрембльовані сигнали звичайними телефонними каналами зв'язку. За видом перетворення способи с. а. поділяється на частотне і часове, за режимом закриття — на статичне і динамічне. У відповідності до способів с. а. розрізняють скремблери з інверсією спектру, з частотними перестановками, з інверсією кадру, з часовими перестановками, а також скремблери комбіновані.

СКРИНЬКА /ящик/ [box] — невеликий ящик з кришкою й замком.

С. поштова персональна /персональный почтовый я./ [personal letter-b.] — дисковий простір на сервері поштовому, виділений для збереження листів користувача, що надходять на його адресу. Після приєднання до поштового сервера користувач працює з поштовою скринькою: поміщає в нього листи для відправлення, забирає ті, що надходять до нього і т. ін.)

СКРИТНІСТЬ /скрытность/ [secrecy] — властивість навмисного приховування чогось від інших; дотримання в таємниці так, щоб ніхто не зміг дізнатися, таємність, секретність, замаскованість.

СЛОВНИК /словарь/ [glossary, dictionary] — 1) Впорядкований перелік слів, символічних імен або найменувань з їхніми значеннями або тлумаченнями. 2) В обчислювальній техніці — структура даних, що забезпечує доступ до даних за текстовим іменем.

СЛОВО /слово/ [word] — 1) Послідовність символів в деякому алфавіті, що має деяке смислове значення. 2) Див. машинне слово.

С. машинне /с. машинное/ [computer w.] — послідовність бітів або знаків, що розглядається апаратною частиною ЕОМ як єдине ціле.

СЛУЖБА /служба/ [service] — яка-небудь спеціальна галузь праці разом із закладами, що відносяться до неї.

С. безпеки /с. безопасности/ [security s.] — організація (підрозділ) чи сукупність організацій, які постійно здійснюють практичну діяльність щодо забезпечення безпеки.

С. іменування доменів (система іменування доменів) /с. именования доменов (система именования доменов)/ [Domain Name S. (System)(DNS)] — ієрархічна служба імен, створена для більш ефективного використання величезного простору імен. Основне призначення DNS — трансляція імен в адресі IP (хоча DNS забезпечує і такі послуги, як зберігання і надання інформації про користувачів і списки розсилки, а також спрощує обмін поштою). Наприклад, www.kubstu.ru — 194.186.178.21; www.sony.com — 209.67.25.41; www.music.ru — 195.54.192.45. Основні поняття, що визначаються DNS, — простір імен, розподілена база даних і протокол обміну інформацією. DNS як і служба каталогів, або імен, традиційно подається у вигляді дерева, кожний елемент якого — вузол — має унікальне ім'я домена (або повністю визначене ім'я домена). Вузол на вершині називається коренем. Ім'я домена будується за наступним правилом: до власного імені вузла додаються імена батьківського вузла і усіх прабатьків аж до кореня. В імені домена імена вузлів розділяються точками. Корінь також позначають точкою, але в імені домена її часто пропускають. Кожний компонент імені домена може складати до 63 байт, а загальна довжина обмежена 256 байтами. Всі компоненти, звичайно, (але не обов'язково) складаються з ASCII-символів, що друкуються. Імена доменів в DNS не чутливі до регістра символів.

С. інформаційна /с. информационная/ [information s.] — організація (підрозділ, установа) чи сукупність організацій, які постійно здійснюють практичну роботу щодо інформаційного обслуговування. С. і. можуть мати різноманітний характер в залежності від масштабів роботи: від с. і. установ (підприємств) до загальнодержавних та міжнародних інформаційних служб.

С. інформаційно-аналітична /с. информационно-аналитическая/ — орган діяльності інформаційно-аналітичної. В практичній роботі важливо, щоб в с. і.-а. здійснювався замкнутий цикл підготовки мате-

ріалів, — від процедури визначення показників збирання інформації, її класифікації, автоматизованого оброблення до аналізу інформації, розроблення прогнозів і практичних рекомендацій. Можна виділити три рівні діяльності с. і.-а.: інформаційно-технологічний, який передбачає наявність комп'ютерів, мереж, засобів зв'язку та програмного середовища, яке дозволяє нагромаджувати, обробляти й шукати інформацію в автоматизованому режимі; інформаційний, що передбачає наявність інформації, яка використовується для аналізу (перевага повинна надаватися власним базам даних, що створюються для вирішення конкретних завдань); аналітичний (ґрунтується на залученні до роботи аналітиків і експертів). При вирішенні завдань с. і.-а. використовується методологія моніторингу і центрів ситуаційних.

С. інформаційної безпеки /с. информационной безопасности/ [infosecurity s.] — підрозділ, призначений для здійснення контролю і керування захистом інформації в процесі підготовки і експлуатації системи оброблення інформації (див. заходи по безпеці інформації організаційні). Крім того, в процесі експлуатації системи рекомендується проводити: періодичні перевірки повноважень осіб, що працюють на it комплекс засобів автоматизації (КЗА); інспектування правильності і повноти виконання персоналом заходів по забезпеченню збереження необхідних дублікатів файлів, бібліотеки програм, обладнання КЗА; практичну перевірку функціонування окремих засобів захисту; контроль недозволених змін програм і обладнання; контроль усіх процедур з бібліотеками файлів на носіях і т. ін.; стимулювання персоналу в питаннях забезпечення захисту; розробку і забезпечення усіх протипожежних заходів і навчання персоналу діям по тривозі; консультування усіх співробітників, що працюють на КЗА, з питань захисту інформації. Одним з найважливіших обов'язків с. і. б. є організація і навчання персоналу методам захисту інформації. Навчання є необхідним для усіх співробітників, починаючи з моменту їхнього вступу до роботи, включаючи керівний склад організації — споживачів інформаційної системи.

С. каталогів /с. каталогов/ [directory s.] — служба, призначена для організації пошуку комп'ютерними програмами об'єктів за їхніми атрибутами, такими як рівень доступу, членство в доменах і групах, способи автентифікації, мережні адреси і адреси портів. Для керування величезними обсягами інформації с. к.

реалізують у вигляді бази даних, що зберігається на окремому сервері. Клієнт приєднується до с. к. для перегляду або обновлення її бази даних. Деякі с. к. здатні обмінюватися інформацією з аналогічними службами. С. к., як правило, виконують перетворення мнемонічних імен в адреси IP і навпаки, що носить назву служба імен (name service) і є однією з множини послуг, що надаються с. к. Найбільш популярна служба імен — служба (система) іменування доменів.

С. новин /с. новостей/ [news s.] — організація, що займається збиранням новин і їх підготовкою для розповсюдження серед мас-медіа. За характером своєї діяльності такі служби схожі на агентства новин, але за масштабами діяльності вони можуть бути більш локалізованими. Можливі випадки розростання с. н. і перетворення їх у великі інформаційні комплекси, які конкурують з видними агентствами новин. Суттєвий вплив на можливості подальшого розвитку різноманітних форм і функцій с. н. здійснює процес розгортання глобальних супермагістралей інформаційних.

С. охорони /с. охраны/ — підрозділ, призначений для своєчасного виявлення і затримання порушників, що намагаються проникнути на об'єкт (з об'єкта), в режимні приміщення (будівлі, склади, сховища), а також для збереження матеріальних цінностей, попередження подій і ліквідації їхніх наслідків на об'єкті, що охороняється.

С. радіозв'язку /с. радиосвязи/ [radio s.] — див. радіослужба.

С. радіомовлення /с. радиовещания/ [broadcasting s.] — служба радіозв'язку, в якій передача призначена для безпосереднього приймання населенням.

С. розвідки /с. разведки/ [intelligence s.] — організація (підрозділ, установа) чи сукупність організацій, що постійно здійснюють практичну роботу щодо добування, оброблення та доведення споживачам інформації, необхідної для прийняття рішень.

С. розвідувальна /с. разведывательная/ [intelligence s.] — див. служба розвідки.

С. рухомого радіозв'язку /с. подвижной радиосвязи/ [mobile radio s.] — служба радіозв'язку між

рухомою та нерухомою радіостанціями, або між рухомими станціями.

С. секретна /с. секретная/ [secret s.] — традиційна і неофіційна назва загальнонаціональних розвідувальних організацій.

С. сервісна автентифікації джерела даних /сервисная с. аутентификации источника данных/ — служба сервісна захисту інформації в мережах телекомунікацій, яка реалізує свої функції за допомогою процедур шифрування даних (на рівнях мережному і транспортному моделі взаємодії відкритих систем) та підпису цифрового (на мережному, транспортному і рівні прикладному).

С. сервісна автентифікації однорівневих об'єктів /с. сервисная аутентификации обноуровневых объектов/ — служба сервісна захисту інформації в мережах телекомунікацій, яка реалізує свої функції за допомогою процедур автентифікації (на рівнях мережному, транспортному і прикладному моделі взаємодії відкритих систем) та шифрування даних і підпису цифрового (на мережному та транспортному рівнях МВВС).

С. сервісна забезпечення цілісності вибіркових полів без з'єднання /с. сервисная обеспечения целостности выборочных полей без соединения/ — служба сервісна захисту інформації в мережах телекомунікацій, яка реалізує свої функції за допомогою процедур забезпечення цілісності даних, шифрування даних (на рівні прикладному моделі взаємодії відкритих систем) та цифрового підпису (на рівнях мережному, транспортному і прикладному).

С. сервісна забезпечення цілісності вибіркових полів даних /с. сервисная обеспечения целостности выборочных полей данных/ — служба сервісна захисту інформації в мережах телекомунікацій, яка реалізує свої функції за допомогою процедур забезпечення цілісності даних та шифрування даних на рівні прикладному моделі взаємодії відкритих систем.

С. сервісна забезпечення цілісності даних без встановлення з'єднання /с. сервисная обеспечения целостности данных без установления соединения/ — служба сервісна захисту інформації в мережах телекомунікацій, яка реалізує свої функції за допомогою процедур забезпечення цілісності даних, шифру-

вання даних (на рівнях мережному, транспортному і прикладному моделі взаємодії відкритих систем) та підпису цифрового (на транспортному рівні МВВС).

С. сервісна забезпечення цілісності з'єднання без відновлення /с. сервисная обеспечения целостности соединения без восстановления/ — служба сервісна захисту інформації в мережах телекомунікацій, яка реалізує свої функції за допомогою процедур забезпечення цілісності даних та шифрування даних на рівнях мережному, транспортному і прикладному моделі взаємодії відкритих систем.

С. сервісна забезпечення цілісності з'єднання з відновленням /с. сервисная обеспечения целостности соединения с восстановлением/ — служба сервісна захисту інформації в мережах телекомунікацій, яка реалізує свої функції за допомогою процедур забезпечення цілісності даних та шифрування даних на рівнях транспортному і прикладному моделі взаємодії відкритих систем.

С. сервісна засекречування в режимі без з'єднання /с. сервисная в режиме без засекречивания соединения/ — служба сервісна захисту інформації в мережах телекомунікацій, яка реалізує свої функції за допомогою процедур шифрування даних (на рівнях канальному, мережному, транспортному, представницькому і прикладному моделі взаємодії відкритих систем) та керування маршрутом (на мережному рівні МВВС).

С. сервісна засекречування вибіркових полів /с. сервисная засекречивания выборочных полей/ — служба сервісна захисту інформації в мережах телекомунікацій, яка реалізує свої функції за допомогою процедури шифрування даних на рівнях представницькому і прикладному моделі взаємодії відкритих систем.

С. сервісна засекречування з'єднання /с. сервисная засекречивания соединения/ — служба сервісна захисту інформації в мережах телекомунікацій, яка реалізує свої функції за допомогою процедур шифрування даних (на рівнях фізичному, канальному, мережному, транспортному, представницькому і прикладному моделі взаємодії відкритих систем) та керування маршрутом (на мережному рівні МВВС).

С. сервісна засекречування потоку даних /с. сервисная засекречивания потока данных/ — служба

сервісна захисту інформації в мережах телекомунікацій, яка реалізує свої функції за допомогою процедур шифрування даних (на рівнях фізичному і представницькому моделі взаємодії відкритих систем), заповнення потоку (на рівні мережному, і прикладному МВВС) та керування маршрутом (на мережному рівні МВВС).

С. сервісна інформування про відправлення /с. сервисная информирования про отправку/ — служба сервісна захисту інформації в мережах телекомунікацій, яка реалізує свої функції за допомогою процедур підтвердження характеристик даних, забезпечення цілісності даних та цифрового підпису на рівні прикладному моделі взаємодії відкритих систем.

С. сервісна інформування про доставку /с. сервисная информирования про доставку/ — служба сервісна захисту інформації в мережах телекомунікацій, яка реалізує свої функції за допомогою процедур підтвердження характеристик даних, забезпечення цілісності даних та цифрового підпису на рівні прикладному моделі взаємодії відкритих систем.

С. сервісна контролю доступу /с. сервисная контроля доступа/ — служба сервісна захисту інформації в мережах телекомунікацій, яка реалізує свої функції за допомогою процедури керування доступом до ресурсів телекомунікаційної системи на рівнях мережному, транспортному і прикладному моделі взаємодії відкритих систем.

С. сервісні захисту інформації в мережах телекомунікацій /с. сервисные защиты информации в сетях телекоммуникаций/ — сукупність заходів захисту інформації в мережах телекомунікацій, які у відповідності до рекомендацій МОС реалізуються за допомогою спеціальних процедур. У рекомендаціях визначені вісім процедур захисту, спільне використання яких дозволяє організувати 14 сервісних служб.

СМАРТ-КАРТКА (ІНТЕЛЕКТУАЛЬНА КАРТКА) /смарт-карта (интеллектуальная карта)/ [chip-in card, integrated circuit card, intelligent card, smart card] — картка з мікросхемою, що являє собою повний мікрокомп'ютер (мікроконтролер) з операційною системою, програмним забезпеченням і системою захисту даних.

СМУГА /полоса/ [band] — довга вузька частина якого-небудь простору.

С. затримування фільтра /п. удержания фильтра/ — смуга частот, в якій загасання передавання фільтра дорівнює або більше заданого значення.

С. пропускання каналу зв'язку /п. пропускания канала связи/ [communication channel pass b. (communication channel transmission b.)] — смуга частот, яку пропускає канал зв'язку. За шириною смуги частот канали зв'язку поділяються на вузькосмугові і широкосмугові.

С. пропускання радіоприймача /п. пропускания радиоприемника/ [receiver pass b.] — смуга частот, по краях якої коефіцієнт підсилення радіоприймача від входу до детектора зменшується відносно найбільшої величини у встановлене число разів.

С. пропускання фільтра /п. пропускания фильтра/ [filter pass b., filter transmission b.] — смуга частот, в якій загасання передавання фільтра дорівнює або менше заданого значення.

С. радіочастот контрольна /п. радиочастот контрольная/ [check frequency b.] — смуга частот, за верхнім і нижнім краями якої будь-яка складова має послаблення на 30 дБ і більше відносно рівня випромінювання, прийнятого за 0 дБ.

С. радіочастот надана /разрешенная п. радиочастот/ — смуга частот, в межах якої радіостанції дозволене випромінювання. Ширина с. ч. н. дорівнює смузі радіочастот необхідній плюс подвоєне абсолютне допустиме значення відхилення частоти, а для космічних станцій — плюс подвоєний максимальний допплерівський зсув частоти відносно будь-якої точки земної поверхні.

С. радіочастот необхідна /п. радиочастот необходимая/ [necessary bandwidth] — мінімальна смуга частот певного класу випромінювання, необхідна для передавання повідомлень із заданою якістю.

С. частот /п. частот/ [frequency b.] — ділянка частот, обмежена нижнім і верхнім краями.

СПЕКТР /спектр/ [spectrum] (від лат. spectrum — образ, видіння) — 1) Сукупність всіх значень будь-якої величини, що характеризує систему або процес. Наприклад: оптичний с., акустичний с., с. електромагнітних

хвиль, с. радіочастот. 2) Кольорова смуга, що утворюється від розкладу білого світла.

С. звуку /с. звука/ [sound s.] — сукупність гармонічних складових звукових хвиль. Основна частота спектра визначає при цьому сприйняту на слух висоту звуку, а набір гармонічних складових — тембр звуку. В с. з. мови наявні форманти — стійкі групи частотних складових, що відповідають певним фонетичним елементам.

С. сигналу /с. сигнала/ [signal s.] — сукупність гармонічних складових сигналу. Для періодичного сигналу будь-якої форми амплітуда кожної спектральної складової характеризує енергію відповідної гармоніки основної частоти сигналу. Чим більша швидкість зміни амплітуди сигналу, тим більше у його спектрі високочастотних складових. Різниця між максимальною і мінімальною частотами с. с., між якими зосереджена основна частина енергії сигналу, називається шириною спектра сигналу. Частоти складових спектра неперіодичного сигналу безперервно змінюються. Тому при спостереженні спектра такого сигналу положення і рівень різноманітних спектральних складових безперервно змінюються і спектр виглядає як суцільний.

СПЕЦИФІКАЦІЯ /спецификация/ [specification] (від лат. species — вид, різновид і ...ficatio, що від facio — роблю) — формалізований опис властивостей, характеристик і функцій об'єкта.

С. ІТ-продукту загальна /с. спецификация Т-продукта общая/ — специфікація, що відображає реалізацію продуктом інформаційних технологій вимог безпеки за допомогою визначення високорівневих специфікацій функцій захисту, що реалізують вимоги безпеки функціональні і вимоги гарантій безпеки "критеріїв Загальних".

С. параметрів /с. параметров/ [parameter s.] — опис типу й способу передавання параметрів, а також обмежень, яким вони повинні задовольняти.

С. програми /с. программы/ [program s.] — точне й повне формулювання задачі, що містить інформацію, необхідну для побудови алгоритму (програми) вирішення цієї задачі.

С. рівня гарантій /с. уровня гарантий/ — специфікації, що визначають заявлений рівень гарантій за-

хисту продукту інформаційних технологій і його відповідність вимогам гарантій безпеки у вигляді подання параметрів технології проектування й створення IT-продукту. Ці параметри повинні бути представлені у форматі, що дозволяє визначити їхню відповідність стандартним вимогам гарантій "критеріїв Загальних".

С. функцій захисту /с. функций защиты/ — специфікації, що описують функціональні можливості засобів захисту продукту інформаційних технологій та заявлені його розробником як такі, що реалізують декларовані вимоги безпеки. Форма подання специфікацій повинна дозволяти визначити відповідність між функціями захисту й вимогами безпеки.

СПИСОК /список/ [list] — 1) Перелік об'єктів. 2) Структура даних, яка являє собою логічно зв'язану послідовність записів — елементів списку. 3) В програмуванні — організація зберігання послідовності даних в пам'яті ЕОМ, яка передбачає послідовне оброблення елементів цієї послідовності, а також динамічну зміну її складу і упорядкування.

С. доступу /с. доступа/ [access control l.] — перелік користувачів і (або) процесів з зазначенням їхніх прав доступу до об'єкта комп'ютерної системи, з яким пов'язаний цей перелік.

С. повноважень /с. полномочий/ [privilege l., profile] — перелік об'єктів з зазначенням прав доступу з боку користувача або процесу, з яким пов'язаний цей перелік.

С. скасованих сертифікатів /с. аннулированных сертификатов/ [Certificate Revocation L. (CRL)] — список, якій містить імена й повноваження користувачів, чиї сертифікати більше не дійсні.

СПІВРОБІТНИК /сотрудник/ — 1) Той, хто працює разом із ким-небудь, допомагає йому в якійсь справі. 2) Особа, що працює в якійсь установі; службовець. 2) В американській розвідці те ж, що і агент.

С. розвідки /с. разведки/ — професіональний (кадровий) співробітник спеціальної служби. Як правило, це військовослужбовець, який пройшов спеціальну розвідувальну підготовку.

С. розвідувальної служби /с. разведывательной службы/ — співробітник розвідки, що дає вказівки агенту, а також здійснює вербування нових агентів в інтересах дорученої йому операції розвідувальної і відповідає за роботу з ними.

СПІВРОБІТНИЦТВО /сотрудничество/ [collaboration] — сумісні праця або дії, сумісна участь в загальній справі.

С. ініціативне /с. инициативное/ — метод добування інформації, який передбачає залучення до співробітництва людей, які шукають контакту з розвідкою іноземної держави або конкурента. Таких людей виявляють органи розвідки шляхом спостереження за співробітниками організації, що мають потрібні джерела (носії) інформації, і виявлення їхньої поведінки, інтересів, моральних якостей, слабостей, зв'язків, фінансового положення. В основі і. с. або зради в переважній більшості випадків лежать корисні і аморальні мотиви, які часто прикриваються міркуваннями про високі цілі.

С. під загрозою /с. под угрозой/ — метод добування інформації, який передбачає залучення до співробітництва людей на основі насильницьких дій зловмисників. Такими діями можуть бути психологічні впливи, загрози особистій безпеці, безпеці рідних, майна, а також переслідування і шантаж, що присилують співробітника (посадову особу) порушувати свої обов'язки щодо нерозголошення таємниці. Якщо в результаті попереднього вивчення особистих якостей співробітника, його життя і поведінки виявляються компрометуючі дані, то можливий шантаж співробітника з метою схилення його до с. п. з. розголошенням компрометуючих відомостей. Іноді для одержання компрометуючих матеріалів для наступного шантажу, для конкретної особи створюють різного роду провокаційні ситуації. Основним способом одержання інформації від с. п. з. може бути випитування.

С. через підкуп /с. через подкуп/ — метод добування інформації, який передбачає залучення до співробітництва через підкуп. Підкуплена людина може стати постійним і ініціативним джерелом інформації.

СПІЧРАЙТЕР /спичрайтер/ [speechwriter] — укладач промов для президентів та інших політичних діячів. Часто для цієї роботи залучаються журналісти, що знають на власному досвіді, якою мовою треба розмовляти з аудиторією за допомогою різних засобів масової інформації, а на нинішньому етапі в першу чергу за допомогою телебачення.

СПОВІЩУВАЧ /извещатель/ — те ж, що сигналізатор.

СПОЖИВАННЯ /потребление/ [consumption] — використання, витрачання для задоволення яких-небудь потреб.

С. інформації /п. информации/ [information c.] — пошук, одержання, передавання і використання інформації.

СПОЖИВАЧ /потребитель/ [consumer] — 1) Особа або організація, що споживає продукцію будь-якого виробництва. 2) Особа або служба, що використовують інформацію або дані розвідувальні, одержані за допомогою розвідки.

С. інформації /п. информации/ [information c.] — 1) Особа або колектив, що отримують чи використовують інформацію у практичній роботі. 2) Людина (користувач), ЕОМ або система, що одержує інформацію з носія або лінії зв'язку для її зберігання, оброблення або передавання.

С. інформації потенційні /п. информации потенциальные/ [potential information users] — споживачі інформації, що в даний момент не включені до системи обслуговування, але потенційно зацікавлені в отриманні матеріалів, що розповсюджуються органом інформаційним.

СПОСІБ /способ/ [method] — певна дія, прийом або система прийомів, яка дає можливість зробити, здійснити що-небудь, досягти чогось.

С. блокування інформації /с. блокирования информации/ — спосіб інформаційної боротьби наступальний, що відноситься до категорії способів інформаційної боротьби силових. Полягає у тому, що на етапі підготовки і в ході бойових дій шляхом виконання комплексу заходів протидії інформаційної повністю або частково припиняється добування (збирання) інформації про обстановку і обмін інформацією в системах управління військами і зброєю противника. Для реалізації цього способу застосовується вогневе, радіоелектронне і інформаційне ураження (придушення) елементів систем управління військами (силами) і зброєю противника.

С. великої брехні /с. большой лжи/ — спосіб маніпулювання свідомістю, що ґрунтується на твердженні, що чим нагліша і неправдоподібніша брехня, тим скоріше в неї повірять, головне — подавати її

максимально серйозно.

С. вимотування противника /с. изматывания/ — спосіб інформаційної боротьби наступальний, який полягає в проведенні комплексу заходів протидії інформаційної з метою примусити противника здійснювати невигідні і марні дії і, як наслідок, вступити в бій з розтраченими ресурсами і пониженою боєздатністю. При цьому можуть проводитися обмежені бойові або відволікаючі дії.

С. відвернення уваги /с. отвлечения внимания/ — спосіб інформаційної боротьби наступальний, який полягає в тому, що на етапі підготовки бойових дій шляхом проведення комплексу заходів протидії інформаційної намагаються створити реальну або удавану загрозу для одного з найбільш уразливих місць противника і тим самим переконати його у своїх намірах діяти на одному з можливих напрямів з метою відволікти головні сили противника на вирішення другорядних завдань.

С. гри в простонародність /с. игры в простонародность/ [plain Folks] —- спосіб навіювання неспецифічного, оснований на спонуканні об'єкта навіювання до ототожнення суб'єкта і поданих ним ідей (понять, суджень) з позитивними цінностями внаслідок "народності" цих ідей або внаслідок належності джерела інформації до так званих "простих людей". Саме тому свої пропагандистські матеріали органи психологічної війни часто подають від імені рядових громадян або військовослужбовців противника.

С. деблокування інформації /с. деблокирования информации/ — спосіб інформаційної боротьби оборонної, який передбачає проведення комплексу заходів захисту інформаційного з метою одержання інформації, що приховується або модифікується противником. При цьому можуть застосовуватися всі можливі методи, сили і засоби, аж до проведення широкомасштабних операцій.

С. дезінтеграції /с. дезинтеграции/ — спосіб інформаційної боротьби наступальний, який використовується для вирішення політичних завдань в міждержавних конфліктах. Реалізація способу полягає в проведенні комплексу заходів протидії інформаційної, що дозволяє нав'язати противнику уяву про необхідність діяти всупереч коаліційним інтересам. З цією метою може використовуватися дезінформування громадської думки, а також формування фальшивих уявлень про воєнно-політичну обстановку у голів

держав, що беруть участь в конфлікті. Крім того, можуть проводитися заходи, що сприяють загостренню реально існуючих або штучно створюваних протиріч у стані ворога з метою понизити його воєнну і економічну могутність.

С. дозування інформації /с. дозирования информации/ — спосіб маніпулювання свідомістю, коли повідомляється тільки частина відомостей, а решта ретельно приховується. Це призводить до того, що картина реальності спотворюється в цю чи іншу сторону, або взагалі стає незрозумілою.

С. емоційного придушення /с. эмоционального подавления/ — спосіб навіювання неспецифічного, який використовується для формування у військовослужбовців противника таких астенічних психічних станів як тривога, депресія, апатія. Прийоми емоційного придушення, що використовуються в практиці психологічної війни, надзвичайно різноманітні. Вибір того чи іншого з них обумовлюється умовами впливу, характером бойових дій, специфікою об'єкта навіювання. Серед них виділяють: емоційне придушення засобами невербального звукового впливу (звуки запису дитячого плачу, похоронної музики, важкої рок-музики, різноманітних дратівливих звуків [крики, завивання сирени, звуки вибухів, свист падаючих бомб]); придушення шляхом демонстрації безглуздості війни; придушення шляхом показу реальності загибелі або каліцтва; придушення шляхом посилання на ті реальні труднощі (брак продовольства, боєприпасів, медикаментів і т. ін.), які зазнає противник (необхідно навіювати, що такі труднощі набули постійного характеру і все більше збільшуються); придушення шляхом апеляції до незадоволених сексуальних потреб військовослужбовців; емоційне придушення шляхом ствердження, що "поки солдат б'ється на фронті, його сім'я терпить в тилу утиски, його близькі залишились без засобів до існування, а жінка змушена займатися проституцією. Фахівцями психологічної війни пропонується ряд рекомендацій з використання с. е. п.: правильний вибір об'єкта впливу (найбільш ефективним є емоційне придушення противника, що знаходиться в оточенні або відступає, терпить різноманітні труднощі, або має низький морально-психологічний потенціал); урахування умов впливу (найбільш піддаються емоційному придушенню деморалізовані військовослужбовці, у яких почуття страху і безвихідності загострені до межі); правильний вибір часу впливу

(на відміну від залякування [див. спосіб залякування], емоційне придушення доцільно використовувати не тільки перед боєм, але і в період між бойовими діями).

С. загальної платформи /с. общей платформы/ [band wagon] — спосіб навіювання неспецифічного, що полягає в спонуканні об'єкта впливу прийняти ідею (судження, оцінку, думку), що міститься в інформації, на основі, що нібито більшість представників даної соціальної групи або військового підрозділу поділяють її. Інша назва — загальний вагон.

С. залякування (ініціювання страху) /с. устрашения (инициирования страха)/ — спосіб навіювання неспецифічного, що полягає у формуванні станів неспокою, депресії або апатії; пробудження почуття страху перед реальною або вигаданою небезпекою, а також перед невідомістю. Кінцева мета залякування — максимальне зниження морально-психологічної стійкості противника, параліч його волі до опору. Залякування доцільно проводити для впливу на противника який: несе великі втрати; знаходиться в оточенні; перейшов до оборони; відступає; зазнає нестачу продовольства, боєприпасів та інших засобів; поступається в чисельності; піддається ураженню від високоточної зброї або зброї масового ураження; терпить поразки в бойових діях. Велике значення має вибір часу залякування. Наприклад, залякування доцільно використовувати відразу після вогневої підготовки, коли ступінь психічної напруги й інтенсивність реакції страху у військовослужбовців противника максимальна. Іншим важливим фактором є вибір оптимальної форми впливу психологічного. В залежності від особливостей конкретної ситуації необхідно використовувати усну пропаганду, радіозасоби (наприклад, входження в бойові мережі противника), друковані засоби і т. ін.

С. замирення /с. умиротворения/ — спосіб інформаційної боротьби наступальний, який застосовується для нав'язування противнику уяви про нейтральну або союзницьку позицію конфронтуючої сторони. Суть способу полягає у проведенні комплексу заходів протидії інформаційної, основною метою яких є створення у противника уяви про те, що здійснюється не підготовка до бойових дій, а планова оперативна (бойова підготовка) або будь-які інші заходи. Противник повинен впевнитися в дружніх або мирних намірах конфронтуючої сторони і втратити пильність. Таємно ж планується і готується напад на нього при

першому зручному випадку.

С. зволікання /с. затягивания времени/ — спосіб маніпулювання свідомістю, який передбачає зволікання з оголошенням по-справжньому важливих фактів до того моменту, коли буде вже пізно будь-що змінити.

С. зворотного удару /с. возвратного удара/ — спосіб маніпулювання свідомістю, суть кого полягає в тому, що вигадану (вигідну для себе) версію цих або інших подій через підставних осіб розповсюджують в засобах масової інформації, нейтральних по відношенню до обох конфліктуючих сторін. Преса противника за звичай повторює цю версію, тому що вона вважається більш "об'єктивною", ніж думки прямих учасників конфлікту.

С. ініціювання агресивних емоційних станів /с. инициирования агрессивных эмоциональных состояний/ — спосіб навіювання неспецифічного, призначений для формування у військовослужбовців противника таких емоцій як підозріливість, недоброзичливість, гнів, ненависть, лють, з метою внесення суперечностей в їхнє середовище. Агресивні емоційні стани виникають по відношенню до певного об'єкта. Їх, звичайно, супроводжують процеси зараження, а також стереотипізації уявлень в створюваному "образі ворога". Ініціюючи такі стани, психологи за мету ставлять внесення розколу в середовищі противника, пробудження там взаємної ворожості на соціальному, етнічному, релігійному або ідеологічному ґрунті. Визначені також основні теми, використання яких в навіюючому впливі дозволяє вносити розкол у таборі противника. Це: розходження у політичних поглядах між громадянами ворожої держави і їхніми союзниками; етнічні, расові і регіональні суперечності; релігійні, політичні або соціальні відмінності; ворожість цивільного населення противника до своїх військовослужбовців; протиріччя між офіцерським складом, унтер-офіцерами (сержантами) і рядовими солдатами; відмінності між комфортними умовами для військовослужбовців у тилу і важкими умовами для особового складу частин на передових позиціях; невдоволеність цивільного населення противника бюрократичною системою влади; протиріччя між панівною елітою й опозиційними політичними партіями (організаціями); несправедливе оподаткування або їхній високий

рівень; забезпеченість продовольством і предметами широкого вжитку вузької групи керівництва на фоні загального дефіциту. Крім того, можна також використовувати історичні факти, що нагадують про те, що країни-союзники конфронтуючої коаліції раніше воювали між собою та інші теми.

С. інсценування /с. инсценировки/ — спосіб інформаційної боротьби наступальний, який полягає в тому, що на етапі підготовки до бойових дій противнику нав'язується уява про наявність удаваної загрози для одного з його уразливих місць, запобігання якій не потребує виділення сил та засобів. Це робиться з метою, щоб противник помітив обман і його пильність була би приспана. При виникненні справжньої загрози він також прийме її як фальшиву і зможе діяти у відповідності до реальної обстановки.

С. інформаційного перевантаження /с. информационной перегрузки/ — спосіб маніпулювання свідомістю, коли повідомляється дуже велика кількість інформації, основну частину якої складають абстрактні розмірковування, непотрібні подробиці, різноманітні дурниці і т.ін. "сміття". В результаті об'єкт не може розібратися у справжній суті проблеми.

С. інформаційної боротьби /с. информационной борьбы/ — порядок і прийоми застосування сил і засобів інформаційної боротьби для захоплення і утримання інформаційної переваги над противником при підготовці і проведенні бойових дій. С. і. б. включають: вид і послідовність впливів інформаційних на противника; об'єкти впливу; склад сил і засобів, що виділяються для ведення інформаційної боротьби, їхнє оперативне шикування (бойовий порядок). Всі с. і. б. можна поділити на три основні категорії: силові, інтелектуальні і комбіновані, а також за аналогією із збройною боротьбою виділити дві основні групи способів: наступальні і оборонні.

С. інформаційної боротьби інтелектуальні /с. информационной борьбы интеллектуальные/ — категорія способів інформаційної боротьби, що реалізують рефлексне управління противником. Застосування таких способів дозволяє досягти переваги інформаційної в якості інформації, що використовується для управління військами (силами).

С. інформаційної боротьби комбіновані /с. информационной борьбы комбинированные/ — катего-

рія способів інформаційної боротьби, які забезпечують досягнення переваги інформаційної як за кількістю, так і за якістю інформації.

С. інформаційної боротьби наступальні /наступательные с. информационной борьбы/ — вид способів інформаційної боротьби, що реалізують блокування інформації, відвернення уваги, сковування сил противника, вимотування противника, інсценування, дезінтеграції, замирення, залякування противника, провокування противника, перевантаження противника, навіювання на противника і тиск на противника.

С. інформаційної боротьби оборонні /с. информационной борьбы оборонительные/ — вид способів інформаційної боротьби, що реалізують деблокування та ототожнення інформації.

С. інформаційної боротьби силові /с. информационной борьбы силовые/ — категорія способів інформаційної боротьби, які засновані на ураженні об'єктів інформаційної боротьби різноманітними видами зброї (звичайної, радіоелектронної, інформаційної). Застосування с. і. б. с. дозволяє досягти переваги інформаційної в кількості інформації, необхідної для вирішення завдань управління військами (силами).

С. навіювання на противника /с. внушения противнику/ — спосіб інформаційної боротьби наступальний, який полягає у формуванні і наступному використанні інформаційного стереотипу конфронтуючої сторони. Для цього на етапі підготовки і в ході бойових дій шляхом проведення комплексу заходів протидії інформаційної до відома противника доводиться інформація, яка має юридичну, моральну, ідеологічну або іншу силу і спонукає його до здійснення будь-яких дій, вигідних конфронтуючій стороні.

С. ототожнення інформації /с. отождествления информации/ — спосіб інформаційної боротьби оборонний, що передбачає проведення комплексу заходів захисту інформаційного, які забезпечують збирання і співставлення інформації про один і той же факт (явище) від різноманітних джерел, що дозволяє виявити і блокувати дезінформацію, яка розповсюджується противником.

С. перевантаження противника /с. перегрузки противника/ — спосіб інформаційної боротьби наступальний, який полягає в тому, щоб на етапі підготовки і в ході бойових дій довести до противника

таку кількість суперечливої інформації, яка перевантажує його систему управління і змушує приймати і реалізовувати рішення в умовах підвищеної невизначеності обстановки.

С. перенесення /с. переноса/ [transfer] — спосіб навіювання неспецифічного, суть якого — викликати через образ, що подається, (поняття, лозунг, ідею) асоціацію з будь-ким або будь-чим, що має в очах об'єкта незаперечний престиж (цінність), щоб зробити зміст дії прийнятним. Наприклад, фахівці війни психологічної використовують національно й традиційно значимі для противника образи, що викликають у свідомості населення й військовослужбовців позитивне відношення. Часто використовується також негативне перенесення шляхом пробудження асоціацій з негативними (для об'єкта) образами, поняттями й ідеями.

С. перетасовки фактів /с. перетасовки фактов/ [fact stacking] — спосіб навіювання неспецифічного, що полягає в тенденційному відбиранні тільки позитивних або тільки негативних фактів для доказу справедливості позитивної або негативної оцінки будь-якої ідеї (судження, поняття, явища). Об'єкту впливу психологічного фахівці війни психологічної подають в певній послідовності такі факти, осмислення яких неминуче веде до необхідних їм висновків.

С. приклеювання ярликів /с. приклеивания ярлыков/ [name calling] — спосіб навіювання неспецифічного, призначений для того, щоб зганьбити будь-яку ідею, особистість або явище образливими епітетами або метафорами, які викликають негативне відношення. Досвід війни психологічної свідчить про достатньо широке використання цього способу. Найчастіше його застосовують по відношенню до політичних діячів, представників вищого командування та інших загальновідомих осіб. Проте "працює" він тільки в тому випадку, коли війна вже принесла значні страждання населенню й військам противника, а їхній моральний стан є низьким.

С. провокування противника /с. провоцирования противника/ — спосіб інформаційної боротьби наступальний, призначений для спонукання противника до здійснення будь-яких дій, корисних протилежній

стороні.

С. свідчення /с. свидетельства/ [testimonial] — спосіб навіювання неспецифічного, що полягає в цитуванні висловлювань особистості, яку поважає або, навпаки, ненавидить об'єкт впливу. Висловлювання, як правило, носить позитивну оцінку ідеї (поняття, судження), що подається, і має за мету спонукати об'єкт впливу до прийняття нав'язуваної йому позитивної або негативної думки з цього приводу. Інша назва — посилання на авторитети. С. с. використовують як елемент маніпулювання свідомістю противника.

С. своєчасної брехні /с. своевременной лжи/ — спосіб маніпулювання свідомістю, що полягає в повідомленні цілком фальшивої, але надзвичайно очікуваної в даний момент інформації. Чим більше зміст повідомлення відповідає настрою об'єкта, тим ефективніший її результат. Потім обман розкривається, але за цей час гострота ситуації спадає, або певний процес приймає необоротний характер.

С. сковування сил противника /с. сковывания противника/ — різновид способу відвернення уваги. При його застосуванні у противника створюється переконання в наявності загрози для одного з його уразливих місць, запобігання якій потребує виділення частини сил та засобів.

С. сяючого узагальнення /с. сияющего обобщения/ [glittering generality] — спосіб навіювання неспецифічного, що полягає в позначенні конкретної ідеї або особистості узагальнюючим родовим іменем, що має позитивне емоційне забарвлення. Мета с. с. у. — спонукати об'єкт впливу прийняти й схвалити поняття й судження, що подаються. Цей спосіб дозволяє приховувати негативні наслідки засвоєння змісту навіювання і тим самим не провокувати негативні асоціації. Прийом широко застосовується в практиці війни психологічної, він фактично є аналогом обману.

С. тиску на противника /с. давления на противника/ — спосіб інформаційної боротьби наступальний, заснований на доведенні до суспільної думки відомостей, які порочать противника, та змушують державні, міждержавні, суспільні та інші організації здійснювати дії, що утрудняють виконання його замислів.

СПОСТЕРЕЖЕННЯ /наблюдение/ [observation] — спосіб добування інформації дистанційного на основі одержання і аналізу зображення об'єкта спостереження (документа, людини, предмета, простору і т.

ін.). При с. добуваються, в основному, ознаки об'єктів видові. Проте можливе добування інформації семантичної, якщо об'єкт с. являє собою документ, схему, креслення і т.ін. Об'єкти можуть спостерігатися безпосередньо — очима або за допомогою технічних засобів. Розрізняють наступні способи с. з використанням технічних засобів: спостереження візуально-оптичне; спостереження в інфрачервоному діапазоні; спостереження з консервацією зображення; спостереження телевізійне; спостереження лазерне; спостереження радіолокаційне; спостереження радіотеплолокаційне, спостереження гідролокаційне.

С. в інфрачервоному діапазоні /н. в инфракрасном диапазоне/ — спостереження у інфрачервоній частині оптичного діапазону за допомогою технічних засобів, що перетворюють невидиме зображення у видиме на основі використання проникної здатності випромінювання інфрачервоного (приладів нічного бачення, тепловізорів).

С. в оптичному діапазоні /н. в оптическом диапазоне/ — спосіб добування інформації за допомогою засобів спостереження в оптичному діапазоні шляхом візуального, візуально-оптичного, телевізійного спостереження, фото-кінозйомки, спостереження з використанням приладів нічного бачення і тепловізорів.

С. візуально-оптичне /н. визуально-оптическое/ — спостереження у видимій частині оптичного діапазону за допомогою різноманітних засобів візуально-оптичного спостереження (приладів візуально-оптичних) — від спеціальних телескопів до ендоскопів, що забезпечують спостереження прихованих об'єктів через маленькі отвори або щілини.

С. з консервацією зображення /н. с консервацией изображения/ — спостереження в оптичному (видимому і інфрачервоному) діапазоні із збереженням зображення для наступного аналізу. Для консервації (збереження) статичного зображення об'єкта його фотографують, для консервації рухомих об'єктів здійснюють кіно- або відеозйомку.

С. зовнішнє /н. наружное/ — вид спостереження за іноземними агентами і особами, що підозрюються у шпіонажі.

С. лазерне /н. лазерное/ [laser о.] — спостереження в оптичному (видимому і інфрачервоному) діапа-

зоні за допомогою оптичних локаторів, які дозволяють визначати з високою точністю відстань до об'єкта і його координати.

С. радіолокаційне /н. радиолокационное/ [radar o.] — спостереження в радіочастотному діапазоні електромагнітних хвиль за допомогою засобів радіолокації. Дозволяє одержувати зображення об'єкта в будь-які години доби і в несприятливих кліматичних умовах.

С. радіотеплолокаційне /н. радиотеплолокационное/ — спостереження в радіочастотному діапазоні електромагнітних хвиль за допомогою засобів радіотеплолокації. Дозволяє одержувати зображення об'єкта, що відповідає розподілу температури на його поверхні.

С. телевізійне /н. телевизионное/ [television o.] — дистанційне спостереження рухомих об'єктів в оптичному (видимому і інфрачервоному) діапазоні за допомогою засобів телевізійного спостереження.

СПОСТЕРЕЖНІСТЬ /наблюдаемость/ [accountability] — властивість системи (системи комп'ютерної), що дозволяє фіксувати діяльність користувачів і процесів, використання об'єктів пасивних, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання відповідальності за певні дії.

СПОТВОРЕННЯ /искажение/ [distortion] — 1) Представлення в хибному, неправильному вигляді. 2) Неправильність, помилка.

С. нелінійні /и. нелинейные/ [non-linear d.] — спотворення сигналу, що проявляються у появі в частотному спектрі вихідного сигналу додаткових складових, які відсутні у вхідному сигналі. С. н. викликають елементи радіоприймача, що мають нелінійну залежність між входом і виходом. Вони виникають при перевищенні відношення значень максимальної і мінімальної напруг сигналу на вході приймача його динамічного діапазону. С. н. призводять до зміни інформаційних параметрів сигналу на вході демодулятора і, як наслідок, до спотворення інформації після демодуляції.

С. фазові /и. фазовые/ [phase d.] — спотворення сигналу, що виникають із-за порушення фазових співвідношень між окремими спектральними складовими сигналу при проходженні його колами тракту

приймача.

С. частотні /и. частотные/ [frequency d.] — спотворення сигналу, що викликаються придушенням або зміною складових спектра вхідного сигналу радіоприймача. Із-за с. ч. сигнал на вході демодулятора може набувати форми, відмінної від вхідної.

СПРИЙНЯТЛИВІСТЬ /восприимчивость/ [susceptibility] — здатність реагування на будь-які сигнали, завади тощо.

С. ЕОМ до завад /в. ЭВМ к помехам/ [noise s.] — здатність ЕОМ знижувати якість функціонування при дії на неї завад.

СПРИЙНЯТТЯ /восприятие/ [perception] — процес відображення у свідомості людини предметів та явищ об'єктивного світу, що діють у даний момент на органи чуття, ставлення до чого-небудь, реагування на щось певним чином.

С. інформації /в. информации/ [information s.] — процес формування в органі керування уявлення про обстановку, включаючи її кількісні і якісні параметри. Найбільш суттєві характеристики при цьому — розпізнавальні ознаки істинних і неправдивих елементів обстановки. Ступінь відповідності уявлень органу керування про ці характеристики їхнім вихідним величинам створює передумови для виникнення різноманітних ситуацій боротьби інформаційної. Ці передумови реалізуються в залежності від того, наскільки інформація, що поступає, співвідноситься з образами істинних і неправдивих елементів обстановки, які зберігаються в кадастрі інформаційному. Різноманітність ситуацій інформаційної боротьби буде визначатися ступенем відповідності апріорної і поточної інформації про обстановку. Оцінка ступеня такої відповідності повинна проводитися на моделі прийняття органом керування рішення інформаційного.

С. міжгрупове /в. межгрупповое/ — процеси сприйняття соціального, в яких як суб'єктом, так і об'єктом сприйняття виступають групи соціальні або спільності. Специфіка с. м. полягає: в об'єднанні індивідуальних уявлень в деяке ціле, яке якісно відмінне від елементів, що його складають; в тому, якщо с. м. один раз склалося, то воно слабо змінюється під зовнішнім впливом; в обмеженому, спрощеному і схематичному

діапазоні варіантів сприйняття й оцінки іншої групи. С. м. характеризується стереотипністю, суцільністю пізнавальних і емоційних компонентів, афективною забарвленістю (див. афект), різко вираженою оцінною спрямованістю. Саме тому воно визначається упередженістю, а с. м. завжди мають помилки (спотворення) відносно їхньої істинності, що є психологічним підґрунтям ефекту міжгрупової дискримінації.

С. міжособистістне /в. межличностное/ — сприйняття, розуміння й оцінка людини людиною (одними людьми інших людей). Специфіка с. м. у великому ступені упередженості, що знаходить свій прояв в суцільності пізнавальних і емоційних компонентів. В процесі с. м. виникає ряд психологічних ефектів, серед яких ефекти новизни, первинності, стереотипності, ореолу.

С. навколишнього світу (перцепція) /в. окружающего мира (перцепция)/ — цілісне відображення предметів, ситуацій і подій, що виникає внаслідок безпосереднього впливу подразників на органи чуття людини. Сприйняття являє собою комплексний процес, який включає: відображення стимулу й ситуації; їхню реєстрацію; інтерпретацію сприйнятого; відповідну реакцію на сприйняте. Будь-який акт сприйняття зовнішньої інформації здійснюється у формі конкретних образів, які в більшій або меншій мірі зв'язані з іншими психічними пізнавальними процесами — мисленням, пам'яттю, увагою — і спрямовуються мотивацією, мають певне емоційне забарвлення. При організації подавання інформації, необхідно завжди враховувати емоційний настрій об'єкта й здатність інформації, що повідомляється, викликати саме ті переживання, які загострюють сприйняття її (інтерес, цікавість, здивування). Інформація повинна організовуватися й подаватися таким чином, щоб сприяти розрядці емоційної напруги, що виникає у об'єкта в процесі впливу психологічного. Це формує його довіру до суб'єкта, що проявляється в подальшому у формі готовності до одержання і засвоєння нових подібних повідомлень. Розрізняють сприйняття, адекватне реальності та ілюзорне сприйняття.

С. психологічного впливу /в. психологического влияния/ — сприйняття інформації об'єктом впливу психологічного. Ефективність с. п. в. в першу чергу залежить від одного з ключових психічних процесів — сприйняття навколишнього світу, а також від сприйняття соціального. Розроблено ряд рекомендацій, які

дозволяють підвищити ефективність с. п. в.: психологічний вплив повинен організовуватися відповідно до закономірностей сприйняття і бути логічно продуманим, тоді він як би веде думку об'єкта впливу за собою, сприяє формуванню у нього необхідних установок і стереотипів; психологічний вплив доцільно будувати у вигляді ланцюжка — стимули й асоціації, тезиси й аргументи, причини й наслідки, в його змісті слід іти від старого до нового, від відомого до невідомого; необхідно враховувати, які конкретні елементи психологічного впливу в більшій мірі привертають увагу, абстрактні міркування слід чергувати з конкретними фактами, прикладами, ілюстраціями; яскраві, різноманітні, переконливі психологічні впливи дозволяють краще утримувати увагу об'єкта і ефективно впливати на нього; слід приймати заходи усунення всіх можливих джерел відволікання уваги об'єкта психологічного впливу.

С. соціальне /в. социальное/ — сукупність процесів сприйняття міжособистістного і міжгрупового. Те ж, що перцепція соціальна.

СПУФІНГ (ПІДРОБКА) /спуфинг (подделка)/ [spoofing] — процес, в ході якого відправник підроблює свої початкові дані, щоб можна було подумати, що пакет приходить з будь-якого іншого місця. Також називається підробка адреси.

СТАНДАРТ /стандарт/ [standard, norm] (англ. standard) — 1) Норма, зразок, мірило. 2) Прийнятий організацією відповідної компетенції тип виробів, що відповідає певним вимогам за якістю, хімічним складом, фізичними властивостями, вагою, розміром, об'ємом тощо. 3) Нормативно-технічний документ, який регламентує вимоги і правила до виробів, технологічних процесів і прийнятий відповідної компетенції організацією як офіційний документ.

С. ANSI /с. ANSI/ [s. ANSI] — стандарти забезпечення захисту, розроблені Американським національним інститутом стандартів [American National Standards Institute (ANSI)] і присвячені криптографічним алгоритмам та їхньому застосуванню в банківських системах.

С. ANSI X3.106 /с. ANSI X3.106/ [s. ANSI X3.106] — стандарт ANSI, що описує види застосування

алгоритму стандарту шифрування DES.

С. ANSI X3.92 /с. ANSI X3.92/ [s. ANSI X3.92] — стандарт ANSI, що специфікує алгоритм стандарту шифрування DES, який в рамках цього стандарту представляється як алгоритм шифрування даних [Data Encryption Algorithm (DEA)].

С. ANSI X9.17 /с. ANSI X9.17/ [s. ANSI X9.17] — стандарт ANSI, заснований на стандарті ISO 8732 і присвячений процедурам керування ключами, а також засобам розподілу й захисту ключів стосовно банківських систем. В ньому знайшли відображення специфічні аспекти використання ключів, такі як лічильники ключів, перетворення ключів і підтвердження автентичності ключів. Засоби розподілу ключів, представлені в даному стандарті, побудовані за принципом "точка-точка" або використовують третю сторону (KDC або KTC).

С. ANSI X9.19 /с. ANSI X9.19/ [s. ANSI X9.19] — стандарт ANSI, присвячений питанням використання алгоритму стандарту шифрування DES для генерації MAC в конкретних типах банківських систем.

С. ANSI X9.23 /с. ANSI X9.23/ [s. ANSI X9.23] — стандарт ANSI, який описує формати подання даних при використанні алгоритму стандарту шифрування DES у банківських системах, включаючи поля прапорців, поля доданих даних (набивки) і методи оброблення даних, які одержують із каналів зв'язку.

С. ANSI X9.24 /с. ANSI X9.24/ [s. ANSI X9.24] — стандарт ANSI, що описує методи керування ключами, автентифікацію (заснований на алгоритмі стандарту шифрування DES) і шифрування персонального ідентифікаційного номера, ключів та інших даних, а також керівні принципи захисту ключів на всіх етапах життєвого циклу.

С. ANSI X9.26 /с. ANSI X9.2s51086/ [s. ANSI X9.26] — стандарт ANSI, що описує два основних класи автентифікації користувача, яка необхідна для контролю доступу. Перший клас реалізується на основі використання паролів. Другий — на основі використання симетричних алгоритмів шифрування і попередньо розподілених секретних ключів.

С. ANSI X9.28 /с. ANSI X9.28/ [s. ANSI X9.28] — стандарт ANSI, який є продовженням стандарту

ANSI X9.17 і описує процедури розподілу ключів між користувачами, які не мають між собою і третьою стороною попередньо розподіленої ключової інформації.

C. ANSI X9.30 /c. ANSI X9.30/ [s. ANSI X9.30] — стандарт ANSI, що описує асиметричні алгоритми: в ANSI X9.30-1 — DSA, а в ANSI X9.30 — SHA.

C. ANSI X9.31 /c. ANSI X9.31/ [s. ANSI X9.31] — стандарт ANSI, що описує алгоритм генерації й перевірки підпису електронного цифрового на основі використання алгоритму RSA.

C. ANSI X9.42 /c. ANSI X9.42/ [s. ANSI X9.42] — стандарт ANSI, що описує декілька варіантів застосування алгоритму неавтентифікаційного обміну ключами типу Діфі-Хелмана, який забезпечує розподіл симетричних ключів.

C. ANSI X9.45 /c. ANSI X9.45/ [s. ANSI X9.45] — стандарт ANSI, присвячений застосуванню автентифікаційних сертифікатів відкритих ключів.

C. ANSI X9.52 /c. ANSI X9.52/ [s. ANSI X9.52] — стандарт ANSI, що аналогічно стандарту ISO 8372, описує застосування Triple DES і чотирьох режимів його використання.

C. ANSI X9.55 /c. ANSI X9.55/ [s. ANSI X9.55] — стандарт ANSI, що розглядає формат і застосування сертифікатів відповідно до рекомендацій MCE X.509 версії 3.

C. ANSI X9.57 /c. ANSI X9.57/ [s. ANSI X9.57] — стандарт ANSI, що описує керування сертифікатами у сфері електронної комерції.

C. ANSI X9.8 /c. ANSI X9.8/ [s. ANSI X9.8] — стандарт ANSI, присвячений питанням безпеки й керування номером ідентифікаційним персональним.

C. ANSI X9.9 /c. ANSI X9.9/ [s. ANSI X9.9] — стандарт ANSI, який описує застосування MAC на основі використання алгоритму стандарту шифрування DES (у режимах CBC і CFB із блоками довжиною 64 біта) для широкого кола банківських систем.

C. EMV /c. EMV/ [EMV] — Europay-MasterCard-Visa стандарт, розроблений провідними міжнародни-

ми платіжними системами для забезпечення сумісності рішень для фінансових транзакцій.

С. FIPS /с. FIPS/ [Federal Information Protection S. (FIPS)] — Федеральні стандарти забезпечення захисту інформації, що є державними стандартами США.

С. FIPS 112 /с. FIPS 112/ [FIPS 112] — стандарт FIPS, що описує керівні принципи використання паролів та керування ними.

С. FIPS 113 /с. FIPS 113/ [FIPS 113] — стандарт FIPS, що описує алгоритм генерації MAC на основі використання алгоритму стандарту шифрування DES.

С. FIPS 140 /с. FIPS 140/ [FIPS 140] — стандарт FIPS, що описує вимоги безпеки при розробці й застосуванні криптографічних модулів, виконаних як апаратно, так і програмно. Є стандартом для відновлення ключа, який має апаратну реалізацію.

С. FIPS 171 /с. FIPS 171/ [FIPS 171] — стандарт FIPS, що описує засоби розподілу ключів при використанні в державних структурах.

С. FIPS 180 /с. FIPS 180/ [FIPS 180] — стандарт FIPS, присвячений алгоритму SHA, а 180-1 — SHA-1.

С. FIPS 185 /с. FIPS 185/ [FIPS 185] — стандарт FIPS, що описує процедуру депонування ключів і описує алгоритм симетричного шифрування SkipJack.

С. FIPS 186 /с. FIPS 186/ [FIPS 186] — стандарт FIPS, що описує DSA при застосуванні з SHA.

С. FIPS 46 /с. FIPS 46/ [FIPS 46] — стандарт FIPS, що описує керівні принципи застосування й використання алгоритму стандарту шифрування DES.

С. FIPS 81 /с. FIPS 81/ [FIPS 81] — стандарт FIPS, що описує чотири основних типи використання алгоритму стандарту шифрування DES.

С. ISO /с. ISO/ [s. ISO] — стандарти забезпечення захисту, представлені серіями ISO і ISO/IEC, які випущені у світ Міжнародною організацією зі стандартизації [International Organization for Standardization (ISO)] і Міжнародною електротехнічною комісією [International Electrotechnical Commission (IEC)].

С. ISO 10126 /с. ISO 10126/ [s. ISO 10126] — стандарт ISO, що описує методи забезпечення конфіден-

ційності фінансових повідомлень і є аналогом стандарту ANSI X9.23. Частина 10126-1 присвячена основним методам і принципам, а частина 10126-2 стосується питань використання DES для цих цілей.

С. ISO 10202 /с. ISO 10202/ [s. ISO 10202] — стандарт ISO, що описує аспекти безпеки при застосуванні смарт-карток у фінансових транзакціях.

С. ISO 11131 /с. ISO 11131/ [international s. ISO 11131] — стандарт ISO, що описує автентифікацію, засновану на застосуванні ЕЦП, і є міжнародним аналогом стандарту ANSI X9.26.

С. ISO 11166 /с. ISO 11166/ [international s. ISO 11166] — стандарт ISO, що описує асиметричні механізми розподілу симетричних ключів. Частина 11166-1 присвячена основним принципам і процедурам розподілу ключів і форматам надання ключів, а також сертифікації ключової інформації. Частина 11166-2 описує застосування RSA для шифрування й генерації ЕЦП.

С. ISO 11568 /с. ISO 11568/ [s. ISO 11568] — стандарт ISO, що описує засоби й процедури керування ключами при фінансових операціях для симетричних і асиметричних алгоритмів.

С. ISO 7498-2 /с. ISO 7498-2/ [s. ISO 7498-2] — стандарт ISO, присвячений опису архітектури по відношенню до моделі взаємодії відкритих систем, включаючи опис розташування механізмів і служб безпеки на рівнях моделі. В основу стандарту покладені рекомендації МСЕ X.800.

С. ISO 8372 /с. ISO 8372/ [international s. ISO 8372] — стандарт ISO, що описує режими блочного шифрування: режим електронної книги (ECB); режим зчеплення блоків (CBC); режим із зворотним зв'язком по шифртексту (CFB); режим із зворотним зв'язком по виходу (OFB). Дані режими спочатку були представлені в стандарті FIPS 81 (1980 р.) і стандарті ANSI X.3 106 (1981 р.), в той час як ISO 8372 був уперше опублікований у 1987 р.

С. ISO 8730 /с. ISO 8730/ [s. ISO 8730] — стандарт ISO, який разом із стандартом ISO 8731 описує процедуру використання алгоритмів генерації MAC у банківських системах і є міжнародним аналогом стандарту ANSI X9.9. В ньому вводяться незалежні від алгоритмів методи й вимоги використання MAC, включаючи формати подання даних, а також спосіб, за допомогою якого даний стандарт може застосову-

ватися до вибраного алгоритму.

С. ISO 8731 /с. ISO 8731/ [s. ISO 8731] — стандарт ISO, що описує безпосередні алгоритми генерації MAC. В частині ISO 8731-1 описано використання DES у режимі CBC, а частина ISO 8731-2 присвячена алгоритму MAA.

С. ISO 8732 /с. ISO 8732/ [s. ISO 8732] — стандарт ISO, що описує керування ключами в банківських системах і є аналогом стандарту ANSI X9.17.

С. ISO 9564 /с. ISO 9564/ [s. ISO 9564] — стандарт ISO, що описує методи керування й забезпечення безпеки персонального ідентифікаційного номера. В частині ISO 9564-1 розкриваються принципи й засоби захисту PIH протягом його життєвого циклу, які дозволяють зберігати його в таємниці від зловмисників, а частина ISO 9564-2 присвячена використанню алгоритмів шифрування для захисту PIH.

С. ISO 9807 /с. ISO 9807/ [s. ISO 9807] — стандарт ISO, що описує процедури автентифікації повідомлень стосовно банківських систем і є аналогом стандарту ANSI X9.19.

С. ISO/IEC 11770 /с. ISO/IEC 11770/ [s. ISO/IEC 11770] — стандарт ISO, в якому розглядаються питання керування ключами й механізми розподілу ключів. Частина 11770-1 описує основи керування ключами і поняття циклу життя ключів, а також вимоги із захисту ключів і ролі третьої сторони в розподілі ключів. Частина 11770-2 описує механізми розподілу ключів, засновані на симетричних алгоритмах і протоколах, подібних Kerberos і Otway-Rees. В частині 11770-3 розглядаються механізми розподілу ключів, засновані на асиметричних алгоритмах, які, у свою чергу, поділяються на угоди про ключі й протоколи передавання ключів

С. ISO/IEC 13888 /с. ISO/IEC 13888/ [s. ISO/IEC 13888] — стандарт ISO, присвячений проблемі ненегативності ряду факторів, зв'язаних із процесом передавання повідомлень. В ньому також приводяться механізми, що дозволять випадки, зв'язані з відмовою від факту приймання повідомлення, а також механізми ненегативності, зв'язані з використанням довіреної третьої сторони.

С. ISO/IEC 14888 /с. ISO/IEC 14888/ [s. ISO/IEC 14888] — стандарт ISO, присвячений побудові схем

підписів електронних цифрових. Частина 14888-1 знайомить із загальноприйнятими визначеннями і моделями побудови схеми ЕЦП. В частині 14888-2 розглядаються схеми ЕЦП, в яких ключ перевірки підпису є результатом загальнодоступної функції від інформації, яка ідентифікує особу, що підписує. Частина 14888-3 присвячена розподілу відкритих ключів за допомогою сертифікатів відкритих ключів.

C. ISO/IEC 10116 /c. ISO/IEC 10116/ [s. ISO/IEC 10116] — стандарт ISO, який аналогічно міжнародному стандартові ISO 8372, описує чотири типи використання алгоритмів блочного шифрування, проте даний стандарт специфікує операції для загального випадку побудови блочного шифрування, де довжина блока має n біт.

C. ISO/IEC 10118 /c. ISO/IEC 10118/ [s. ISO/IEC 10118] — стандарт ISO, який описує алгоритми генерації хеш-функції. Складається з декількох частин. В 10118-1 представлені основні визначення і вимоги, частина 10118-2 описує дві конструкції хеш-функцій, засновані на алгоритмах блочного шифрування. Частина 10118-3 містить алгоритми SHA-1, RIPEMD-128 і RIPEMD-160, а частина 10118-4 — опис алгоритмів MASH-1 MASH-2.

C. ISO/IEC 10181 (X.810-X.816) /c. ISO/IEC 10181/ [s. ISO/IEC 10181] — стандарт ISO. Складається з опису семи архітектур безпеки, а саме: архітектура контролю доступу; архітектура забезпечення негативності і розбору конфліктних ситуацій; архітектура забезпечення цілісності; архітектура забезпечення конфіденційності; архітектура аудита систем безпеки. Див. також рекомендації МСЕ X.810-X.816.

C. ISO/IEC 15408 /c. ISO/IEC 15408/ [s. ISO/IEC 15480] — стандарт ISO, що представляє собою версію 2.1 критеріїв Загальних безпеки інформаційних технологій. Затверджений у серпні 1999 року.

C. ISO/IEC 17799 /c. ISO/IEC 17799/ [s. ISO/IEC 17799] — стандарт BS 7799, розроблений Британський Інститут Стандартів (BSI) та признаний у 2000 р. міжнародним під назвою “International Standard ISO/IEC 17799. Information technology - Code of practice for information security management”. Він описує модель системи менеджменту, яка визначає загальну організацію, класифікацію даних, системи доступу, напрямки планування, відповідальність співробітників, використання оцінки ризику і т.ін. в контексті ін-

формаційної безпеки. У процесі впровадження стандарту створюється так звана система менеджменту інформаційної безпеки, мета якої скорочення матеріальних втрат, зв'язаних з порушенням інформаційної безпеки. Основна ідея стандарту — допомогти комерційним та державним господарським організаціям вирішити достатньо складне завдання: не тільки забезпечити надійний захист інформації, але також організувати ефективний доступ до даних та нормальну роботу з ними.

С. ISO/IEC 9694-8 /с. ISO/IEC 9694-8/ [s. ISO/IEC 9694-8] — стандарт ISO, присвячений двом типам автентифікації — простої і сильної. Представлена сильна автентифікація складається з двох або трьох повідомлень, що передаються, і основана на використанні підпису електронного цифрового і параметрів, що залежать від часу. У стандарті також описується процедура автентичного розподілу відкритих ключів на основі сертифікатів у форматі рекомендацій МСЕ X.509.

С. ISO/IEC 9796 /с. ISO/IEC 9796/ [international s. ISO/IEC 9796] — стандарт ISO, який визначає уніфікований механізм, що реалізує підпис електронний цифровий з відновленням повідомлення. Основна частина стандарту присвячена надлишковим схемам, призначеним у загальному випадку для використання із широким класом схем ЕЦП.

С. ISO/IEC 9797 /с. ISO/IEC 9797/ [s. ISO/IEC 9797] — стандарт ISO, що описує алгоритм генерації кодів автентифікації повідомлень (MAC), оснований на використанні алгоритму блочного шифрування.

С. ISO/IEC 9798 /с. ISO/IEC 9798/ [s. ISO/IEC 9798] — стандарт ISO. Складається з п'яти частин. В першій частині (9798-1) описується механізм автентифікації користувачів, заснований на використанні симетричного алгоритму шифрування (9798-2), алгоритму генерації підпису електронного цифрового з симетричними ключами (9798-3), криптографічної функції перевірки цілісності або MAC (9798-4), деяких виконавчих механізмів (9798-5).

С. ISO/IEC 9979 /с. ISO/IEC 9979/ [international s. ISO/IEC 9979] — стандарт ISO, який описує процедури, що дозволяють деяким учасникам зареєструвати алгоритм шифрування в органі реєстрації ISO. Результатом є призначення унікального ідентифікатора алгоритму, що використовується в процедурах

взаємодії й вироблення контексту безпеки.

С. ГОСТ Р ИСО/МЭК 15408-2001 — державний стандарт забезпечення захисту Російської федерації, що аналогом міжнародного стандарту ISO/IEC 15408. Повне найменування — "ГОСТ Р ИСО/МЭК 15408-2001. Информационная технология. Методы и средства обеспечения безопасности критерии оценки безопасности информационных технологий".

С. ГОСТ 34.310-95 /с. ГОСТ 34.310-95/ — міждержавний стандарт забезпечення захисту, за який прийнято державний стандарт Російської федерації ГОСТ Р 34.10-94.

С. ГОСТ 34.311-95 /с. ГОСТ 34.311-95/ — міждержавний стандарт забезпечення захисту, за який прийнято державний стандарт Російської федерації ГОСТ Р 34.11-94.

С. ГОСТ Р 34.10-94 /с. ГОСТ Р 34.10-94/ — державний стандарт забезпечення захисту Російської федерації, що встановлює процедури вироблення і перевірки підпису електронного цифрового. Повне найменування — "ГОСТ Р 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметрического криптографического алгоритма". Є модернізованим варіантом алгоритму підпису електронного цифрового з відкритими ключами Ель-Гамаля. Довжина ЕЦП — 512 біт.

С. ГОСТ Р 34.11-94 /с. ГОСТ Р 34.11-94/ — державний стандарт забезпечення захисту Російської федерації, що визначає алгоритм і процедуру обчислення хеш-функції для будь-якої послідовності двійкових символів, які застосовуються в криптографічних методах оброблення і захисту інформації, в тому числі для реалізації процедур підпису електронного цифрового. Повне найменування — "ГОСТ Р 34.10-94. Информационная технология. Криптографическая защита информации. Функция хеширования". Довжина хеш-функції — 256 біт.

С. ГОСТ Р 50739-95 /с. ГОСТ Р 50739-95/ — Державний стандарт забезпечення захисту Російської федерації, що встановлює єдині функціональні вимоги до захисту засобів обчислювальної техніки від несанкціонованого доступу до інформації, до складу документації на ці засоби, а також номенклатуру показників

захищеності ЗОТ, які описуються сукупністю вимог до захисту і визначають класифікацію ЗОТ за рівнем захищеності від НСД до інформації. Повне найменування — "ГОСТ Р 507390-95. Средства вычислительной техники. Защита информации от несанкционированного доступа к информации. Общие технические требования".

С. ГОСТ Р 50922-96 /с. ГОСТ Р 50922-96/ — Державний стандарт забезпечення захисту Російської федерації, що встановлює основні терміни і їхнє визначення в галузі захисту інформації. Повне найменування — "ГОСТ Р 50922-96. Защита информации. Основные термины и определения".

С. ДСТУ 3396.0-96 — державний стандарт забезпечення захисту України, що визначає основні положення технічного захисту інформації в Україні. Повне найменування — "ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення".

С. ДСТУ 3396.1-96 — державний стандарт забезпечення захисту України, що визначає порядок проведення робіт з технічного захисту інформації в Україні. Повне найменування — "ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт".

С. ДСТУ 3396.2-97 — державний стандарт забезпечення захисту України, що визначає основні терміни та визначення технічного захисту інформації. Повне найменування — "ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Терміни та визначення".

С. ДСТУ 4145-2002 — державний стандарт забезпечення захисту України, що визначає основи створення та застосування підпису цифрового, що ґрунтується на криптосистемі на основі еліптичних рівнянь. Повне найменування — "ДСТУ 4145-2002. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих".

С. забезпечення захисту /с. обеспечения защиты/ [security s.] — 1) Опис послідовності оцінок, які необхідно виконати, щоб вважати дану характеристику безпеки підтвердженою з точки зору атестації захисту; 2) Множина характеристик безпеки, які повинна забезпечити система захисту, щоб її можна було використовувати в даному конкретному режимі забезпечення безпеки або у відповідності до загальної стра-

тегії захисту.

С. інформаційної безпеки /с. информационной безопасности/ [information security s.] — стандарти забезпечення захисту, призначені для взаємодії між виробниками, споживачами і експертами з кваліфікації продуктів інформаційних технологій у процесі створення та експлуатації систем оброблення інформації захищених. Найбільш значними с. і. б. є (у хронологічному порядку): "критерії безпеки комп'ютерних систем", "критерії Європейські безпеки інформаційних технологій", "критерії Федеральні безпеки інформаційних технологій", "критерії Канадські безпеки комп'ютерних систем", "критерії Загальні безпеки інформаційних технологій".

С. інформаційно-психологічної безпеки /с. информационно-психологической безопасности/ — параметри середовища інформаційного, що не викликають впливу деструктивного на психіку людини.

С. криптографічні /с. криптографические/ [cryptographic s.] — опис правил криптографічного оброблення інформації для вирішення певного завдання захисту інформації. Існують стандарти, обов'язкові для використання певними організаціями та ті, які носять рекомендаційний або навіть інформативний характер. Відомі стандарти підпису цифрового, керування ключами, функцій хешування та інші. Існують стандарти криптографічні окремих держав (наприклад, стандарти підпису цифрового Росії — Р34.10, США — DSS(Digital Signature Standard)) та міжнародні стандарти ISO.

С. криптографічного оброблення інформації /с. криптографической обработки информации/ — див. стандарти криптографічні.

С. шифрування /с. шифрования/ [encryption s.] — повний опис алгоритму шифрування інформації та правил його використання, призначений для програмної або апаратної реалізації, обов'язковий для використання організаціями, які зазначені в даному с. ш. Ідея с. ш., яка була реалізована Національним бюро стандартів США в 1972 року, практично викликала переворот у криптології. Першим с. ш. став алгоритм DES. Розвиток стандартизації у криптології привів до появи стандартів криптографічних.

С. шифрування AEC /с. шифрования AEC/ [AES (Advances Encryption Standard)] — проект ство-

рення стандарту шифрування США, на зміну DES, строк дії якого до нового перегляду витікає в 1998 році, запропонований NIST (National Institute of Standard and Technilogy). За вимогами NIST це повинен бути симетричний шифр блоковий з змінною довжиною ключа та обов'язковою підтримкою таких варіантів довжини ключа та блоку: 128-128, 192-128, 256-128. До опису алгоритму повинні надаватися коди програм на мовах програмування C та Java та результати тестування швидкодії на IBM-сумісних ПЕОМ з Intel Pentium Pro 200 (на кінець 1999 року), можуть також додаватися результати тестування на 8-бітових мікропроцесорах та інших апаратних засобах. NIST обирає алгоритм з набору кандидатів, серед яких після попереднього просіювання опинилося 15 алгоритмів.

С. шифрування DES /с. шифрования DES/ [DES (Data Encryption Standard)] — федеральний стандарт шифрування США, введений у дію 23 листопада 1976 року Американським національним інститутом стандартів (ANSI), офіційний опис стандарту опублікований 15 січня 1977 року під назвою FIPS PUB 46 "Data Encryption Standard". DES є шифром Фейстеловського типу з довжиною блока 64 біта, довжиною ключа 64 біти (8 з них використовуються для контролю парності, тому дійсна довжина ключа 56 біт) з 16 циклами, один алгоритм використовується і для зашифровування, і для розшифровування інформації. Крокова функція — добуток підстановок (реалізуються за допомогою восьми S-блоків розміром 6x4 біт), перестановок, додавання за модулем 2. Упровадження DES викликало появу цілого класу подібних йому алгоритмів, котрі інколи називають DES-подібними. DES широко розповсюджений за межами США. В 1981 році ANSI прийняв DES як стандарт захисту даних в комерційній галузі (ANSI X3.92). Під назвою (Data Encryption Algorithm) (DEA) він увійшов до міжнародного стандарту ISO 8731-1-87.

С. шифрування ГОСТ 28147-89 /с. шифрования ГОСТ 28147-89/ [Soviet GOST 28147-89] — державний стандарт шифрування СРСР, введений у дію 1 липня 1990 року Державним комітетом СРСР із стандартів, який встановлює єдиний алгоритм криптографічного перетворення для систем оброблення інформації в мережах ЕОМ, окремих обчислювальних комплексах та ЕОМ і визначає правила шифрування та вироблення імітовставки. Повна назва стандарту "Системы обработки информации. Защита криптографи-

ческая. Алгоритм криптографического преобразования. ГОСТ 28147-89". ГОСТ є шифром Фейстеловского типу з довжиною блока 64 біта, довжиною ключа 256 біт з 32 циклами, один алгоритм використовується і для зашифровування, і для розшифровування інформації. Крокова функція — добуток підстановок (реалізуються за допомогою восьми S-блоків розміром 4x4 біти), перестановок (реалізуються за допомогою регістру зсуву), додавання за модулем 2^{32} та 2 (див. Ш. Фейстеловського типу). Вироблення ключа циклового значно простіше за те, яке використовується в стандарті шифрування DES. За думкою фахівців, на сьогодні ГОСТ 28147-89 — це один з найбільш "стійких" алгоритмів.

СТАНДАРТИЗАЦІЯ /стандартизация/ [standardization] (від стандарт) — діяльність, спрямована на встановлення норм, правил і характеристик з метою забезпечення: безпеки продукції, робіт і послуг для навколишнього середовища, життя, здоров'я і майна; технічної і інформаційної сумісності, а також взаємозамінності продукції; якості продукції, робіт і послуг у відповідності до рівня розвитку науки, техніки і технології; єдність вимірювань; економії всіх видів ресурсів; безпеки господарських об'єктів з врахуванням ризику виникнення природних і техногенних катастроф та інших надзвичайних ситуацій; обороноздатності і мобілізаційної готовності країни.

С. термінів /с. терминов/ [terminology s.] — процес підготовки впорядкованої системи термінів і офіційного її оформлення у вигляді державного стандарту.

СТАНЦІЯ /станция/ [station] (від лат. statio — стояння, зупинка) — вхідний, проміжний або вихідний пункт розподіленої системи оброблення даних.

С. активна /с. активная/ [active s.] — станція даних, в якій на даний момент дозволене передавання повідомлень в лінію і приймання повідомлень з лінії.

С. ведена (підлегла) /с. ведомая (подчиненная)/ [slave s.] — станція передавання даних, запрошена станцією ведучою до прийому даних.

С. ведуча (основна) /с. ведущая (основная)/ [master s.] — станція, що здійснює управління терміна-

лами в багатопунктовому з'єднанні з метою опитування і комутації повідомлень від даних терміналів.

С. вторинна /с. вторичная/ [secondary s.] — частина станції передавання даних, яка виконує функції керування каналом передавання даних у відповідності з командами станції первинної, інтерпретує прийняті командні повідомлення і формує повідомлення у відповідь.

С. головна /с. главная/ [master s.] — станція даних, що має на даний момент право на передачу даних до однієї або декількох залежних станцій.

С. графічна /с. графическая/ [graphic s.] — комплекс програмно-апаратних засобів, призначених для побудови систем оброблення графічної інформації (включаючи системи автоматизованого проектування).

С. даних /с. данных/ [data s.] — сукупність кінцевого обладнання апаратури передавання даних.

С. заблокована /с. заблокированная/ [intercepted s.] — станція даних, в якій в даний момент заборонено приймання повідомлень.

С. завад радіоелектронним засобам /с. помех радиоэлектронним средствам/ [jammer] — технічний пристрій для створення активних завад з метою виключення або суттєвого утруднення використання противником засобів зв'язку, локації, навігації, телекерування, наведення зброї і т.ін. За характером впливу на радіоелектронні засоби поділяються на маскуючі й імітуючі (дезінформуючі).

С. керуюча /с. управляющая/ [control s.] — станція в мережі передавання даних, яка здійснює контроль за виконанням запитів на передачу, прийом і відновлення інформації.

С. локаційна лазерна /с. локационная лазерная/ [laser location s.] — установка для виявлення об'єктів (літаків, суден і т. ін.) і визначення їхнього місцезнаходження методами локації оптичної за допомогою лазерного випромінювання (когерентного випромінювання електромагнітного оптичного діапазону хвиль). С. л. л. складається з наступних основних частин: лазерного передавача, передавальної і приймальної оптичної антен, оптичного приймача і вихідного пристрою (індикатора). Вихідний пристрій призначений для перетворення сигналів, що містять корисну локаційну інформацію про об'єкт (ціль), у вид, зручний

для одержувача цієї інформації.

С. місцева /с. местная/ [local s.] — станція даних, пристрій управління якої приєднаний до каналу ЕОМ безпосередньо.

С. пасивна /с. пассивная/ [passive s.] — підпорядкована станція, що чекає запрошення до передавання або прийому.

С. первинна /с. первичная/ [primary s.] — частина станції передавання даних, яка забезпечує виконання функцій первинного управління ланкою передавання даних, формує команди, що передаються, і інтерпретує прийняті відповіді.

С. радіолокаційна (РЛС) /с. радиолокационная (РЛС)/ [radar s.] — установка для виявлення об'єктів (літаків, суден і т. ін.) і визначення їхнього місцезнаходження за допомогою відбитих радіохвиль методами радіолокації.

С. робоча /с. рабочая/ [work s., personal edition] — 1) Місце робоче автоматизоване. 2) ЕОМ професійна. 3) Вузол мережі обчислювальної локальної, призначений для роботи користувача в інтерактивному режимі.

С. робоча автоматизована /с. рабочая автоматизированная/ [automatized work s.] — багатомісний інструментальний комплекс з розподіленим обробленням даних, що забезпечує роботу колективу проектувальників, розробників, програмістів. На відміну від АРМ станція є системою колективного користування.

С. телексного зв'язку /с. телексной связи/ [telex server] — вузол локальної мережі, що забезпечує зв'язок інших вузлів мережі з телексною мережею.

С. транзитна /с. транзитная/ [transient exchange] — станція в мережах передавання даних, за допомогою якої встановлюється з'єднання між іншими станціями,

С. транспортна /с. транспортная/ [transport s.] — в мережах обчислювальних — програма інформаційного процесора, організована як сукупність взаємодіючих паралельних процесів.

С. центральна /с. центральная/ [central s.] — станція в мережі передавання даних (як правило, процесор центральний) в централізованій комутованій двосторонній системі передавання даних.

СТАРІННЯ /старение/ [ag(e)ing] — процес зміни характеристик або параметрів будь-чого внаслідок дії часу.

С. інформації /с. информации/ [a. of information, deterioration of information] — процес втрачення з часом практичної цінності інформації, зумовлений зміною об'єкта інформації. Як характеристики процесу старіння, звичайно, використовують або напівперіод життя наукових документів, або період їхнього життя. Напівперіодом життя наукової літератури вважають час, за який половина всієї опублікованої у теперішній момент літератури в певній галузі перестане використовуватися. Період життя наукової літератури — час, за який перестане використовуватися вся опублікована у теперішній момент література.

С. розвідувальної інформації /с. разведывательной информации/ — часткова або повна втрата інформативності розвідувальних даних для тих, кому вони призначені, з плином часу.

СТВОЛ /ствол/ — назва різних предметів або пристроїв, що мають форму прямої труби.

С. радіочастотний /с. радиочастотный/ — 1) Приймально-передавальний тракт, в якому радіосигнал проходить через спільні підсилювальні елементи оброблення сигналу. 2) Діапазон частот, об'єднаних для передавання інформації одного виду. Розрізняють телефонні, телеграфні, телевізійні і т.ін. стволи. Радіорелейні лінії зв'язку можуть мати до 8 стволів, а кожний ствол, наприклад, телефонний — до 1920 телефонних каналів.

СТЕГАНОГРАМА (СТЕГО) /стеганограмма (стего)/ — контейнер, який містить вбудоване приховане повідомлення.

СТЕГАНОГРАФІЯ /стеганография/ [stegonography] (від грец. $\sigma\tau\acute{\varepsilon}\gamma\eta$ — дах і $\ldots\gamma\rho\acute{\phi}\omega$ — пишу, креслю, малюю) — наука організації зв'язку таким чином, що приховується власне наявність зв'язку. С. вивчає методи синтезу та аналізу приховування факту наявності секретної інформації в повідомленні. На відміну від криптографії, де противник має можливість виявляти, перехоплювати і декодувати повідомлення — при тому, що йому протидіють певні заходи безпеки, гарантовані тією чи іншою криптосистемою,— методи стеганографії дозволяють вставляти секретні повідомлення в невинні послання так, щоб не можна було

навіть підозрювати існування підтексту. До с. відносять велику кількість секретних засобів зв'язку, таких як невидимі чорнила, мікрофотознімки, умовне розташування знаків (на відміну від криптографічних методів підстановки і перестановки), цифрові підписи, таємні канали і засоби зв'язку на плаваючих частотах і т.ін. С. займає своє місце в забезпеченні безпеки інформації: вона не замінює, а доповнює криптографію. Приховування повідомлень методами стенографії значно знижує ймовірність його виявлення. А якщо повідомлення до того ж зашифровано, то воно має додатковий рівень захисту, і на випадок його перехоплення необхідно проводити складний криптоаналіз.

С. інформаційна /с. информационная/ [information s.] — наука про вивчення методів стеганографії лінгвістичної та комп'ютерної.

С. комп'ютерна /с. компьютерная/ [computer s.] — частина стеганографії інформаційної, наука про вивчення стеганографічних методів для інформаційних контейнерів, які використовуються в сучасних інформаційно-обчислювальних системах. Методи с. к. поділяються за типами контейнерів на методи для контейнерів довільного доступу і потокових контейнерів. До першого типу відносяться файли відомого розміру, які містять випадкові дані (наприклад, цифрові картинки (растрові зображення), звукові файли). До інших — потік безперервних даних, подібно цифровому телефонному зв'язкові. За методами вбудовування повідомлень в контейнери розрізняють стеганографію селективну, сурогатну та конструюючу.

С. конструююча /с. конструирующая/ [construction s.] — процес стеганографічного перетворення, при якому шум контейнера моделюється повідомленням, що в нього вбудовується.

С. лінгвістична /с. лингвистическая/ [lingvistical s.] — наука про вивчення стеганографічних методів, що засновані на використанні надмірності людської мови. Лінгвістичні методи поділяються на умовне письмо та семаграми. Умовне письмо засноване на використанні надмірності (а звідси — "зашумленості") людської мови (наприклад, англійської або російської), яка і використовується в якості контейнера. Існує три види умовного письма: жаргонний код, пустишечний код та геометричні системи. Семаграми використовують для передавання повідомлення надмірність повідомлень будь-якого характеру, які не містять

букви та цифри. Наприклад, передача секретних повідомлень в малюнках, що містять крапки та тире для читання по коду Морзе, або положення стрілок в годиннику, або вид аналогового відеосигналу (при збереженні якості відеоінформації) і т.ін.

С. механічна /с. механическая/ [physical s.] — наука про вивчення стеганографічних методів, які засновані на використанні властивостей різних матеріальних носіїв інформації. Це хімічні (застосування невидимих (симпатичних) чорнил) та фізичні методи (мікроточки, запис на магнітні носії спеціальними методами так, що запис виявляється тільки за допомогою спеціальної апаратури і т.ін.). Симпатичні чорнила в свою чергу поділяються на органічні речовини та синтетичні хімікалії.

С. селективна /с. селективная/ [selective s.] — процес стеганографічного перетворення, при якому спочатку отримують декілька різних контейнерів, наприклад, за допомогою цифрового сканування фотокартки (цифрові дані будуть принципово випадкові). Потім обчислюють від кожного контейнера деяку функцію, наприклад, хеш-код так, щоб довжина результату співпадала з довжиною повідомлення. Обираємо контейнер, хеш-код якого співпадає з повідомленням. Стеганограмою є цей контейнер.

С. сурогатна /с. суррогатная/ [surrogate s.] — процес стеганографічного перетворення, при якому біти контейнера змінюють відповідно до секретного повідомлення таким чином, щоб ця заміна не була помітною. До найвідоміших алгоритмів с. с. відноситься алгоритм LSB.

С. технічна /с. техническая/ [technical s.] — стеганографія, що вивчає методи, засновані на застосуванні спеціальних технічних засобів схову та аналізу факту наявності інформації, прихованої в повідомленні.

СТЕГОАНАЛІЗ /стегоанализ/ [stegoanalysis] — наука про вивчення методів виявлення існування секретної інформації у відкритих повідомленнях. В с. розрізняють дві основних стратегії дій противника (стегоаналітика): пасивну та активну. При пасивній стратегії противника намагається тільки виявити факт існування і власне секретну інформацію, при активній — знищити таку секретну інформацію у відкритому повідомленні.

СТЕГОАНАЛІТИК /стегоаналитик/ — фахівець, що займається розробленням атак стегоаналітичних

на системи стеганографічні.

СТЕГОКЛЮЧ /стегоключ/ — ключ, який використовується в системі стеганографічній для приховування інформації.

СТЕРЕОТИП /стереотип/ (від грец. *στερεός* — твердий, просторовий і *τύπος* — слід, відбиток) — 1) Те, що часто повторюється, стало звичайним, загальноприйнятим і чого дотримуються, що наслідують у своїй діяльності; стандарт, трафарет, догма, норма, канон. 2) Розповсюджені в певних соціальних і етнічних групах схематизовані уявлення про факти дійсності, що обумовлюють надто спрощені (як правило — неадекватні реальності) оцінки й судження представниками цих груп. Вони формуються в результаті неодноразового смислового й емоційного акцентування свідомості людей на цих або інших явищах і подіях, багаторазового їхнього сприйняття і закарбовування у пам'яті. С. найчастіше відображають не суттєві, а зовнішні, найбільш помітні, найбільш яскраві риси явищ або подій. Будь-яка оцінка останніх, відповідно до с., приймається без доказів і вважається правильною, тоді як всяка інша піддається сумніву. С. виникають в індивідуальній, груповій і суспільній свідомості в результаті впливу не тільки навколишнього середовища, але і внаслідок сприйняття досвіду, поглядів, суджень інших людей. С. можуть стати об'єктами впливу психологічного. Їхня трансформація є одночасно і передумовою дії такого впливу, і умовою, дотримання якої дозволяє змінювати поведінку людей.

С. динамічний /с. динамический/ — відносно стійка система реакцій організму на вплив зовнішнього середовища.

С. соціальний /с. социальный/ — звичний, усталений спосіб духовної діяльності, стійкі форми й оцінки соціальних об'єктів та явищ, нормативні утворення групової і суспільної свідомості.

СТЕРЕОТРУБА /стереотруба/ [hinged stereotelescope] — бінокулярний стереоскопічний прилад для огляду із схованки та вивчення місцевості і цілей, вимірювання кутів та відстаней. Складається з двох шарнірно з'єднаних зорових труб з окулярами, держака, лімба та механізму для вимірювання вертикальних кутів (механізм рівня); укомплектовується триногою, оптичною насадкою і т.ін. Збільшення С. 10-ти кратне (з

оптичною насадкою 20-ти кратне). Точність вимірювання вертикальних та горизонтальних кутів 1,8'.

СТЕТОСКОП /стетоскоп/ [stethoscope] (від грец. *στῆθος* — груди і *...σκοπέω* — спостерігаю, розглядаю) — пристрій для прослухування розмов через стіни. С. являє собою вібродатчик, підсилювач та головні телефони. Може оснащуватися проводовим, радіо або іншим каналом передавання інформації.

СТІЙКІСТЬ /стойкость/[stability] — здатність витримати зовнішній вплив, протидіяти чомусь.

С. до відмов /с. к отказам/ [fault s.] — послуга, що забезпечує здатність комп'ютерної системи продовжувати функціонування в умовах виникнення збоїв і відмов окремих компонентів.

С. замка /с. замка/ — здатність замка протистояти несанкціонованому відкриванню. С. з. залежить від його конструкції, типу металу і секретності запірного механізму, що оцінюється кількістю комбінацій положень штифтів або кодових комбінацій.

С. захисту /с. защиты/ — імовірність неподолання захисту порушником за певний проміжок часу.

С. сейфа (сховища) до зламу /с. сейфа (хранилища) к взломыванию/ — умовна одиниця опору (C_E або RU), яка визначається як добуток проміжку часу, витраченого на злам сейфа (сховища), і коефіцієнта складності застосованого для цього інструмента з врахуванням складності його доставки та використання. При цьому розрізняють злам з повним доступом, коли відкриваються двері сейфа або сховища, і частковий злам. Злам з частковим доступом передбачає створення у сейфі отвору, достатнього для просовування у нього руки. Весь інтервал одиниць стійкості (30–4500 C_E) розподілений на 13 класів стійкості до злому. Групу найбільш високої стійкості створюють сховища 11–13 класів (2000–4500 C_E). Тривалість їхнього зламу при використанні найбільш ефективного інструмента (електрорізального інструмента з алмазним буром потужністю до 11 кВт, газових горілок і т.ін. повинно бути не менше 45–120 хв. Сейфи мають меншу стійкість до зламу, ніж сховища. До сейфів з високою стійкістю відносяться сейфи 7–10 класів (400–1350 C_E). Наприклад, для часткового доступу до сейфа 5 класу з використанням лома, ковадла і зубила потрібно 22 хв., газового різака — 14,1 хв., а колонкового бура з алмазною коронкою — 8,7 хв.

С. сейфа до вологості навколишнього середовища /с. сейфа от влажности окружающей сре-

ды/ — для сейфів, призначених для зберігання машинних носіїв, оцінюється проміжком часу, протягом якого вологість всередині сейфа не перевищить значень граничної вологості 80–85% при 100% вологості навколишнього середовища.

С. сейфа до температури (пожежі) /с. сейфа к температуре (пожару)/ — проміжок часу, протягом якого температура усередині сейфа не перевищує температури загоряння паперу або інших вкладень. Цей проміжок часу оцінюється з моменту нагрівання сейфа до температури біля 1000° С і складає 1–2 години. Температура всередині сейфа не повинна перевищувати для паперу 170° С, для магнітних стрічок і дисків, фото- і кіноплівки — 70° С, гнучких магнітних дисків — 50° С.

С. сховища до зламу вибухівкою /с. хранилища к зломыванию взрывчаткой/ — здатність сховища витримати випробування вибухом вибухівки з масою заряду до 500 Г у тротиловому еквіваленті. С., що витримують таке випробування маркуються додатковим індексом “ВВ”.

С. шифру /с. шифра/ — здатність шифру погано піддаватися розкриттю. Ніякий шифр не є абсолютно стійким. С. ш. визначається часом, необхідним для його дешифрування. Хорошими є шифри, для розкриття яких потрібні роки. За цей час засекречена за допомогою шифру інформація втратить свою актуальність, або вартість дешифрування перевищить вартість самої інформації.

СТОРІНКА /страница/ [page] — встановлена порція інформації для обміну між пам’яттю і пристроєм перекачки в системі із сторінковим обміном.

С. Web /с. Web/ [Web-p.] — файл із гіпертекстовим документом у форматі HTML. Звичайно, має розширення .htm або .html, посилання на інші сторінки, лічильники відвідувань, фрейми, Java-апплети, посилання на CGI-скрипти, елементи керування (рядки введення, елементи вибору, кнопки). Створення WEB-с. — процес підготовки інформаційного змісту сервера Web, що включає: розроблення концепції, стилю, інформаційного змісту й оформлення. Звичайно, виконується колективом відповідних фахівців. Для розроблення Web-сторінок використовується широкий спектр програмного забезпечення: редактори Web-сторінок Microsoft FrontPage 98, Microsoft Word 97, Netscape Navigator; графічні редактори Corel Draw,

Adobe PhotoShop, спеціалізовані програми Map This!, Microsoft GIF Animator, і т. ін., аж до мов програмування для створення Java-апплетів, CGI-скриптів.

С. персональна /с. персональная/ — сукупність сторінок Web, із змістом, яка описує сферу інтересів якоїсь людини (групи осіб), що, звичайно, створена ним самим. Розміщується на вже існуючому сервері Web у каталозі для домашніх сторінок.

СТРАТЕГІЯ /стратегия/ [strategy] (грец. $\sigma\tau\rho\alpha\tau\eta\gamma\acute{\iota}\alpha$) — 1) Мистецтво підготовки і ведення війни та великих воєнних операцій. 2) Мистецтво суспільного і політичного керівництва масами, яке має визначити головний напрям їхніх дій, вчинків. 3) Спосіб дій, лінії поведінки кого-небудь.

С. захисту /с. защиты/ [security s.] — формальне визначення критеріїв, якими слід керуватися при забезпеченні захисту системи від відомих загроз.

С. інформаційна /с. информационная/ [information s.] — сукупність принципів і методів, які використовуються державою при управлінні ресурсами інформаційними.

С. інформаційної війни /с. информационной войны/ [information war s.] — теорія і практика підготовки до війни інформаційної, її планування і ведення. С. і. в. найбільш необхідна збройним силам, коли їм доводиться проводити операції воєнні у середовищі, що відрізняється від звичайного середовища ведення бойових дій. С. і. в. визначають воєнні, політичні і економічні інтереси держави.

С. маркетингова в політиці і владі /с. маркетинговая в политике и власти/ [marketing s. in politics and power] — система специфічних прийомів і методів цілеспрямованих дій на сцені політичних подій (“політичному ринкові”). Вони застосовуються з метою проникнення на політичний ринок конкурента, виведення на сцену політичного життя нового лідера, усунення лідера, що став непопулярним (стратегія “виходу з ринку”). Розрізняють такі види політичного маркетингу, як стимулюючий, розвиваючий, конверсійний, підтримуючий, протидіючий і т. ін., а у зв’язку з цим стратегії — наступальну, оборонну, очікувальну, демаркетинг і т. ін.

СТРАХ /страх/ [fear, flight, terror] — негативна емоція у ситуації реальної або уявної небезпеки.

СТРУКТУРА /структура/ [structure] (лат. structura — побудова, розміщення, від struo — будую, зводжу) — 1) Взаєморозміщення та взаємозв'язок складових частин цілого; будова. 2) Устрій, організація чого-небудь; форма.

С. листівки /с. листовки/ — сукупність усіх шрифтових, графічних і ілюстративних елементів, що відображають вид і тематичний замисел листівки. Різноманітні види листівок мають як загальні, так і своєрідні структурні елементи. Так, структура листівок інформаційних відрізняється формою основного тексту, який складається з окремих повідомлень, нерідко взятих із різноманітних джерел, із своїми заголовками. Інформаційні листівки мають також свої назви, номери і дати випуску. Структура листівок спеціальних залежить від їхніх різновидів. Наприклад, листівки-документи, як правило, відтворюють той чи інший документ. Листівки маскувальні відповідають тому документові, який вони імітують і т.ін. Основними елементами структури аналітичних листівок є: заголовок, звернення, вступ, основний текст, кінцівка, підпис, ремарка, перепустка. Кожний з елементів листівки виконує свою власну функцію: заголовок, ремарка, звернення та ілюстрація привертають увагу до листівки, зацікавлюють читача, спонукають його до читання основного тексту; функція основного тексту — переконати читача в необхідності дотримуватися рекомендацій, що містяться в ньому.

С. ознакова /с. признаковая/ — набір залежних або незалежних ознак, про які достовірно відомо, що вони відносяться до об'єкта, що розглядається.

С. ознакова еталонна /с. признаковая эталонная/ — набір достовірно відомих ознак об'єкта або сигналу, одержаних із першоджерел або за даними, добутими з різних джерел.

С. програм усного мовлення /с. программ устного вещания/ — взаєморозташування та взаємозв'язок складових частин програм усного мовлення. Залежить від чотирьох основних факторів: мети передачі; психологічних особливостей об'єкта впливу; тривалості програми; обстановки, в якій здійснюється мовлення. Програми усного мовлення, звичайно, включають наступні структурні елементи: сигнал про початок передачі, який служить для попередження своїх військ про те, що не можна заважати передачі, і привертає

увагу противника, емоційно налаштовує його на прослухування; вступ, який з однієї сторони, продовжує привертати увагу противника, а з іншої — готує його до сприйняття основної частини програми; текст програми усного мовлення основний; кінцівка, в якій підводять підсумки передачі, і яка, на відміну від основного тексту, містить політичні висновки, пропагандистські лозунги, заклики до практичних дій (вона як би незалежна від основного тексту, але логічно зв'язана з його положеннями). У кінцівці також повідомляють про наступні сеанси усного мовлення; сигнал про закінчення передачі. Додатковий, але важливий елемент програми усного мовлення складають музика, шуми й сигнали.

СТРУКТУРУВАННЯ /структурирование/ [structuring, stucturization] — визначення внутрішнього устрою чого-небудь.

С. завдань на добування інформації /с. задач на добывание информации/ — аналіз поставленого в загальному вигляді завдання на добування інформації та його конкретизація з врахуванням наявних апріорних даних про можливі джерела інформації, їхнє місцезнаходження, способи доступу і перешкоди, параметри засобів добування інформації і т.ін. В результаті аналізу завдань і апріорних даних розроблюється задум операції розвідувальної, в якому намічаються шляхи вирішення поставлених завдань.

С. інформації /с. информации/ [information s.] — класифікація інформації у відповідності до структури, функцій і завдань організації з прив'язкою елементів інформації до її джерел. Деталізацію інформації доцільно проводити до рівня, на якому елементові інформації відповідає одне джерело. Вихідними даними для с. і., що потребує захисту, є перелік відомостей, що складають державну, відомчу або комерційну таємницю, та перелік джерел інформації в організації. Результати с. і. оформляються у вигляді схеми класифікації інформації та таблиці, розробленої на основі схеми класифікації інформації.

СТУПОР /ступор/ [stupor] (від лат. stupor — заціпеніння) — стан нечутливості, отупіння, нерухомості з відсутністю реакції на зовнішні подразники (в тому числі больові).

СУБ'ЄКТ /субъект/ [subject] (від лат. subjectum — підкладене) — 1) Носій певного роду діяльності;

джерело активності, спрямованої на об'єкт. 2) Особа або організація, що має певні права й обов'язки.

С. атаки /с. атаки/ — сторона, що реалізовує атаку. Див. також віддалена атаки на мережу обміну інформацією.

С. безпеки /с. безопасности/ [security s.] — активна складова системи, до якої застосовується методика безпеки.

С. доступу /с. доступа/ [access s.] — активна сутність (процес, користувач, пристрій і т. ін.), що викликає утворення інформаційного потоку між об'єктами доступу або зміну стану обчислювальної системи. Дії с. д. регламентуються правилами розмежування доступу.

С. інформаційної безпеки /с. информационной безопасности/ [information security s.] — держава, що здійснює свої функції через відповідні органи; громадяни, суспільні або інші організації і об'єднання, що володіють повноваженнями по забезпеченню безпеки інформаційної у відповідності до законодавства.

С. правового регулювання в інформаційній сфері /с. правового регулирования в информационной сфере/ — юридичні і фізичні особи, які створюють (продукують) і споживають інформацію; юридичні і фізичні особи, які розробляють і застосовують системи інформаційні, технології і засоби їхнього забезпечення; органи державної влади і місцевого самоврядування; інформаційні організації, підприємства, заклади, які формують ресурси інформаційні і надають користувачам інформацію з них.

СУВАЛЬДИ /сувальды/ — деталі замка, які штовхають ригель внаслідок дії "свого" ключа. Конструкція і конфігурація підпружинених сувальд утворюють "секрет" ключа,

СУГЕСТІЯ /суггестия/ [suggestion] (лат. suggestio, від suggero — навчаю, навіюю) — 1) Вплив, навіювання. 2) Прихований інформаційний вплив на інформаційну систему із самонавчанням.

СУМА /сумма/ [sum, total] (від лат. summa — сукупність) — 1) Результат додавання двох або кількох величин; підсумок. 2) Загальна кількість, сукупність чого-небудь; обсяг. 3) Певна кількість грошей.

С. контрольна /с. контрольная/ [control (hash) t., checksum] — сума всіх елементів масиву даних (бітів, байтів або слів), що обчислюється з метою контролю вірності передавання даних.

СУМІСНІСТЬ /совместимость/ [compatibility] — властивість різноманітних за конструкцією пристроїв виконувати ідентичні функції.

С. інформаційна /с. информационная/ [data c.] — використання різних баз даних автоматизованими системами оброблення інформації різних рівнів.

С. лінгвістична /с. лингвистическая/ [linguistic c.] — вживання однозначності термінів, а також інших мовних засобів, що використовуються в АСОІ, і правил формалізації мови природної, в тому числі методи стискання і розгортання текстів.

С. математична /с. математическая/ [mathematical c.] — можливість використання єдиних математичних методів, моделей і алгоритмів в АСОІ різних рівнів.

С. організаційна /с. организационная/ [organization c.] — поєднання організаційної структури АСОІ різних рівнів і різного функціонального призначення.

С. програмна /с. программная/ [program c.] — можливість використання програм в АСОІ різних рівнів і різного функціонального призначення.

С. технічна /с. техническая/ [technical c.] — забезпечення автоматичного функціонування комплексу технічних засобів АСОІ різних рівнів, в тому числі обмін інформацією і можливість спільного розв'язання великомасштабних завдань.

СУПЕР... /супер/ [super...] (лат. super...) — префікс, що означає зверхність, найвищу якість, посилену дію.

СУПЕРГЕТЕРОДИН /супергетеродин/ [superheterodyne] (від. супер... і гетеродин) — див. приймач супергетеродинний.

СУПЕРМАГІСТРАЛЬ /супермагистраль/ [superunibus] (від супер... і магістраль) — найголовніший напрям, найосновніша лінія в комунікаціях.

С. інформаційна /с. информационная/ [information s.] — надшвидкісна мережа передавання даних, що дозволяє будь-якому користувачеві обмінюватися інформацією з будь-яким іншим користувачем незалежно від його місцезнаходження. Ґрунтується на принципі синтезу обчислювальної техніки і телебачення. Для

розвитку с. і. необхідна горизонтальна і вертикальна інтеграція не тільки різноманітних засобів зв'язку (телефонно-кабельних, телевізійних, комп'ютерних, супутникових) але і тих промислових підприємств, що створюють технічне забезпечення таких засобів. Крім того, необхідні зусилля у відношенні фінансової бази, маркетингу і суспільно-політичного консенсусу в національному й транснаціональному масштабах. Побудова всієї такої складної інформаційної структури потребує розроблення правил експлуатації і. с. для нормального трафіка інформаційного з метою безвідмовного й безпечного обслуговування усіх абонентів. Проте в с. і. можуть виникнути і труднощі зі захистом інтелектуальної власності від терористів кіберспейсу (див. тероризм комп'ютерний) і змісту інформації від елементів, що суперечать нормам загальнолюдської моралі.

СУПЕРСЕРВЕР /суперсервер/ [superserver] (від супер... і сервер) — багатопроцесорна система для мереж обчислювальних локальних, що використовує процесори з повною системою команд.

СУПЕРСМАРТ-КАРТКА /суперсмарт-карта/ [super smart card] (від супер... і смарт-картка) — смарт-картка, яка має невеликий дисплей, а також клавіатуру для введення даних.

СУПУТНИК /спутник/ [satellite] — небесне тіло, яке рухається навколо планети або зірки.

С. зв'язку /с. связи/ [communications s.] — супутник Землі штучний, призначений для ретрансляції радіосигналів систем зв'язку, що передаються із Землі, на великі відстані між стаціонарними пунктами або рухомими об'єктами. С. з. можуть мати еліптичні і кругові орбіти, в числі яких можуть бути екваторіальні, полярні і похилі до площини екватора. В залежності від способу ретрансляції радіосигналів с. з. поділяються на активні і пасивні.

С. зв'язку стаціонарний /с. связи стационарный/ — супутник зв'язку, запущений на кругову стаціонарну орбіту з періодом обертання 24 години. Висота орбіти с. с. з. над поверхнею Землі близько 38800 км, а дальність радіозв'язку з наземним пунктом може сягати 18 тис. км. Використовуються в космічних (супутникових) системах радіозв'язку.

С. Землі штучний (ШСЗ) /с. Земли искусственный (ИСЗ)/ [artifical Earth s.] — апарат космічний,

виведений в космічний простір для вирішення певних завдань і який здійснює вільний рух по навколоземній орбіті.

С. інфрачервоної розвідки /с. інфракрасной разведки/ — супутник розвідувальний, оснащений спеціальною інфрачервоною апаратурою, яка складається з наступних частин: антенного пристрою для сприйняття інфрачервоного випромінювання і фокусування зображень об'єктів; приймача оптичного для перетворення інфрачервоного сигналу в електричний сигнал; засобів оброблення і розпізнавання сигналів, а також блоку управління і зв'язку. Основним призначенням с. і. р. є раннє виявлення міжконтинентальних балістичних ракет відразу після їхнього запуску на активній ділянці траєкторії польоту, а також крилатих ракет середньої дальності. Розташовані на супутнику інфрачервоні системи стратегічної розвідки можуть забезпечувати виявлення і ідентифікацію промислових і воєнних об'єктів, адміністративних центрів, шосейних доріг і т.ін. В с. і. р. широко застосовується фотографічна апаратура, яка має багатооб'єктові камери, які дозволяють вести одночасне фотографування декількома каналами у відповідності з вибраними зонами на поверхні Землі. При цьому для фотографування використовуються різноманітні плівки (чорно-білі, спектральні, інфрачервоні) з відповідним фільтром.

С. радіо- і радіотехнічної розвідки /с. радио- и радиотехнической разведки/ — супутник розвідувальний, обладнаний засобами радіо- і радіотехнічної розвідки, які дозволяють: вести пошук і перехоплення сигналів РЛС і радіостанцій в широкому діапазоні частот; визначати їхні основні технічні характеристики; реєструвати інформацію, що добувається; передавати зафіксовану інформацію на наземні центри.

С. радіолокаційної розвідки /с. радиолокационной разведки/ — супутник розвідувальний, обладнаний радіолокаційними станціями бічного огляду, за допомогою яких одержують зображення місцевості з ясним обрисом — мостів, аеродромів, будинків та інших наземних предметів — окремо рухомих і окремо нерухомих. Зображення переносяться на фотоплівку за допомогою спеціального пристрою. На супутнику є апаратура передавання даних, яка дозволяє передавати на Землю не тільки готові зображення на фотоплівці, але і безпосередньо інформацію з екрана індикатора локатора без погіршення якості зображення.

С. р. р. обладнані лазерними локаторами в нічних умовах дозволяють одержувати знімки, що за чіткістю зображення аналогічні фотознімкам, які зроблені у світлий час доби.

С. розвідувальний /с. разведывательный/ [intelligence s., reconnaissance s., surveillance s.] — супутник Землі штучний, призначений для виявлення різних цілей, що знаходяться на суші, водній поверхні або в атмосфері, зокрема, для виявлення запусків міжконтинентальних балістичних ракет і ядерних вибухів. В залежності від виконуваних функцій р. с. можуть мати на борті станції радіорозвідки і станції радіотехнічної розвідки, фото- і телевізійну апаратуру, приймачі інфрачервоного випромінювання та інші засоби радіоелектронні, а також спеціальне обладнання для передавання інформації розвідувальної на наземні, корабельні та інші пункти прийому.

С. фотографічної розвідки /с. фотографической разведки/ — супутник розвідувальний, призначений для ведення розвідки фотографічної. С. ф. р. застосовуються у двох варіантах — для оглядової і для детальної фотографічної розвідки. Оглядова фотографічна розвідка ведеться шляхом суцільного фотографування території ймовірного противника з використанням короткофокусної фотоапаратури. Детальна фотографічна розвідка призначається для вибіркового фотографування районів або об'єктів, виявлених при оглядовій фотографічній розвідці.

СУСПІЛЬСТВО /общество/ [society] — 1) Сукупність форм сумісної діяльності людей, що утворилися в процесі історичного розвитку. 2) Історично конкретний тип соціальної системи.

С. індустріальне /о. индустриальное/ [industrial s.] — суспільство з високим рівнем технічного, індустріального розвитку.

С. інформаційне /о. информационное/ [information s.] — суспільство, яке в кінці 20 ст. прийшло на зміну суспільству індустріальному (див. ознаки інформаційного суспільства). В с. і. велике значення мають системи розповсюдження, зберігання і оброблення інформації, яка є його основним об'єктом. Відображаючи реальну дійсність, інформація проникає в усі напрямки діяльності держави, суспільства, громадянина. З появою інформаційних технологій нових, заснованих на широкому впровадженні засобів обчислювальної

техніки, зв'язку, систем телекомунікацій, вона стає постійним і необхідним атрибутом забезпечення діяльності держави, юридичних осіб, суспільних об'єднань і громадян. Від її якості і достовірності, оперативності одержання залежить більшість рішень, що приймаються на різних рівнях — від голови держави і до громадянина. Вплив інформаційний на державу, суспільство, громадянина зараз більш ефективний і економний, ніж політичний, економічний і навіть воєнний. Ресурси інформаційні стають в один ряд з найважливішими ресурсами держави — природними, трудовими, фінансовими та іншими, що складають його потенціал. Основу с. і. складає простір інформаційний світовий. Сфера інформаційна стає не тільки однією з найважливіших сфер міжнародного співробітництва, але і об'єктом суперництва. Країни з більш розвиненою інфраструктурою інформаційною, встановлюючи технологічні стандарти й надаючи покупцям свої ресурси, визначають умови формування і діяльності інформаційних структур в інших країнах, та здійснюють суттєвий вплив на розвиток їхніх сфер інформаційних. Розвиток і забезпечення безпеки інформаційної сфери є пріоритетними при формуванні політики інформаційної державної і програми входження в інформаційне суспільство.

С. масове /о. массовое/ [mass s.] — в комунікативістиці — поняття для визначення атрибутики масмедіа і його історичного закономірного зв'язку з такими наслідками індустріалізації, як масове об'єднання людей, різних за своїм соціально-етнічним, релігійним і культурним статусом за допомогою споживацької економіки й психології, які впроваджуються в суспільство за допомогою засобів масової інформації повсюдно, швидко й безупинно, підкоряючись імперативам комерційних інтересів, розвиненого товарно-грошового бізнесу.

С. постіндустріальне /о. постиндустриальное/ [postindustrial s.] — суспільство індустріальне, в якому центр тяжіння переноситься у сфери надання послуг і науково-дослідних закладів. Таке суспільство стає функціонально більш залежним не від індустрії, а від комплексних наукових сил і знань. Для нього характерний вирішальний вплив електронних засобів масової інформації на усі сфери економічного, політичного і культурного життя. Культура в с. п. стає більш гедоністичною (грец. *ἡδονή* — насолода)і

вседозволяючою, оскільки електронні ЗМІ, апелюючи до почуттів, а не до розуму, вступають в протиріччя з класичними традиціями раціоналістичної естетики й етики і починають підтримувати замість дисципліни думок і почуттів безмежний егоцентризм.

С. технотронне /о. технотронное/ [technetronic s.] (абревіатурний синтез слів technological та electronic) — концепція, яка стверджує, що через бурхливий розвиток електронно-обчислювальної техніки й аудіовізуальних ЗМІ суспільство постіндустріальне перетвориться в технотронне і на його основі формується глобалізуюча комунікаційна система, за допомогою якої люди набувають нове глобальне бачення світу, засноване на образах і почуттях. Технотронна революція, що формує с. т., носить не ідеологічний і не соціальний, а просторово-часовий характер, охоплюючи весь світ через найновіші засоби аудіовізуального зв'язку, і розповсюджує повсюди єдині стилі одягу й поведінки, подібність в організації побуту та дозвілля, що виникають внаслідок ескалації модних товарів культури масової по каналах ЗМІ. Відповідно до цієї концепції, електронні аудіовізуальні засоби зв'язку створюють і новий шлях до рівності через деідеологізацію — звільнення від усіх організованих системних форм віри й право вибирати стилі життя, опираючись на почуття, а не на раціональні ідеали, що лежать в основі різноманітних політичних програм і суспільних рухів.

СУТНІСТЬ /сущность/ [entity, essence] — 1) Найголовніше, основне, істотне в кому-, чому-небудь; суть, зміст. 2) У філософії — головне, визначальне в предметі, що зумовлене глибинними зв'язками й тенденціями розвитку і пізнається на рівні теоретичного мислення. 3) Елемент моделі (сукупність атрибутів і знаків), які описують закінчений об'єкт або поняття.

СФЕРА /сфера/[sphere] (від грец. $\sigma\varphi\alpha\tilde{\imath}\rho\alpha$ — куля) — 1) Область фізичного або духовного життя, діяльності людини або суспільства. 2) Сукупність точок, рівновіддалених від даної точки (центра сфери).

С. інформаційна /с. информационная/ [information environment] — сфера діяльності суб'єктів, зв'язана із створенням, перетворенням і споживанням інформації. С. і. умовно поділяється на три основні предметні частини: створення і розповсюдження інформації вихідної та похідної; формування ресурсів

інформаційних, підготовки продуктів інформаційних, надання послуг інформаційних; споживання інформації та дві забезпечувальні предметні частини: створення і застосування систем інформаційних, технологій інформаційних і засобів їхнього забезпечення; створення і застосування засобів і механізмів інформаційної безпеки.

СХЕМА /схема/ [schema, scheme, circuit] (від грец. $\sigma\chi\tilde{\eta}\mu\alpha$ — вид, форма) — 1) Графічне зображення умовними символами структури якого-небудь об'єкта. 2) Опис складу і властивостей об'єкта.

С. інтегральна /с. интегральная/ [integrated c.] — мініатюрна електронна схема, що містить електронні елементи (транзистори, діоди, резистори і т. ін.) і створена на поверхні або всередині напівпровідникового кристала. Розрізняють і. с. малого ступеня інтеграції (MIC), середнього ступеня інтеграції (CIC), схеми інтегральні великі (BIC) і схеми інтегральні надвеликі (HBIC).

С. інтегральна велика (BIC) /с. интегральная большая/ [large scale integration c.] — мікросхема інтегральна, що містить від декількох сотень до декількох тисяч елементів і компонентів в одному кристалі напівпровідника.

С. інтегральна надвелика (HBIC) /с. интегральная сверхбольшая(СБИС)/ [very large-scale integration] — мікросхема інтегральна із ступенем інтеграції понад 1000 елементів в кристалі.

С. сертифікації / с. сертификации/ — склад і послідовність дій третьої сторони під час проведення сертифікації.

СХОВИЩЕ /хранилище/[depository] — конструкція захисту об'єктів інженерна, призначена для зберігання особливо цінних документів, речей, великих сум грошей. С. являє собою споруду з площею основи внутрішнього простору більше 2 м^2, захищену від злому і стійку до впливу високої температури при пожежі. За конструкцією с. можуть бути монолітними, збірними і збірно-монолітними. Монолітні залізобетонні с. з товщиною захисних стін більше 100 см розташовуються у підвалі будівлі на її фундаменті. На міжповерховому перекритті будівлі встановлюються більш легкі збірні (модульні) с. з тонкостінних конструкцій, що складаються зі стальної обшивки і заповнювача з армованого бетону з високою міцністю. С. характе-

ризується стійкістю до зламу.

Т

ТАБЛИЦЯ /таблица/ [table] (польс. tablica, від tabula — дошка) — зведення, перелік предметів, розпис відомостей про що-небудь, розміщених у певному порядку, за графами.

Т. маршрутизації /т. маршрутизации/ [routing t.] — список діючих шляхів передавання даних.

ТАЄМНИЦЯ /тайна/ [mystery, secret, secrecy, privacy] — 1) Дещо ще не розгадане, не пізнане. 2) Дещо, що старанно приховується від інших, відоме тільки обмеженому колу осіб, інформація, що не підлягає розголошенню, секрет. 3) Таємна або конфіденційна інформація (відомості), що відома вузькому колу суб'єктів унаслідок виконання службових, професійних обов'язків або окремих доручень, яка охороняється особливим чином, а розголошення її може спричинити юридичну відповідальність. Причому юридична відповідальність наступає не тільки за розголошення таємниці, але й і за її незаконне одержання та використання. В законодавствах розвинених країн звичайно виділяють наступні види таємниць: таємницю приватного життя, професійну, комерційну, службову, державну таємницю.

Т. банківська /т. банковская/ — відомості щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку і розголошення якої може завдати матеріальної чи моральної шкоди клієнту. Такими відомостями в державі, зокрема, є: відомості про стан рахунків клієнтів, у тому числі стан кореспондентських рахунків банків у Національному банку; операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди; фінансово-економічний стан клієнтів; системи охорони банку та клієнтів; інформація про організаційно-правову структуру юридичної особи - клієнта, її керівників, напрями діяльності; відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація; інформація щодо звітності по окремому банку, за винятком тієї, що підлягає опублікуванню; коди, що використовуються банками для захисту інформації. Інформація про

банки чи клієнтів, що збирається під час проведення банківського нагляду, також становить т. б.

Т. голосування /т. голосования/ [s. of the ballot] — відомості зафіксовані в бюлетені для голосування, які розкривають відношення громадянина до вибору того чи іншого кандидата.

Т. державна /т. государственная/ [State s.] — відомості в галузі воєнної, зовнішньополітичної, економічної, розвідувальної, контррозвідувальної і оперативно-розшукової діяльності, що підлягають захисту державою, і розповсюдження яких може заподіяти шкоду безпеці держави (див. також відомості, що складають державну таємницю). Забезпечення д. т. досягається організацією діяльності спеціальних органів, осіб, введенням відповідних правил, інструкцій і т. ін. Див. також система захисту державної таємниці.

Т. комерційна /т. коммерческая/ [commerce s.] — конфіденційні відомості в галузі виробничо-господарської, управлінської, фінансової діяльності організації, які охороняються законом та мають реальну або потенційну цінність в силу того, що вони невідомі третім особам, до них нема вільного доступу на законній основі, власник відомостей застосовує заходи щодо їх конфіденційності, незаконне одержання або розголошення яких створює загрозу спричинення шкоди власнику цих відомостей та надає йому право на захист відповідно до законодавства держави.

Т. особиста /т. личная/ — відомості про стан здоров'я, особливо у тих випадках, коли людина страждає такими хворобами, які вважаються ганебними з позиції суспільної моралі, любовні зв'язки, особливо коли вони супроводжуються подружніми зрадами, погані звички, пристрасті, вроджені, спадкові та набуті пороки, що межують часом з нервово-психічними аномаліями, приховані фізичні вади; порочне соціальне минуле громадянина, а також ділові та шлюбові зв'язки, порочать людину. До т. о. можна віднести також відноситься таємниця спілкування і творчості, таємниця інтимних відносин, таємниця щоденників, особистих паперів. Кожна особистість сама визначає коло і межі т. о. Т. о. є складовою частиною приватного життя, відносно відособленою зоною найбільш делікатних, інтимних сторін життя людини, коли розголошення певних відомостей є не тільки небажаним, але й шкідливим, пагубним з моральної точки

зору.

Т. переписки, поштових, телеграфних та інших повідомлень /т. переписки, почтовых, телеграфных и иных сообщений/ [p. of correspondence, p. of letters, postal p.] — таємниця будь-яких, у тому числі конфіденційних відомостей, що передаються особою по пошті, телеграфом, телефоном, комп'ютерною мережею, іншими каналами зв'язку.

Т. приватного життя /т. частной жизни/ — конфіденційні відомості, що охороняються законом та складаю таємницю особисту або таємницю сімейну особи, незаконне збирання або розповсюдження яких може нанести шкоду правам та законним інтересам цієї особи та надає їй право на захист відповідно до законодавства держави. У свою чергу особиста та сімейна таємниці можуть включати в себе таємницю голосування, таємницю сповіді, таємницю усиновлення, таємницю переписки, поштових, телефонних, телеграфних та інших повідомлень.

Т. професійна /т. профессиональная/— відомості, що охороняються законом, які були довірені або стали відомими особам виключно при виконанні ними своїх професійних обов'язків, не зв'язаних з державною або муніципальною службою, незаконне одержання або розповсюдження яких може спричинити по собі шкоду правам в обов'язкам іншої особи, що довірила ці відомості, та надає їй право на захист відповідно до законодавства держави.

Т. сімейна /т. семейная/ — відомості, що стосуються сім'ї, і за моральними міркуваннями приховуються від сторонніх очей сім'єю, під якою в соціальному аспекті розуміють союз осіб, заснований на шлюбі, спорідненості, прийняті дітей на виховання, та характеризується спільністю життя, інтересів, а в юридичному смислі — коло осіб, пов'язаних правами і обов'язками, що виходять із шлюбу, спорідненості, усиновлення або іншої форм прийняття дітей на виховання.

Т. службова /т. служебная/ — конфіденційні відомості про діяльність державних органів, які охороняються законом, доступ до яких обмежений законом або внаслідок службової необхідності, а також такі, що стали відомими в державних органах та органах місцевого самоуправління тільки на законній основі

і внаслідок виконання їх представниками службових обов'язків та мають реальну або потенційну цінність в силу того, що вони невідомі третім особам, до них нема вільного доступу на законній основі, власник відомостей застосовує заходи щодо їх конфіденційності, незаконне одержання або розголошення яких створює загрозу спричинення шкоди власнику цих відомостей та надає йому право на захист відповідно до законодавства держави.

Т. сповіді /т. исповеди/ [seal of confession] — відомості, які повідомляє віруючий священнослужителю на сповіді. До них можуть відноситися відомості з особистого та сімейного життя, про наявні порушення моралі та закону. Т. с. — гарантія недоторканності приватного життя віруючих.

Т. усиновлення /т. усыновления/ — відомості про факт усиновлення дитини, інформація про відмову від нього справжніх батьків, інших обставин усиновлення. Надання розголосу цих відомостей третім особам, яким не було відомо про факт усиновлення, означає розголошення т. у.

ТАЙНИК /тайник/ [hiding-place] — заздалегідь призначене секретне місце, призначене для таємної закладки і вилучення повідомлень і грошей без очної зустрічі сторін (агент і співробітник розвідки приходять до тайника у різний час).

ТАЙНОПИС /тайнопись/ [cryptography, cryptographic writing] — умовне таємне письмо; класичний метод забезпечення секретності переписки у розвідці.

ТЕАТР /театр/ [theater, theatre] (французьке th*éâ*tre, від грецького $\vartheta\acute{\varepsilon}\alpha\tau\rho\varnothing\nu$ — місце для видовищ) — місце, де розгортаються, відбуваються якісь події.

Т. бойових інформаційних дій /т. боевых информационных действий/ — сукупність сфер у межах яких можуть здійснюватися інформаційні бойові дії: поле бою електронне, простір для атак в мережах обміну інформацією автоматизованих систем керування, інфраструктури інформаційні, а також сфери, що включають поняття розвідка та шпіонаж промисловий, конфіденційність.

ТЕГА /тега/ [teg] — сукупність атрибутів асоційованих із користувачем, процесом або проектом. Т. може бути унікальний ідентифікатор, мітка безпеки або цілісності, ключ криптографічний, Таблиця прав доступу

або інші атрибути у відповідності з реалізованою в комп'ютерній системі політикою безпеки.

ТЕЗАУРУС /тезаурус/ [thesaurus] (від грец. *θησαυρός* — скарб, скарбниця) — 1) Сукупність понять із певної галузі науки, накопичених людиною чи колективом. У вузькому розумінні — словник, який відображає смислові зв'язки між словами або іншими смисловими елементами даної мови, і призначений для пошуку слів за їхнім смислом. 2) В системах інформаційних автоматизованих — автоматичний словник, що відображає семантичні відношення між лексичними одиницями інформаційно-пошукової мови і призначений для пошуку слів за їхнім смислом. запитів.

ТЕКСТ /текст/ [text] (від лат. textum — тканина, зв'язок, побудова) — 1) Відтворені на письмі або друком авторська праця, висловлювання, документи, пам'ятки тощо. 2) В комунікативістиці — інформаційний зміст документа, програми, повідомлення. Розвиток комп'ютерної техніки і процесів мультимедіатизації створив передумови для розповсюдження концепцій, що нівелюють поняття стабільності і канонічності авторських текстів та акцентують увагу на їх варіативності й багатозначності тлумачень при сприйнятті аудиторією. Наприклад, стверджується, що модифікація і полісемія текстів, що розповсюджуються в засобах масової інформації, є однією з умов їх популярності. В залежності від обсягу полісемії т. поділяються на відкриті для нових інтерпретацій (див. текст відкритий) і закриті (див. текст закритий).

Т. відкритий /т. открытый/ [open t.] — 1) Текст, семантичне значення якого доступно; дані з доступним семантичним змістом. 2) Текст, який піддається множині різних інтерпретацій. До т. в. можна віднести, наприклад, новини м'які.

Т. закритий /т. закрытый/ [closed t.] — 1) Текст, семантичне значення якого недоступно; дані з недоступним семантичним змістом. 2) Текст, який не сприяє полісемії його сприйняття. До т. з. можна віднести, наприклад, новини тверді.

Т. листівки основний /т. листовки основной/ — елемент структури листівки, в якому міститься основний тезис листівки й сукупність аргументів, які його підтверджують. Для досягнення необхідного ефекту важливе значення має розташування інформації в т. л. о.: краще сприймається та інформація, яка розта-

шована в кінці (кульмінація) або на початку (антикульмінація), але не на середині тексту. Антикульмінація більш ефективна в тексті, який адресований ворожій (або байдужій) аудиторії, для впливу на яку необхідний сильний аргумент на початку тексту, який заставить дочитати його до кінця. Причому найкраще починати з відомостей, прийнятних для даної аудиторії, а потім уже переходити до аргументів, негативних з її точки зору. Кульмінація найбільш ефективна тоді, коли текст адресований зацікавленому, доброзичливому читачеві, для якого достатньо невеликого стимулу, щоб прочитати весь текст до кінця, де він очікує найвагоміших аргументів. В 50% людина пропускає т. л. о., якщо він довгий, важкослівний, набраний дрібним шрифтом. Тому листівки зі скороченою до мінімуму основною частиною мають, як правило, більшу силу впливу.

Т. повідомлення /т. сообщения/ [message t.] — частина повідомлення, яка містить фактичну інформацію, що направляється користувачеві, програмі або системі.

Т. програми усного мовлення основний /т. программы устного вещания основной/ — інформаційний зміст програми усного мовлення, що складається з різнорідних текстових елементів, з'єднаних між собою музичними (шумовими) елементами. Текст містить в собі інформацію або аргументацію впливу психологічного. Його мета — не пряма агітація, а підведення слухача до потрібного розуміння проблеми і до потрібних висновків. Основний текст повинен бути легким для розуміння, вразливим, переконливим, добре сприйматися на слух, бути прийнятним для слухачів з точки зору норм їхньої мови.

ТЕЛЕ... /теле.../ [tele...] (від грец. $\tau\tilde{\eta}\lambda\varepsilon$ — далеко) — у складних словах означає здійснюваний на відстані, той, що діє на далеку відстань, телевізійний.

ТЕЛЕБАЧЕННЯ (ТВ) /телевидение (ТВ)/ [TeleVision (TV)] (від теле... і ...бачення) — передавання на відстань зображень динамічних об'єктів за допомогою радіоелектронних пристроїв. У процесі розвитку т. створено різноманіття форм, засобів і функцій телевізійної індустрії, що знайшло своє відображення й у множині термінів і понять в комунікативістиці, що вивчає цей процес. Генетичні зв'язки з радіомовленням зафіксовані в позначення масового ефірного т. як широкомовної трансляції (broadcast t. over the air). Т.

поділяється на два основних типи — комерційне (commercial t.), що має прибутки в основному від реклами, і некомерційне (public t.), що функціонує за рахунок суспільних і приватних благодійних фондів, що зацікавлені в розповсюдженні культурно-просвітницької інформації. Кабельним стали називати т., що працює з антеною комунального користування (cable t. with community antenna). Іноді кабельне т. так і називають — Community Antenna TeleVision (CATV). На базі супутникових комунікацій (satellite communications) створюються кабельно-інформаційні комплекси типу Сі-ен-ен (Cable News Network — CNN), що займаються цілодобовим розповсюдженням новин в глобальному охопленні за допомогою космічних ретрансляційних пристроїв, до яких через спеціальні антени можуть підключатися індивідуальні абоненти. Очікується розповсюдження телевізійних приймачів з керуванням з будь-якої точки Землі і портативних пристроїв для підключення до супутникових ліній зв'язку різноманітних станцій від головних до ретрансляційних і рухомих. Поряд з розширенням глобального телевізійного інформаційного середовища відбувається і подальший розвиток телемовних зв'язків з інформаційними ресурсами комп'ютерних систем та інших засобів, в ході інтеграції яких виникають все нові й нові гібридні форми комфортного розповсюдження інформації (телегазети, пошта електронна, відеотекси, телетексти), відеоцентри для дому й офісів, наукових лабораторій, медичних і культурних закладів, що мають виходи у міжнародні комп'ютерні супермагістралі інформаційні. Оптимальні режими роботи телевізійних систем та результати їхнього впливу на аудиторію вивчаються комунікативістикою.

ТЕЛЕГРАФ /телеграф/ [telegraph] (від теле... і ...граф, від грец. $\gamma\rho\acute{\alpha}\varphi\omega$ — пишу, креслю, зображую) — заклад зв'язку, обладнаний комплексом пристроїв для зв'язку телеграфного.

ТЕЛЕКОМУНІКАЦІЇ /телекоммуникации/ (telecommunication(s)] (від теле... і комунікація) — загальна форма електронного обміну інформацією будь-якого типу (даних, телевізійних зображень, факсиміле і т. ін.). Т. складають інфраструктуру сучасної економіки. Одна з найбільш важливих тенденцій їхнього розвитку — процес злиття локальних, місцевих і глобальних мереж, який істотно впливає на масштабність економічних процесів, діяльність корпорацій і фірм. Це об'єднання здійснюється на основі технологій Ін-

тернету як найбільш зручного засобу взаємодії різноманітних інформаційних систем. Транспортна функція т. забезпечує високошвидкісне, надійне переміщення інформації і буде зростати разом із становленням глобальної економіки. В багатьох галузях т. стають необхідним елементом виробництва (банківська справа, телемаркетинг, комп'ютерне проектування і виробництво, торгівля і т. ін.).

ТЕЛЕКОНФЕРЕНЦЗВ'ЯЗОК /телеконференцсвязь/ [teleconferencing] (від теле..., конференція і зв'язок) — використання мереж обчислювальних для забезпечення комунікацій між розосередженими групами користувачів.

ТЕЛЕКОНФЕРЕНЦІЯ /телеконференция/ [teleconference] (від теле... і лат. conferentia від confero — збираю в одне місце) — інтегральний перелік послуг мережі обчислювальної, який використовується з метою комунікації користувачів на основі передавання і оброблення мовної, текстової інформації і відеоінформації.

ТЕЛЕКС /телекс/ [telex] (від теле... і англ. ex (change) — обмін) — міжнародна служба зв'язку, що забезпечує обмін повідомленнями між телеграфними апаратами (телетайпами) абонентів через комутований зв'язок загального призначення.

ТЕЛЕОБ'ЄКТИВ /телеобъектив/ [telephoto lens] (від теле... і об'єктив) — об'єктив з великою фокусною відстанню (300 — 4800 мм), призначений для спостереження (зйомки) на великій відстані від об'єкта спостереження.

ТЕЛЕТЕКС /телетекс/ [teletex] (від теле... і англ. tex) — система (служба) передавання літеро-цифрової ділової кореспонденції, що побудована за абонентським принципом, в якій як пункти абонентські використовуються комп'ютери персональні або спеціалізовані пристрої.

ТЕЛЕТЕКСТ /телетекст/ [teletext] (від теле... і англ. text) — система одностороннього широкомовного передавання текстової інформації на екрани телевізорів.

ТЕЛЕСКОП /телескоп/ [telescope] (від грец. $\tau\eta\lambda\varepsilon\sigma\kappa\acute{o}\pi\varnothing\varsigma$ – далекоглядний) — прилад для спостереження і дослідження небесних світил та їхнього фотографування.

Т. спеціальний /т. специальный/ [special t.] — телескоп для скритого спостереження віддалених об'є-

ктів. Обладнаний об'єктивом з великою фокусною відстанню. Великі т. с. встановлюються на спеціальному штативі з електроприводом. Дальність упізнавання наземних об'єктів може сягати 10 км.

ТЕЛЕТАЙП /телетайп/ [teletype] (англ. teletype, від грец. *τῆλε* — далеко і англ.- type — відбиток) телеграфний апарат для приймання повідомлень в цифро-літерній формі.

ТЕЛЕФАКС /телефакс/ [telefax] (від теле... і франц. fac-simile, від лат. fac simile — зроби подібне) — абонентська система, яка працює на базі телефонної мережі загального користування і призначена для передавання текстів.

ТЕЛЕФОН /телефон/ [telephone] — система електричних апаратів і пристроїв для телефонного зв'язку.

ТЕМБР /тембр/ [timbre, tone quality] (франц. timbre, від грец. *τύμανøν*) — барабан) — забарвлення звуку; якість за якою розрізняють звуки тієї самої висоти і завдяки якій звучання одного голосу або інструмента відмінне від іншого.

ТЕМПЕРАМЕНТ /темперамент/ [temperament] (від лат. temperamentum — узгодженість, устрій) — індивідуальні особливості людини, що виявляються в силі, швидкості, напруженості й врівноваженості перебігу її психічної діяльності, у порівняно більшій чи меншій стійкості її настроїв. Розрізняють чотири основні види т.: сангвінік, холерик, меланхолік і флегматик.

ТЕОРІЯ /теория/ [theory] (від грец. *ϑεωρία* — розгляд, дослідження) — 1) Логічне узагальнення практичного досвіду людей. 2) Система вірогідних наукових знань про якусь сукупність об'єктів, яка описує, пояснює і передбачає явища певної частини предметної. Т. є найдосконалішою формою відображення дійсності.

Т. алгоритмів /т. алгоритмов/ [algorithm t.] — розділ математики, який вивчає загальні властивості алгоритмів. Виділяють дві гілки теорії: логічну теорію, яка займається питаннями конструктивного обґрунтування математики і вивченням феномена алгоритмічної невирішеності проблем, і аналітичну теорію алгоритмів, зв'язану з вивченням самих алгоритмів, аналізом їхньої структури, методами еквівалентних

перетворень, способами побудови і оцінкою ефективності.

Т. забезпечення безпеки інформації /т. обеспечения безопасности информации/ — наукова дисципліна, яка з єдиних системних позицій вивчає методи попередження випадкового або навмисного розкриття, спотворення інформації, що зберігається, обробляється або передається в системах керування, що функціонують із застосуванням засобів техніки обчислювальної або мереж обміну інформацією. Вона об'єднує основні положення теорії алгоритмів, теорії інформації, теорії кодування, криптології і т.ін. .

Т. захисту інформації /т. защиты информации/ [data protection t.] — складова частина теорії інформаційної боротьби. Включає загальні положення, що визначають: предмет, завдання і зміст теорії; об'єкти і елементи захисту інформації; основні фактори, що впливають на зміст і ефективність захисту інформації, а також визначає та вивчає загрози інформації і методологічні основи її захисту, систему показників оцінки ефективності захисту інформації, загальну математичну модель захисту інформації, організаційно-технічні і правові основи захисту інформації.

Т. інформації /т. информации/ [information t.] — математична дисципліна, що вивчає властивості інформації та процеси її передавання. Т. і. фокусує увагу на таких аспектах зв'язку, як кількість інформації (даних), швидкість та коректність їхнього передавання, пропускна здатність каналу як стосовно інформації в каналі зв'язку, так і стосовно інформації в суспільстві. Т. і., сформульована математиком К. Шеноном у 1948 р., спочатку призначалася для інженерного зв'язку, але нині має відношення до різних сфер діяльності, включаючи комп'ютерну галузь.

Т. інформаційна /т. информационная/ [information t.] — математична дисципліна, що вивчає методи аналізу процесів інформаційних, насамперед при вивченні засобів масової інформації. Інформація розглядається як повідомлення, що передається від відправника до одержувача і долає при цьому шуми і завади. Задача зводиться до "зменшення невизначеності", і її рішення пов'язується з точністю й об'єктивністю статистичних методів дослідження, що доводять вимірюваність кількості і якості інформації, незважаючи на форми її виразу — від словесного до образного. В т. і. застосовуються наступні параметри — щільність,

ширина, глибина даних і читабельність, що залежить від надлишку інформації, відкритості чи закритості текстів, їх різноманітності, пов'язаної з мірою невизначеності результатів — ентропією і заданим обсягом потоку інформаційного. Можна, наприклад, вивчати обсяг цього потоку шляхом порівняння швидкості проходження словесних, музичних або візуальних образів в задані відрізки часу по різних каналах зв'язку і в різних країнах.

Т. інформаційного суспільства /т. информационного общества/ — наукова дисципліна, що вивчає об'єктивні основи і загальні закономірності становлення суспільства інформаційного, вплив технологій інформаційних і телекомунікаційних на різноманітні сфери життєдіяльності суспільства та роль державної політики в процесі переходу до інформаційного суспільства. Завданнями т. і. с. є: формулювання базових понять, що характеризують інформаційне суспільство; виявлення основних положень концепції інформаційного суспільства як типу суспільства, що виникло еволюційним шляхом з постіндустріальних суспільств; вивчення загальних закономірностей становлення інформаційного суспільства; визначення економічних, правових, соціально-культурних, технологічних основ інформаційного суспільства й піддавання їх філософсько-методологічному аналізові; виявлення методологічних принципів державної політики з формування інформаційного суспільства в державі та світі.

Т. інформаційної боротьби /т. информационной борьбы/ [information struggle t.] — система знань про характер, закони, закономірності, принципи, форми, способи підготовки і ведення боротьби інформаційної. Структуру т. і. б. визначають мета і завдання інформаційної боротьби, згідно яких вона може включати основи теорії інформаційної боротьби загальні, теорію ураження інформації і теорію захисту інформації.

Т. кодування /т. кодирования/ [coding t.] — розділ теорії інформації, що вивчає способи ототожнення повідомлень з сигналами (див. кодування).

Т. сил і засобів ураження інформації /т. сил и средств поражения информации/ — складова частина теорії ураження інформації, що визначає та вивчає показники оцінки ефективності ураження інформації,

математичну модель ураження інформації, стан підготовки і вирішення завдань ураження інформації.

Т. систем /т. систем/ [t. of systems] — галузь науки, пов'язана з вивченням систем з метою виявлення їхніх загальних характеристик і класифікації.

Т. складності обчислень /т. сложности вычислений/ — розділ теорії алгоритмів, що вивчає складність процесу застосування алгоритму до вихідних даних.

Т. ураження інформації /т. поражения информации/ — складова частина теорії інформаційної боротьби. Включає загальні положення і теорію сил і засобів ураження інформації. Загальні положення визначають предмет, завдання і зміст т. у. і., форми і способи ураження інформації, основні фактори, що впливають на зміст і ефективність ураження інформації.

Т. чисел /т. чисел/ — наука про цілі числа.

ТЕПЛОБАЧЕННЯ /тепловидение/ [infrared imaging, thermal imaging] — одержання видимого зображення тіл за їхнім тепловим (інфрачервоним) випромінюванням, власним або відбитим. Використовується для визначення форми і місцезнаходження об'єктів, що знаходяться в темряві або в оптично непрозорих середовищах.

ТЕПЛОВІЗОР /тепловизор/ [infrared imager, thermal imager, infrared (to visible) image converter] — прилад (система) теплобачення, в якому інфрачервоне (теплове) випромінювання від окремих точок об'єкта, що знаходиться в полі огляду, почергово спрямовується оптичною системою (об'єктивом) на світлоелектричний перетворювач, що перетворює його в електричні сигнали, які підсилюються і відображаються на екрані індикатора. Як правило індикатор показує не саму інтенсивність випромінювання, а її зміну відносно деякого середнього рівня. У сучасних т. для світло-електричного перетворення використовуються лінійки з фотодіодами (60–200 штук), що утворюють лінійку кадру. Розгортка по вертикалі (сканування) здійснюється шляхом механічного гойдання дзеркала, що направляє світлові промені від об'єктива до фотоприймача. Для пониження рівня шумів перетворювача здійснюється його охолодження рідкими газами в спеціальній посудині або спеціальними мікрогабаритними охолоджуючими пристроями, в яких реалізуються принципи

термоелектричного охолодження, розширення газу у вакуумі, термодинамічні цикли Стирлінга і т. ін.

ТЕПЛОЛОКАТОР /теплолокатор/ [InfraRed (IR) l.] — оптико-електронний пристрій для виявлення (розпізнавання) об'єктів (цілей) та визначення їхнього місцезнаходження за допомогою хвиль електромагнітних інфрачервоного діапазону. Т. — різновид оптичного локатора. Складається з оптичної системи, передавача, приймача, індикатора, блоків синхронізації та управління, джерела електроживлення. Як і радіолокатор, т. опромінює ціль електромагнітними хвилями, приймає частину відбитого від неї випромінювання, перетворює його у видиме зображення або в електричні сигнали. Пошук цілей та їхнє супроводження здійснюється шляхом синхронного огляду простору ІЧ променем передавача і миттєвим кутом поля зору приймача. Кутові координати виявленої цілі визначаються за положенням осі оптичної системи в момент візування цілі, а дальність — за часом проходження ІЧ випромінювання від т. і назад.

ТЕРМІН /термин/ [term] (лат. Terminus) — слово або словосполучення, що виражає певне поняття якоїсь галузі науки, техніки, мистецтва, суспільного життя тощо.

Т. абсолютний /т. абсолютный/ [absolute t.] — термін, що виражає тільки одне поняття.

Т. еквівалентний /т. эквивалентный/ [equivalent t.] — термін, який визначається на одній природній мові і за обсягом поняття відповідає терміну на іншій природній мові.

ТЕРМІНАЛ /терминал/ [terminal] (від лат. terminus — межа, край) — 1) Пристрій для взаємодії користувача або оператора з системою обчислювальною. 2) В мережах ЕОМ — пристрій, що є джерелом або одержувачем даних.

Т. індивідуальний (приватний) /т. индивидуальный (частный)/ [private t.] — термінал, що знаходиться в розпорядженні одного користувача; термінал індивідуального використання.

Т. користувача /т. пользователя/ [user t.] — термінал, призначений для індивідуальної роботи користувача.

ТЕРМІНОЛОГІЯ /терминология/ [terminology] (від термін і ...логія, що від грец. *λόγος* — слово, вчення) — 1) Розділ лексики, що охоплює терміни різних галузей знань. 2) Сукупність термінів якоїсь галузі науки,

техніки, мистецтва або всіх термінів даної мови.

ТЕРОРИЗМ /терроризм/ [terrorism] (франц. terrorisme від terreur, з лат. terror — страх, жах) — загроза або використання насильства в політичних цілях окремими особами або групами, які можуть діяти як на стороні, так і проти існуючого уряду, коли такі дії спрямовані на те, щоб вплинути на більше число людей, ніж безпосередні жертви. Т. є засобом впливу психологічного. Об'єктом т. є не ті, хто став жертвою, а ті, хто залишився живими. Його мета не убивство, а залякування і деморалізація живих, тобто, жертви — інструмент, убивство — метод.

Т. комп'ютерний /т. компъютерный/ [computer t.] — вид тероризму, що передбачає атаки інформаційні на обчислювальні центри, центри керування військовими мережами і медичними закладами, банківські та інші фінансові мережі, засоби передавання даних. Може здійснюватися з метою саботажу (урядових закладів і т. ін.), спричинення економічних збитків (виробничим корпораціям), дезорганізації роботи з потенційною можливістю смертей (атаки на аеропорти і т. ін.).

ТЕСТ /тест/ [test] (від англ. test — випробування) — стандартне завдання, метод випробування, що застосовується у різних галузях науки для одержання кількісної характеристики певних явищ.

Т. на простоту /т. на простоту/ [primality testing] — алгоритм вирішення задачі розпізнавання приналежності натурального числа до класу чисел простих. Розрізнюють тести на простоту детерміновані, ймовірнісні та гіпотетичні.

Т. на простоту гіпотетичний /гипотетический т. на простоту/ [hypothesis primality t.] — тест на простоту, який відноситься до детермінованих тестів на простоту, якщо деяка (покладена в його основу) гіпотеза справедлива, і до тестів на простоту ймовірнісних в противному випадку. Прикладом тесту на простоту гіпотетичного є тест Міллера.

Т. на простоту детермінований /т. на простоту детерминированный/ [deterministic primality t.] — алгоритм вирішення задачі розпізнавання належності натурального числа до множини чисел простих. Прикладами детермінованих тестів є тести тест пробного ділення (сито Ератосфена), тест просіювання в за-

гальному полі (Number Field Sieve Tets (NFST)) Босми, Ленстри та Коена та тест з використанням теорії еліптичних кривих Аткіна, Гольвассера та Кілліана.

Т. на простоту ймовірнісний /т. на простоту вероятностный/ [probable prime t.] — алгоритм імовірнісний вирішення задачі розпізнавання належності натурального числа до множини простих чисел. Прикладами ймовірнісних тестів є тести Ферма, Соловея-Штрассена, Міллера-Рабіна.

Т. на простоту ймовірнісний сильний /т. на простоту вероятностный сильный/ [strong probable prime t.] — назва тесту на простоту ймовірнісного Міллера-Рабіна, а також подібних до нього тестів на простоту, заснованих на використанні властивостей послідовностей Люкаса (сильний псевдопростий тест Люкаса) та тесту Фробеніуса.

Т. пробного ділення /т. пробного деления/ [t. of sampling dividing] — тест на простоту детермінований, відомий ще давньогрецькому математику Ератосфену (сито Ератосфена). Для тестування належності n до множини простих чисел з множини натуральних чисел, менших n, треба виключити всі парні числа, далі 3 та кожне третє число, далі 5 та кожне п'яте число і так далі усі числа, кратні першому за величиною елементу числового ряду на кожній ітерації. Цей процес повторювати до тих пір, доки перший за величиною елемент числового ряду на даній ітерації менший за $\sqrt{n}$. Числа, які залишилися, будуть співпадати з множиною простих чисел $A = \{p|\sqrt{n} < p \leq n\}$. Якщо $n \in A$, то n — просте число. Тест сита Ератосфена (зрозуміло не до $\sqrt{n}$) застосовується на практиці для попереднього відкидання складених чисел при тестуванні чисел великої розмірності на простоту.

Т. простоти /т. простоты/ — те ж, що тест на простоту.

ТЕСТУВАННЯ /тестирование/ [testing] — процес виконання тесту за певною методикою.

Т. на проникнення /т. на проникновение/ [penetration t.] — випробування, метою яких є здійснення спроби обминути або відключити механізми захисту.

Т. наступного біту /т. последующего бита/ [next-bit test] — тестування ансамблю. Ансамбль витримує т. н. б., якщо він є непередбачуваним.

ТЕТРАГРАМА /тетраграмма/ [tetragramm] (від грец. *τετράς* і *...γράμμα* — літера, написання) — послідовність з чотирьох символів алфавіту. Див. також поліграма.

ТЕХНІКА /техника/[engineering, technics, technique, equipment] (грец. *τεχνικός* — вправний, досвідчений, від *τέχøη* — майстерність, мистецтво) — 1) Певне коло наук, зв'язаних з вивченням і створенням засобів виробництва, знарядь праці. 2) Сукупність засобів праці, знань і діяльності, що розвиваються в системі суспільного виробництва, а також використання різних прийомів і методів впливу на природу в процесі виробництва матеріальних благ.

Т. зв'язку /т. связи/ [communication e.] — засоби зв'язку, засоби автоматизації зв'язку, засоби забезпечення зв'язку, рухомі засоби та предмети, призначені для оснащення системи зв'язку.

Т. інформаційна /т. информационная/ [hardware for information processing] — технічні прилади, призначені для збирання, реєстрації, зберігання, оброблення, передавання та відтворення інформації.

Т. криптографічна /т. криптографическая/ — засоби, призначені для перетворення інформації криптографічного.

Т. обчислювальна /т. вычислительная/ [computer science, computing machinery] — 1) Галузь техніки, що об'єднує засоби автоматизації обчислень і оброблення інформації в різноманітних сферах людської діяльності. 2) Наука про принципи побудови, дії і проектування цих засобів.

ТЕХНОКРАТІЯ /технократия/ [technocracy] (від грец. *τέχνη* (техно...) — майстерність і *κράτøς* (...кратія) — сила, влада) — влада, зосереджена в руках професіоналів — фахівців в галузі техніки і технічних наук, менеджменту і т.ін. з метою найкращого використання результатів і можливостей техніко-технологічної революції. Технократична теорія стала частиною сучасної західної соціології, відображена в концепціях суспільства індустріального, суспільства постіндустріального і т. ін.

ТЕХНОЛОГІЯ /технология/ [technology] (від грец. *τέχνη* (техно...) — майстерність і ...логія, що від грец. *λόγøς* — слово, вчення) — сукупність взаємозв'язаних способів обробки матеріалів, виготовлення виробів і

процесів, що супроводжують ці види робіт.

Т. високі /т. высокие/ [high tech] — термін для ускладнених, часто комплексних та спеціалізованих, технічних нововведень.

Т. влади /т. власти/ [t. of power] — сукупність, система тих чи інших способів діяльності влади, розрахована на досягнення необхідного (заданого, задуманого) результату. Різноманітні т. в. включають способи як досягнення негайного, локального, короткочасного ефекту, так і одержання результату вирішального, великомасштабного, фундаментального, довготривалого, стратегічного.

Т. добування інформації /т. добывания информации/ — сукупність взаємопов'язаних методів, засобів та заходів, об'єднаних в певну послідовність для реалізації процесу добування інформації. Т. д. і. передбачає наступні етапи: організація добування інформації; добування даних і відомостей; робота інформаційна (оброблення інформації); доведення інформації до споживача.

Т. інформаційні /т. информационные/ [information t.] — сукупність методів, процесів і програмно-технічних засобів, об'єднаних в технологічну послідовність, що забезпечує збирання, зберігання, оброблення, виведення і розповсюдження (доведення) інформації для зниження трудомісткості процесів використання ресурсу інформаційного, підвищення їхньої надійності і оперативності.

Т. інформаційні нові /т. информационные новые/ — технології, що визначають характер людської діяльності в новому суспільстві інформаційному, яке в кінці 20-го сторіччя приходить на зміну індустріальному суспільству. Центральне завдання створення т. і. н. — це пошук технологій, які би з послідовності "завдання-рішення" виключили би людей, що спеціально зайняті перетворенням завдань в форму, зрозумілу для ЕОМ. Це завдання вирішується при передаванні функцій програмістів прикладних, а потім і аналітиків ЕОМ. Для цього необхідно розробити засоби взаємодії кінцевого користувача з ЕОМ, які одержали назву інтелектуального (дружнього) інтерфейсу.

Т. інформаційні спеціальні (СІТ) /т. информационные специальные (СИТ)/ — технології інформаційні, призначені для забезпечення інформаційного відокремлення реальних систем інформаційних. СІТ

являють собою сукупність процедур формування (рецепції), інтерпретації (перетворення, пошуку, реорганізації) і комунікації (передавання, зберігання) інформації на основі використання проблемно-орієнтованої бази даних і знань (БДЗ), елементами якої є логіко-лінгвістична модель предметної частини, раціональна стратегія, продукційні правила і комплекс ефективних алгоритмів вироблення рішень, а також засоби діалогу з оператором-парапрограмістом, які дозволяють йому заповнювати (уточнювати) фактографічний зміст БДЗ та інтерпретувати результати. Розробка і впровадження нових СІТ повинна базуватися на інфраструктурі виробництва конкретної держави, враховуючи ментальність і рівень технічної культури персоналу систем управління. Особливе значення така стратегія розвитку СІТ набуває в умовах підсилення взаємодії протиборчих сторін на всіх рівнях, часткової інтеграції і нав'язування неприйнятних або малоефективних моделей функціонування систем.

Т. інформаційно-комунікаційні (ІТТ) /т. информационно-коммуникационные (ИТТ)/ — те ж, що технології інформаційні.

Т. політичні /т. политические/ [political t.] — сукупність цілеспрямованих дій, орієнтованих на досягнення заданого політичного результату, метод "переведення" об'єктивних законів політики в механізм управління, тобто переведення абстрактної мови політичної науки на конкретну мову рішень, документів, приписів, що регламентують діяльність людей і стимулюють їх на найбільш ефективне досягнення поставленої мети.

ТИП /тип/ [type] (франц. type від грец *τύπος* — 1) Зразок, модель для групи предметів; вид, рід, різновидність чого-небудь. 2) Форма чого-небудь, що має певні ознаки.

Т. доступу /т. доступа/ [access t.] — суттєвість доступу до об'єкта, що характеризує зміст здійснюваної взаємодії, а саме: проведені дії, напрям потоків інформації, зміни в стані системи (наприклад, читання, запис, запуск на виконання, видаляння, дозапис).

ТОВАРИСТВО /сообщество/ [community] — об'єднання людей, народів, держав, що мають загальні

інтереси, цілі.

Т. Інтернету /с. Интернета/ [Internet Society (ISOC)] — група професіоналів і експертів, що координує життєдіяльність і розвиток Інтернету. Основна діяльність ISOC — розроблення стандартів і протоколів (див. група Інтернету консультативна технічна) разом з іншими організаціями.

Т. розвідувальне /с. разведывательное/ [intelligence c.] — об'єднання різноманітних служб розвідувальних в межах однієї держави. Наприклад, в США т. р. об'єднує більше 12 розвідувальних служб.

ТОКЕН /токен/ [token] — засіб захисту інформації, який використовується в процесі автентифікації для підтвердження особи або прав доступу.

eToken /eToken/ [eToken] — повнофункціональний аналог інтелектуальної картки, виконаний у вигляді брелока; з'єднується з ЕОМ крізь USB-порт та не вимагає додаткового пристрою зчитування/запису.

ТРАКТ /тракт/ [path] (від лат. tractus — волочіння, низка, протяжність) — сукупність пристроїв, що утворюють шлях слідування чого-небудь.

Т. зв'язку /т. связи/ — сукупність пристроїв, які забезпечують передавання повідомлень від джерела до одержувача, а також джерело повідомлень, одержувач повідомлень і лінія зв'язку (лінія передавання), по якій проходить сигнал. Т. з., в якому здійснюється перетворення повідомлень в сигнал і прийнятого сигналу в повідомлення, називається системою одностороннього зв'язку. В системі двостороннього зв'язку передача повідомлень здійснюється в обох напрямках.

Т. передавання даних /т. передачи данных/ [data transmission p.] — тракт,що створюється при передаванні інформації від користувача до користувача. Склад тракту визначається маршрутом повідомлення: користувач 1 — елемент автоматизованої системи 1 — система передавання даних — елемент автоматизованої системи 2 — користувач 2. Елементи автоматизованої системи — станції робочі, сервери комунікаційні. Елементи системи передавання даних — апаратура передавання даних, канали зв'язку, вузли комутації.

Т. передавання інформації /т. передачи информации/ [data transmission p.] — сукупність каналів зв'язку, організованих в лініях зв'язку різноманітного типу за допомогою апаратури ущільнення, пристроїв

перетворення сигналів (модемів) і пристроїв підвищення вірогідності.

ТРАНСЛЯТОР /транслятор/ [translator] (лат. translatio — перенесення) — 1) Проміжний пристрій для підсилення, перетворення й передавання сигналів електричних зв'язку, радіосигналів, телевізійних тощо. 2) Програма або технічний засіб ЕОМ, призначені для перекладу описів алгоритмів з однієї формальної мови на іншу.

ТРАНСП'ЮТЕР /транспьютер/ [transputer] (від transistor і computer) — схема інтегральна надвелика, яка має процесор, засоби міжпроцесорного зв'язку, власну пам'ять оперативну і засоби доступу до пам'яті зовнішньої.

ТРАНСПОРТУВАННЯ /транспортировка/ [transport] (від лат. transporto — переношу, переміщую) — перевезення кого-, що-небудь з одного місця в інше.

Т. ключів /т. ключей/ [key t.] — методи встановлення ключа, при яких ключ генерується одним з абонентів та передається іншому (іншим).

ТРАНС... /транс.../ [trans...] (лат. префікс trans...) — префікс, що означає "крізь", "через", "за", "пере", "по той бік".

ТРАНСДЕЗІНФОРМУВАННЯ /трансдезинормирование/ (від транс... і дезінформування) — передавання органу керування трансдезінформації (інформація про неправдиву обстановку, перетворена в інформацію про правдиву обстановку).

ТРАНСІНФОРМУВАННЯ /трансинформирование/ (від транс... і інформування) — передавання органу керування трансінформації (інформація про істинну обстановку, трансформована в інформацію про неправдиву обстановку).

ТРАНСФОКАТОР /трансфокатор/ [variable magnification zoom lens, zoom] (від лат. префікса trans... — крізь, через, за і фокус) — оптична система, що складається з афокальної насадки зі змінним, плавним збільшенням зображення і об'єктива з постійною фокусною відстанню.

ТРАНСФОРМАЦІЯ /трансформация/ (лат. transformatio) — зміна, перетворення виду, форми, істотних

властивостей чого-небудь.

ТРАСУВАННЯ /трассирование/ [tracing] — проведенні лінії, що вказує напрямок проходження, проляга-ння чогось.

Т. маршрутизації /т. маршрутизации/ — процедура одержання інформації про маршрутизатори (вузли), через які проходять пакети до комп'ютера (здійснюються командою tracert). Дозволяє виявити помилки маршрутизації, наприклад, "зациклення" — передавання пакетів від хоста до хоста по колу.

ТРАФІК /трафик/ [traffic] — потік повідомлень в мережі передавання даних; робоче навантаження лінії зв'язку.

Т. інформаційний /т. информационный/ [information t.] — 1) Див. трафік. 2) В комунікативістиці — термін, що одержав активне застосування в дослідженнях проблем керування і контролю, які виникають в різноманітних інформаційних системах і мережах, а особливо складними стають в супермагістралях інформаційних (наприклад, керування трафіком, контроль трафіка тощо).

ТРЕТЯ СТОРОНА /третья сторона/ [third party] — особа або орган, які визнаються незалежними від сторін учасників у питанні, що розглядається.

Т. С. надійна /т. с. надежная/ [Trusted T. P. (TTP)] — третя сторона, яка використовується іншими сторонами для служб верифікації.

ТРИВОГА /тривога/ — емоційний стан, що виникає в ситуаціях з неясним кінцем і зв'язаний з очікуванням неблагополучного розвитку подій. Т. може проявлятися як відчуття безпорадності, невпевненості у собі, безсилля перед зовнішніми факторами, як перебільшення їхньої могутності і небезпечності. Поведінкові прояви т. полягають в загальній дезорганізації діяльності, що порушує її спрямованість і продуктивність.

ТРИГРАМА /триграмма/ [trigram] (від грец. *τρεῖς* — три і *...γράμμα* — літера, написання) — послідовність з трьох символів алфавіту. Див. також поліграма.

ТРОПОСФЕРА /тропосфера/ [troposphere] (від грец. *τρόπøς* — поворот і *σφαῖρα* — куля, сфера) — приземна частина атмосфери на висоті до 8–10 км у помірних широтах і до 16–18 км біля екватора.

ТРОЯНСЬКА МАТРЬОШКА /троянская матрешка/ — різновид троянського коня, особливістю якого є те, що у фрагмент програми вставляються не команди, котрі самі виконують несанкціоновані операції, а команди, котрі формують ці команди і після виконання своєї функції, тобто коли вже автоматично на програмному рівні створений троянський кінь, самоліквідуються. Інше визначення: т. м. — програмні модулі-фрагменти, які створюють троянського коня і самоліквідуються на програмному рівні по закінченню виконання свого завдання.

ТРОЯНСЬКИЙ КІНЬ /троянский конь/ [trojan horse] — програма, яка в доповнення до основних (проектних і документованих) надає додаткові, але не описані в документації функціональні можливості, спрямовані на те, щоб обійти контроль доступу і привести до несанкціонованого знищення, блокування, модифікації або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ або їхні мережі. Ці можливості можуть самоліквідуватись, що робить неможливим їхнє виявлення, або ж можуть реалізуватися постійно, але існувати потай. За характером загрози т. к. належить до загроз активних, що реалізуються програмними засобами, які працюють у пакетному режимі. Найбільш небезпечним є опосередкований вплив, при якому т. к. діє в межах повноважень одного користувача, але в інтересах іншого користувача, встановити особу якого інколи неможливо. Див. закладка.

Т. К. в електронних колах /т. к. в электронных цепях/ — створення певних логічних зв'язків в електронних колах апаратних засобів комп'ютерної техніки для автоматичного виконання несанкціонованих маніпуляцій за аналогією з програмною реалізацією троянського коня.

ТРОЯНСЬКИЙ ЧЕРВ'ЯК /троянский червь/ — різновид троянського коня, особливістю якого є те, що в нього закладений алгоритм саморозмноження, програмне автоматичне відтворення троянського коня. Програми-черв'яки автоматично копіюють себе в пам'яті одного або декількох комп'ютерів (при наявності комп'ютерної мережі) незалежно від інших програм. При цьому використовується тактика вірусів комп'ютерних (див. вірус-черв'як).

ТУНЕЛЮВАННЯ /туннелирование/ [tunneling] — процес, в ході якого створюється логічне з'єднання

між двома кінцевими точками. Тунелі, звичайно, описуються у віртуальних приватних мережах, де дві кінцеві точки здійснюють комунікацію за допомогою інкапсуляції різних протоколів.

Т. багатоточкове /т. многоточечное/ [multipoint t.] — тунелювання, створене на основі технології мереж віртуальних приватних, яке допускає багато сеансів усередині тунелю.

У

УДАР /удар/ [thrust] — форма оперативного (бойового) застосування військ (сил) в операції і бою. Полягає в короткочасному потужному ураженні противника ядерною, звичайною зброєю або наступом військ (у. військами). За масштабами у. можуть бути стратегічними, оперативними і тактичними, а в залежності від застосованих засобів — ядерними (ракетно-ядерними) і вогневими (артилерійськими, ракетними, авіаційними).

У. інформаційний /у. информационный/ [information t.] — короткочасний потужний узгоджений інформаційний вплив сил і засобів на найбільш важливий елемент (елементи) системи управління (керування) противника для досягнення рішучих цілей із завоювання інформаційної переваги (зниження інформаційної переваги противника). У. і. можна класифікувати за масштабом (стратегічні, оперативно-стратегічні, оперативні, оперативно-тактичні, тактичні), типами (радіоелектронні, радіоелектронно-вогневі, комп'ютерні, спеціальні і комбіновані) і ступенем зосередження сил і засобів (вибіркові, зосереджено-масовані і масовані).

У. комп'ютерний (програмний) /у. компьютерный (программный)/ [computer (program) t.] — узгоджений за часом, глибиною і завданнями масований комплексний вплив атакуючих сил і засобів деструктивного програмно-математичного впливу на об'єкти АСК противника з метою зриву управління на окремих напрямках (або з окремих пунктів) на певний час.

У. радіоелектронний /у. радиоэлектронный/ [radio-electronic t.] — узгоджений за часом, глибиною та завданнями масований комплексний вплив різноманітних сил і засобів радіоелектронного придушення і функціонального ураження радіоелектронних об'єктів системи керування противника з метою зриву

управління на окремих напрямках (або з окремих пунктів управління) на певний час.

У. радіоелектронно-вогневий /у. радиоэлектронно-огневой/ [electronic and fiery t.] — узгоджений за часом, глибиною та завданнями масований комплексний (радіоелектронний і вогневий) вплив сил і засобів РЕБ, ракетних військ і артилерії, авіації та інших сил і засобів, виділених для боротьби з системами керування противника, з метою зриву управління на окремих напрямках на певний час.

У. спеціальний /у. специальный/ [special t.] — узгоджений за часом, глибиною завданнями масований комплексний морально-психологічний вплив залучених до ведення боротьби інформаційної сил і засобів на особовий склад (насамперед на персонал органів управління) угруповання противника з метою зриву (утруднення) управління на окремих напрямках на певний час.

УМОВА /условие/ [condition, specification] — 1) Обставина, від якої будь-що залежить. 2) Обстановка, в якій відбувається, здійснюється що-небудь.

У. розвідувального контакту /у. разведывательного контакта/ — умови, за яких стає можливим розвідувальний контакт. Поділяються на просторові, енергетичні і часові.

У. розвідувального контакту енергетична /у. разведывательного контакта энергетическое/ — умова, що передбачає забезпечення на вході розвідника приймача відношення сигнал/завада, достатнього для одержання на його виході інформації з необхідною якістю.

У. розвідувального контакту просторова /у. разведывательного контакта пространственное/ — умова, що передбачає таке просторове розташування розвідника відносно джерела інформації, при якому розвідник “бачить” джерело інформації.

У. розвідувального контакту часова /у. разведывательного контакта временное/ — умова, що передбачає необхідність функціонування органу добування інформації синхронно з роботою джерела інформації.

УМОВИВОДИ /умовыводы/ [inference] — розумова діяльність на основі властивих індивідуальній свідо-

мості норм висновків, які співпадають багато в дечому з правилами і законами логіки.

У. логічний /у. логический/ [logical i.] — функція систем експертних, яку ще називають вбудованою машиною логічного висновку. Ця машина зіставляє ствердження з фактами бази знань (або бази даних) і намагається генерувати висновок, оснований на узгоджених із твердженням фактах.

УПРАВЛІННЯ /управление/ [management, control, agency] — 1) Направлення ходу, руху кого-, чого-небудь. 2) Діяльність органів державної влади. 3) Великий підрозділ якого-небудь закладу, велика адміністративна установа (наприклад, управління розвідувальне Центральне — координуючий центр товариства розвідувального США). 4) Будь-яка керуюча діяльність. У. має багато видів, форм, характеристик (державне, стратегічне, централізоване, наукове і т. ін.).

У. даними /у. данными/ [data m.] — сукупність функцій забезпечення необхідного представлення даних, їхнього накопичення і зберігання, поновлення, вилучення, пошуку і видачі.

У. державне /у. государственное/ [State administration, government m.] — одна з форм діяльності держави, яка виражається в практичній реалізації законів, в організації суспільних відносин з метою забезпечення державних інтересів і політики, що проводиться державою.

У. інформацією /у. информацией/ [information m.] — 1) Назва галузі досліджень, спрямованих на виявлення конкретних форм і засобів регулювання процесів вибору і розповсюдження інформації каналами зв'язку (засобами масової інформації). 2) Керуюча діяльність щодо процесів інформаційних, яка включає збирання (добування), оброблення та розповсюдження (доведення) інформації. Важливу роль в у. і. відіграють зворотні зв'язки з рівня споживання інформації на рівні оброблення та добування.

У. ключами /у. ключами/ [key m.] — те ж, що керування ключами.

У. мережею адміністративне /у. сетью административное/ [network m.] — функції управління мережею обчислювальною, зв'язані з умиканням і вимиканням системи, каналів передавання даних, терміналів, з діагностикою несправностей, збором статистики, підготовкою звітів і т. ін.

У. ризиком /у. риском/ [risk m.] — сукупність заходів, що проводяться протягом усього життєвого ци-

клу системи автоматизованої щодо оцінки ризику, вибору, реалізації й упровадження заходів забезпечення безпеки, спрямована на досягнення прийнятного рівня ризику залишкового.

У. розвідувальне /у. разведывательное/ — в багатьох країнах так називаються керівні органи розвідки, призначені для координації розвідувальної діяльності підпорядкованих їм сил і засобів розвідки.

У. розвідувальне Центральне (ЦРУ) /у. разведывательное Центральное (ЦРУ)/ [Central Intelligence Agency (CIA)] — одна з найпотужніших організацій США, що займається збиранням і обробленням інформації розвідувальної та розповсюдженням по світу впливу США за допомогою операцій таємних. ЦРУ є керівним і координуючим центром товариства розвідувального США. Вона єдиний орган розвідки, що має адміністративну самостійність. На директора ЦРУ покладені обов'язки підсилення потенціалу всього розвідувального товариства. Він як директор центральної розвідки США несе відповідальність перед президентом і Радою національної безпеки за здійснення усіх операцій розвідувальних за національною програмою.

УРАЗЛИВІСТЬ /уязвимость/ [vulnerability] — 1) Чутливість до чогось, легке піддавання дії, впливові чого-небудь. 2) Властивість будь-чого легко і швидко піддаватися дії зовнішніх впливів.

У. системи /у. системы/ [system v.] — нездатність системи протистояти реалізації певної загрози або сукупності загроз. В. с. може бути наслідком неадекватного проектування чи неповного налагодження системи або результатом злого наміру, наприклад, при наявності "троянського коня".

У. мережі обміну інформацією /у. сети обмена информацией/ — характеристика мережі обміну інформацією, що обумовлює можливість виникнення загрози її безпеці.

УСТАНОВКА /установка/ [unit, equipment, plant] — 1) Встановлений, змонтований будь-де механізм, пристосування, або система механізмів, пристосувань. 2) Стан внутрішньої готовності (налаштованості) людей на специфічний для них прояв почуттів, інтелектуально-пізнавальної і вольової активності, динаміки й характеру спілкування, предметно-практичної діяльності і т. ін., який відповідає наявним у них потребам.

У. рентгенівські /у. рентгеновские/ [X-ray u.] — засоби на основі рентгенівських апаратів, призначені

для просвічування предметів, призначення яких не вдається виявити без їхнього розбирання, насамперед, тоді, коли розбирання неможливе без руйнування предмета. Для просвічування предметів застосовують переносні флюороскопи з відображенням зображень на екрані приставки для перегляду та рентгенотелевізійні установки.

УЯВА /воображение/ — психічний процес. Виражається в побудові образу засобів і кінцевого результату діяльності суб'єкта, у створенні програми поведінки в невизначеній ситуації, у створенні образів, що відповідають опису об'єкта.

УЯВЛЕННЯ /представление/ — чуттєво-наочний образ предметів або явищ дійсності, що зберігається й відтворюється у свідомості людини поза безпосереднім їхнім впливом на органи чуттів.

Ф

ФАГ /фаг/ — див. поліфаг.

ФАЙЕРВОЛ /файэрвол/ [firewall] — системний компонент, який виконує роль шлюзу для фільтрації пакетів у мережі, тим самим реалізує принцип брандмауера. На жаргоні системних адміністраторів ф. називається стіною.

ФАЙЛ /файл/ [file] — 1) Ідентифікована сукупність екземплярів описаного в програмі типу даних, що знаходяться в зовнішній пам'яті і доступних програмі після проведення спеціальних операцій. 2) В мікроЕОМ — пойменована область у зовнішній пам'яті.

Ф. захищений /ф. защищенный/ [protected f.] — файл, для доступу до записів якого необхідно ввести пароль.

Ф. обліковий /ф. учетный/ [accounting f.] — файл, що містить відомості про використання ресурсів обчислювальної системи її користувачами.

ФАКТ /факт/ [fact] (від лат. factum — зроблене) — 1) Дійсна подія, вище. 2) Реальність, дійсність.

ФАКТОР /фактор/[factor] (лат. factor — той, що робить, від facio — роблю) — умова, рушійна сила, причина будь-якого процесу.

Ф. дестабілізуючі /ф. дестабилизирующие/ [destabilizing f.] — явища та процеси природного і штучного походження, що породжують загрози інформаційні. Джерелами ф. д. можуть бути як окремі особи, так і організації, об'єднання. До найбільш сильних із них відносяться ворожі держави або коаліції — в них для формування інформаційних загроз створюються і функціонують спеціальні органи і служби. Особливу групу джерел складають інформаційні системи і засоби, оскільки вони одночасно є знаряддям приведення в дію інформаційних загроз, каналом їхнього проникнення у свідомість особистості або суспільну свідомість і генератором спонтанних загроз, що виникають внаслідок технічних несправностей і інших причин. Джерелом ф. д. може бути також природне середовище. Кожному джерелу притаманні певні види ф. д., які можна представити двома групами: фактори дестабілізуючі міждержавні і фактори дестабілізуючі внутрідержавні. Сукупність джерел разом із властивими їм видами ф. д. формують цілий спектр інформаційних загроз, що впливають на стан інформованості особистості, суспільства і держави. До них відносяться: викрадення, знищення, втрата, приховування, спотворення, розголошення, фальсифікація, компрометація корисної (істинної) інформації, а також фабрикування, розповсюдження і впровадження дезінформації.

Ф. дестабілізуючі внутрідержавні /ф. дестабилизирующие внутригосударственные/ — правовий вакуум у більшості питань забезпечення безпеки інформаційної; навмисне або ненавмисне порушення законодавства з питань інформаційної безпеки; політичні конфлікти; зловмисні дії злочинних елементів або груп; відмови, збої, технічні помилки систем інформаційних (засобів); природні явища (процеси), що утруднюють одержання, передачу, прийом і зберігання інформації або руйнують інформаційні системи.

Ф. дестабілізуючі міждержавні /ф. дестабилизирующие межгосударственные/ — конфлікти різноманітних масштабів і проявів (економіка, політика, ідеологія, дипломатія і т. ін.).

Ф. захисту інформації системостворюючі /ф. защиты информации системообразующие/ — фактори, які повинні визначати структуру і функціонування системи захисту інформації. До таких факторів

відносяться: переліки відомостей, які складають таємницю державну і комерційну; необхідні рівні безпеки інформації, забезпечення яких не приведе до перевищення збитків над витратами на захист інформації; загрози безпеці інформації; обмеження, які необхідно враховувати при створенні або модернізації системи захисту інформації; показники, за якими буде оцінюватися ефективність системи захисту.

ФІДЕР /фидер/ [feeder] (англ. feeder, від feed — живити) — електричне коло і допоміжні пристрої, за допомогою яких енергія сигналу радіочастотного підводиться від радіопередавача до антени або від антени до радіоприймача.

ФІКСАЦІЯ (ФІКСУВАННЯ) /фиксация (фиксирование)/ [fixing, fixation] (від франц. fixation — закріплювання, встановлення) — 1) Запис, реєстрація, встановлення чого-небудь; зосередження уваги на чомусь. 2) Закріплення чого-небудь у певному положенні.

Ф. контролю засобів захисту /ф. контроля средств защиты/ [security audit trail] — сукупність відомостей про стан засобів захисту, що накопичуються з часом і призначені для спрощення керування засобами захисту.

ФІЛОСОФІЯ /философия/ [philosophy] (від грец. *φιλøσøφία* — любов до мудрості) — 1) Форма суспільної свідомості, яка виробляє загальний цілісний погляд на світ і місце людини в ньому, досліджує відношення мислення до буття, практичне, пізнавальне, ціннісне, етичне та естетичне відношення людини до світу. 2) Методологічні принципи, покладені в основу певної науки,галузі знання (наприклад, ф. математики, ф. права).

Ф. інформаційного суспільства /ф. информационного общества/ — напрям у філософії, оснований на нових філософських концепціях об'єднання кібернетики, інформатики і синергетики з класичною теорією розвитку.

Ф. користувачів Інтернету /ф. пользователей Интернета/ [p. of Internet users] — комплекс ідей, що виникають внаслідок впливу віртуальної образності комп'ютерного моделювання, яке створює ілюзії умовності часу і простору, реалій і цінностей життя і надмогутності медіа електронних нових.

ФІЛЬТР /фильтр/ [filter] (франц. filtre, від лат. filtrum — повсть) — 1) Електронний, електромеханічний, механічний пристрій або програма, призначені для розділення (відділення) чого-небудь. 2) У зв'язку та радіоелектроніці ф. — апаратні або програмні засоби, які вибірково передають тільки певні елементи сигналу і виключають або мінімізують інші. Найчастіше використовують частотні фільтри: фільтри нижніх частот, фільтри верхніх частот і фільтри із смугою пропускання (фільтри смугові). 3) Програма, що запобігає проникненню в базу даних, програму або систему некоректних даних.

Ф. верхніх частот (ФВЧ) /ф. верхних частот (ФВЧ)/ [high pass f.] — фільтр частотний, що має смугу пропускання вище заданої частоти зрізу і смугу затримування для більш низьких частот.

Ф. гребінчастий /ф. гребенчатый/ [comb f.] — фільтр частотний, що має декілька смуг пропускання і затримування, розташованих по черзі. **Ф. інформаційний** /ф. информационный/ [data f.] — програмний засіб поточного контролю за поведінкою найбільш важливих даних.

Ф. канальні /ф. канальные/ [circuit f.] — екрани міжмережні, що займають середнє положення між фільтрами пакетними і фільтрами прикладного рівня. Ф. к. зберігає деякі дані про попередні пакети і рішення по маршрутизації наступного пакета приймає, як на основі використання цих даних, так і на основі вмісту пакета. У правилах фільтрування можна враховувати як адреси відправника і одержувача, так і тип обслуговування. К. ф. реалізуються у вигляді шлюзів: клієнт зв'язується з фільтром, який від імені клієнта взаємодіє із зовнішніми серверами.

Ф. коаксіальний /ф. коаксиальный/ [coaxial f.] — фільтр, що складається з відрізків коаксіальних ліній передавання і застосовується для селекції сигналів у дециметровому і сантиметровому діапазонах хвиль.

Ф. мережний /ф. сетевой/ [power-line f.] — фільтр частотний, призначений для придушення небезпечних сигналів, що розповсюджуються мережами електроживлення, на вході (виході) силового кабелю в контрольовану зону. Ф. м. являють собою фільтри нижніх частот з частотою зрізу біля 50 Гц, що забезпечують мале загасання струму електроживлення і високе — мовних і більш високочастотних сигналів.

Ф. м. мають різноманітні конструкції в залежності від струму електроживлення і характеристик фільтра. Для зменшення паразитного зв'язку між входом і виходом через магнітні і електричні поля котушки і конденсатори фільтра розташовуються в корпусі (екрані).

Ф. нижніх частот (ФНЧ) /ф. нижних частот (ФНЧ)/ [low pass f.] — фільтр частотний, що має смугу пропускання нижче заданої частоти зрізу і смугу затримування для більш високих частот.

Ф. пакетні /ф. пакетные/ [packet-level f.] — екрани міжмережні, які блокують або пропускають пакети виключно на основі їхніх властивостей (адреса і порти джерела і одержувача) і не запам'ятовують минулого стану. Цей тип міжмережного екрана найпростіший в реалізації та обслуговуванню і майже ніяк не впливає на пропускну здатність мережі. Проте рівень такого захисту невисокий. Так, наприклад, правила фільтрування можна обійти, використовуючи вкладення протоколів. Тобто, якщо заборонений протокол HTTP, але дозволений протокол Telnet, то для проходження HTTP-трафіка його можна вложити в сеанс Telnet.

Ф. пасивний /ф. пассивный/ [passive f.] — фільтр частотний, який не має підсилюючих елементів.

Ф. прикладного рівня /ф. прикладного уровня/ [application-level f.] — виділені екрани міжмережні, які функціонують на рівні прикладному моделі взаємодії відкритих систем і відокремлюють внутрішню мережу від Інтернету. Фактично клієнт не може виявити, що взаємодіє з міжмережним екраном, який в цьому випадку називають сервером проксі прикладним. З іншої сторони, міжмережний екран "прикидається" клієнтом і пересилає прийняті клієнтські запити справжньому серверові. Але спочатку міжмережний екран на основі заданих правил вирішує питання про допустимість такого запиту і наявність у клієнта права на дії, що запитуються.

Ф. режекторний /ф. режекторный/ [eliminator, rejector, trap] — фільтр частотний, який має смугу затримування, що розташована між двома заданими смугами пропускання.

Ф. слідкуючий /ф. следящий/ [swept f., tracking f.] — фільтр частотний, у якого середня частота

смуги пропускання (затримування) автоматично підтримується рівною середній частоті вхідного сигналу.

Ф. смуговий /ф. полосовой/ [band pass f.] — фільтр частотний, що має смугу пропускання, розташовану між двома частотами зрізу.

Ф. цифровий /ф. цифровой/ [digital f.] — цифровий пристрій, призначений для розподілу коливань різних частот. Для побудови довільного лінійного ц. ф. з постійними параметрами досить мати лише три базові цифрові пристрої — елемент затримки, помножувач, та суматор, які виконують такі операції: затримку сигналу на один відлік, помноження відліку на константу (його зважування), додавання відліків на кожному такті. Ф. ц. з колами зворотного зв'язку називаються рекурсивними, в протилежному випадку — нерекурсивними.

Ф. частотний /ф. частотный/ [frequency f.] — схема, коефіцієнт загасання якої в певних смугах частот менший або більший, ніж на усіх інших частотах.

ФІЛЬТРАЦІЯ (ФІЛЬТРУВАННЯ) /фильтрация (фильтрование)/ [filtration] (франц. filtration) — процес зміни (спотворення) новин (інформації) при проходженні їх через різні стадії журналістської (інформаційної діяльності), коли "інформація з перших рук" (first-hand) попадає у другі руки (second-hand), а потім і в треті і мимоволі в результаті перетворюється в тому чи іншому плані. Визнання неминучості ф., фактично ставиться під сумнів повну об'єктивність новин.

ФІРМА /фирма/ [firm] (італ. firma, букв. — підпис, від лат. firmus — міцний, надійний) — найменування господарського, торговельного чи промислового підприємства.

Ф. підставна /ф. подставная/ — приватна комерційна організація, здатна займатися реальною підприємницькою діяльністю, але насправді заснована і контрольована спеціальними службами. Зв'язок такої фірми з розвідкою, звичайно, замовчується.

ФЛЕГМАТИК /флегматик/ [phlegmatic person] (лат. phlegmaticus, від грец. $\varphi\lambda\varepsilon\gamma\mu\alpha\tau\iota\kappa\acute{o}\varsigma$ — запальний) — людина із сильним, врівноваженим, але інертним типом вищої нервової діяльності. Див. темперамент.

ФЛЕШ-ПАМ'ЯТЬ /флэш-память/ [flash memory] — вид пристрою запам'ятовуючого постійного з еле-

ктричним перезаписом.

ФЛОПІ-ДИСК /флоппи-диск/ — див. диск магнітний гнучкий.

ФОКУС /фокус/ [focus, focal point] (від лат. focus — вогнище, осередок) — точка, в якій збираються промені, відбиті сферичним дзеркалом або заломлені лінзою.

ФОНД /фонд/ [fund, collection] франц. fond, від лат. fundus — основа) — 1) Запаси, ресурси, нагромадження; капітал. 2) Систематизоване зібрання будь-яких об'єктів: вхідних документів, алгоритмів, програм, файлів.

Ф. алгоритмів і програм /ф. алгоритмов и программ/ [algorithm and program c.] — систематизована бібліотека апробованих алгоритмів і програм вирішення задач на ЕОМ, описаних в стандартній формі.

Ф. архівний /ф. архивный/ [archival c.] — систематизоване та забезпечене зібрання архівних документів, створених і накопичених у процесі діяльності якої-небудь установи або окремої особи.

Ф. інформаційний /ф. информационный/ [data c.] — в системах інформаційних — сукупність даних, що використовуються споживачами інформації. Так, в банках даних, ф. і. складається з баз даних і архівів.

ФОРМА /форма/ [form] (від лат. forma — зовнішність, устрій) — 1) Спосіб існування змісту, його внутрішня структура, організація і зовнішній вираз. 2) Спосіб здійснення, виявлення будь-якої дії.

Ф. інформаційної боротьби /ф. информационной борьбы/ — способи ведення боротьби інформаційної. Ф. і. б. є вплив інформаційний, атака інформаційна, битва інформаційна і операція інформаційна. Для досягнення мети інформаційних впливів, атак, битв і операцій застосовується вся сукупність способів інформаційної боротьби.

Ф. психологічної війни /ф. психологической войны/ — способи реалізації впливу психологічного, що визначають внутрішній зміст і зовнішні атрибути війни психологічної. Основними ф. п. в. є усне (звукове) мовлення, вплив друкованими іобразотворчими засобами, вплив радіо і телевізійним мовленням. При виборі ф. п. в. необхідно враховувати їхні специфічні особливості. Так, мовлення усне є вельми продуктивним, але не завжди можливим. Радіо й телебачення забезпечує охоплення великої аудиторії, але потребує спеціальної

апаратури для приймання й умов для прослухування (перегляду), що в воєнний час є не завжди можливим. Друковані матеріали програють в оперативності, неадекватно сприймаються малограмотними людьми і потребують спеціальних засобів доставки до об'єкта. Проте їх можна вивчати неодноразово, передавати з рук в руки, зберігати довгий час. Найчастіше різноманітні ф. п. в. застосовують комплексно, щоб сильні сторони одних компенсували слабкі сторони інших.

ФОРМАНТА /форманта/ [formant] (від лат formans — створюючий) — 1) В акустиці — призвук, майже незмінний за частотою, властивий усім тонам даного голосу або музичного інструмента, який надає звучанню характерного забарвлення — тембру. 2) Область концентрації енергії в спектрі звуку мови або співацького голосу, а також музичного інструмента.

ФОРМУЛЯР /формуляр/ [form] (нім. Formular, франц. formulaire, від лат. formula — форма) — бланк (картка), куди вносять основні відомості про щось.

ФОТО... /фото.../ [photo...] (від грец. $\varphi\tilde{\omega}\varsigma$ ($\varphi\omega\tau\acute{o}\varsigma$) — у складних словах відповідає поняттям: "той, що діє за допомогою світла", "застосований на дії світла".

ФОТОГРАММЕТРІЯ /фотограмметрия/ [photogrammetry] (від фото..., грец. $\gamma\rho\acute{\alpha}\mu\mu\alpha$ — запис і $\mu\varepsilon\tau\rho\acute{\varepsilon}\omega$ — вимірюю) — науково-технічна дисципліна, що розробляє способи визначення форми, розмірів і положення об'єктів за їхнім фотографічним зображенням. За способом одержання знімків розрізняють наземну ф. та аерофотограмметрію. У військовій справі засоби ф. використовуються для ведення розвідки фотограмметричної, а також при створенні спеціальних карт, фотодокументів, визначенні координат цілей і бойових порядків військ (див. дешифрування зображень). Теоретична основа ф. — залежність між координатами точок місцевості і координатами їхнього зображення на знімку (парі знімків).

ФОТОГРАФУВАННЯ /фотографирование/ [photography] (від фото... — і грец. $\gamma\rho\acute{\alpha}\varphi\omega$ — пишу) — процес фіксації зображень за допомогою фізико-хімічних властивостей світла.

ФРІКІНГ /фрикинг/[phreaking] — теж саме, що і хакінг, але з метою отримання доступу неавторизованого до телефонних мереж зв'язку.

ФРУСТРАЦІЯ /фрустрация/ — переживання невдачі, що виникає при наявності реальних або удаваних перепон на шляху до мети. Ф. виникає у людей внаслідок реального або уявного незадоволення їхніх потреб у фізичній і соціальній безпеці, у спілкуванні, в їжі, у побутових зручностях і т. ін.

ФУНКЦІЯ /функция/ [function] (від лат. functio — виконання, звершення) — 1) Діяльність, обов'язок, робота; призначення. 2) Змінна величина, значення якої залежить від значень іншої величини (величин). 3) Одне з призначень пристрою, програми, системи.

Ф. важкооборотна (одностороння) /ф. труднооборотная (односторонняя)/ [one-way f.] — функція f така, що: f обчислюється за допомогою алгоритму поліноміального; для зворотної функції f^{-1} не існує поліноміального алгоритму обчислення. Ф. в. є центральним поняттям в багатьох розділах криптології, зокрема, в асиметричній криптографії.

Ф. важкооборотна із секретом /ф. труднооборотная с секретом/[one-way f. with trapdoor] — функція f з параметром S така, що: f — функція важкооборотна; знання параметра S (секрету) дозволяє ефективно обчислювати f^{-1}. Більш точно, для f^{-1} можна визначити функцію g на множині $\Im$ наступним чином: $\Im \xrightarrow{g} \{0,1\}$, для $i \in \Im$

– $g(i) = 0$, якщо f — важкооборотна функція;

– $g(i) = 1$, якщо існує алгоритм поліноміальний обчислення f^{-1} із входом i.

– g, приймає значення 1 рівно на одному значенні i, а саме — S.

Ф. відображення /ф. с отображением/ — правило, за яким кожному елементу x деякої множини X поставлено у відповідність деякий елемент $y = f(x)$ деякої множини Y. Кажуть, що задано відображення або функція $f : X \to Y$ із множини X у множину Y.

Ф. вкорочуюча /ф. укорачивающая/ — те ж, що хеш-Функція.

Ф. Ейлера /ф. Эйлера/ [Euler phi f.] — для цілих чисел, більших або рівних 1, функцією Ейлера $\varphi(n)$ є кількість чисел, менших за n та взаємно простих з n, тобто таких, які не мають з n спільних дільників, відмінних від 1. Ф. Е. відіграє значну роль в теорії криптосистем асиметричних. Так від складності її

обчислення для досить великих чисел залежить стійкість криптосистеми RSA.

Х

ХАКЕР /хакер/ [hacker] — 1) Особа, яка порушує систему захисту системи автоматизованої з метою висвітлення її недосконалості та отримання доступу (без корисних інтересів). 2) Програміст-фанатик, який займається досконалим вивченням систем обчислювальних з метою розширення їхніх можливостей та створенням більш-менш корисних допоміжних програм, які здебільшого погано документовані та інколи спричиняють небажані побічні результати.

ХАКІНГ /хакинг/ [hacking] — неавторизоване використання або спроба обходу чи зламу механізмів захисту інформаційної обчислювальної системи або мережі.

ХАРАКТЕР /характер/ [character] (грец. $\chi\alpha\rho\alpha\kappa\tau\acute{\eta}\rho$ — ознака, риса, особливість) — 1) Сукупність стійких психічних властивостей людини, що формуються в процесі її виховання, навчання, праці, громадської діяльності; вдача. 2) Твердість, сила волі, наполегливість у досягненні мети. 3) Образ, що узагальнює типові риси певної групи людей.

Х. національний /х. национальный/ [national c.] — сукупність найбільш стійких, основних для даної національної спільноти особливостей сприйняття навколишнього світу та реакцій на нього. Насамперед, це сукупність емоційно-почуттєвих проявів, що виражаються в першу чергу в емоціях, почуттях та настроях — способах емоційно-почуттєвого освоєння світу, а також у швидкості та інтенсивності реакції на події, що відбуваються. За походженням поняття х. н. не теоретико-аналітичне, а описове. Тому синтетичне, узагальнене трактування х. н. носить комбінаторний і від того недостатньо цілісний характер. Вважають, що х. н. — складовий елемент і одночасно основа психічного складу нації й національної психології у цілому. Складна, взаємопов'язана і взаємозумовлена сукупність емоційних та раціональних елементів являє собою "психічний склад нації" — ту специфіку духовності та поведінки, яка робить представників однієї нації не подібними на представників інших національних груп.

ХАРАКТЕРИСТИКА /характеристика/ [description, characteristic, reference] (від грец. *χαρακτηριστικός* — той, що служить відмітною ознакою) — опис, аналіз, оцінка певних явищ, відмітних особливостей когось або чогось.

Х. випадкових величин числові /х. случайных величин численные/ — функціонали розподілу ймовірностей випадкової величини, які характеризують різноманітні її властивості. Найважливіша з них — математичне очікування. Більшість інших характеристик є похідними поняттями і виражаються у вигляді математичних очікувань функцій від випадкової величини, як, наприклад, дисперсії.

Х. засобів спостереження в оптичному діапазоні /х. средств наблюдения в оптическом диапазоне/ — числові величини параметрів, що характеризують можливості засобів спостереження в оптичному діапазоні. Основними з них є: діапазон довжин хвиль світлових променів, що сприймаються засобом спостереження (засоби створюються для видимої частини оптичного діапазону або окремих його частин, а також для різноманітних ділянок інфрачервоного діапазону); чутливість (оцінюється мінімальним рівнем енергії світлового променя, при якому забезпечується необхідна якість зображення об'єкта спостереження); роздільна здатність (мінімальні лінійні або кутові розміри між двома сусідніми точками зображення, які можуть спостерігатися як окремі); поле (кут) зору зображення.

Х. інформації специфічні /х. информации специфические/ — інформація існує віртуально, а не фізично; вона є нескінченним ресурсом, може знаходитися одночасно в декількох місцях і використовуватися декількома її власниками; інформація, що являє сама по собі тільки масив фактів, зібраних різними способами, і які не відрізняються точністю і вірогідністю, повинна бути перетворена в знання; при правильному обробленні, аналізі і узагальненні інформація перетворюється в засіб швидкого і адекватного реагування на обстановку, що змінюється; інформація нелінійна за своїм характером: великий обсяг даних може не дати ніякого ефекту, тоді як коротке повідомлення, представлене невеликою кількістю даних, може змінити хід історії; інформація не визнає міжнародних кордонів і не має формальних границь; одна і та ж інформація

або одне і те ж її джерело часто може використовуватися будь-якою з конфліктуючих сторін.

Х. інформаційної зброї /х. информационного оружия/ — відмітні особливості, що характеризують основні риси застосування зброї інформаційної: низька вартість (на відміну від традиційних воєнних технологій, розроблення інформаційної зброї не потребує значних фінансових ресурсів — достатньо мати досвід роботи в системах інформаційних і доступ у глобальні та відомчі мережі); відсутність традиційних кордонів (відмінності між суспільним і особистим, воєнною і кримінальною поведінкою, а також географічні кордони, які історично складалися між націями, розмиваються зростаючою взаємозв'язаністю інфраструктур інформаційних); нові можливості для керування суспільною думкою (сучасні інформаційні технології надають широкі можливості для маніпулювання свідомістю людей і затрудняють державі роботу з політичної підтримки ініціатив у галузі забезпечення безпеки); нові завдання перед органами розвідки (неправильне розуміння ролі, можливостей і цілей інформаційної зброї знижує ефективність традиційної розвідувальної діяльності — необхідні нові форми розвідки, що концентруються на зброї інформаційній стратегічній); складність оцінки загроз і формування системи попередження (на даний час не існує систем попередження, які дозволили би відрізнити стратегічну атаку з використанням інформаційної зброї від інших форм діяльності в інформаційному просторі, включаючи шпіонаж і випадкові помилки); труднощі при створенні й підтримці коаліцій (коаліції тільки збільшують уразливість їхніх учасників від інформаційної поразки); уразливість власних територій (так як інформаційні технології не обмежені в географічному плані, то інформаційною зброєю можуть уражатися цілі як на віддаленому театрі воєнних дій, так і усередині країни).

Х. об'єктива частотно-контрастна /х. объектива частотно-контрастная/ — характеристика здатності об'єктива передавати контраст деталей об'єкта спостереження. Вимірюється відношенням контрастності деталей певних розмірів на зображенні і на об'єкті. Для кількісної оцінки характеристики, як вихідний об'єкт, використовується еталонний об'єкт спостереження — міра у вигляді чорно-білих ліній, нанесених на білий папір.

Х. об'єктів психологічної війни основні /х. объектов психологической войны основные/ — хара-

ктеристики об'єктів психологічного впливу, які підлягають виявленню й врахуванню в війні психологічній: особливості національно-психологічні; особливості індивідуально-особистістні; належність групова; особливості морально-психологічного стану.

Х. об'єктів радіолокаційні /х. объектов радиолокационные/ — характеристики, що визначають можливість виявлення, розпізнавання цілей і вимірювання параметрів їхнього руху засобами радіолокації. Основною х. о. р. є здатність цілі відбивна (інтенсивність відбитого сигналу), яка залежить від геометричних розмірів, конфігурації, матеріалу, ракурсу цілі, довжини хвилі РЛС і виду поляризації електромагнітних хвиль. Практична неможливість врахування усіх перелічених факторів привела до необхідності введення спеціальної розрахункової величини — поверхні розсіювання ефективної цілі (об'єкта), яка враховує відбивні властивості реальних цілей (об'єктів) складної форми (літаки, кораблі, штучні відбивачі і т. ін.).

ХВИЛЕВІД /волновод/ [waverguide] — пристрій або канал у неоднорідному середовищі, уздовж якого можуть розповсюджуватися спрямовані хвилі. Розрізняють екрановані х., утворені дзеркально відбиваючими стінками (металеві радіохвилеводи та різноманітні типи хвилеводів акустичних), а також системи, в яких поперечна локалізація хвиль зумовлена повним внутрішнім відбиттям. Останні можуть мати як різкі (у масштабі довжини хвилі) межі: діелектричні радіохвилеводи, світловоди, так і межі з плавними переходами до однорідного середовища (наприклад, іоносферний х., підводні звукові канали).

Х. акустичний /в. акустический/ [acoustic w.] — канал для розповсюдження хвиль акустичних. Обмежує простір розповсюдження власних мод акустичних коливань. Розрізняють х. а. у вигляді пластини, стрижня, зігнутої труби і т. ін. Найбільше розповсюдження одержали х. а. хвиль акустичних поверхневих, в яких хвилевідний ефект досягається або за рахунок створення на поверхні звукопроводу ділянки, що забезпечує зменшення швидкості розповсюдження хвилі (наприклад, створенням на поверхні звукопроводу шарів із певними фізичними властивостями), або нанесенням виступів у вигляді прямокутників, клинів. Х. а. використовуються для передавання енергії акустичних коливань від перетворювача електроакустичного

до об'єктів впливу, а також затримки акустичних сигналів у акустоелектронних пристроях.

Х. оптичний (світловод) /в. оптический (световод)/ [optical w., light guide] — закритий пристрій для спрямованого передавання (каналізації) світла. Одним із типів світловоду є лінзовий хвилевід: система оптичних лінз, розташованих у трубі на певній відстані одна від іншої і призначених для періодичної корекції хвилевого фронту світлового пучка. Найбільш перспективний тип х. о. — волоконний світловод (оптичний кабель), що дозволяє передавати світло на великі відстані. Він знаходить широке застосування у волоконно-оптичних системах передавання, в техніці обчислювальній, в датчиках різноманітних фізичних полів і т. ін.

ХВИЛІ /волны/ [waves] — коливний рух у фізичному середовищі, а також розповсюдження цього руху.

Х. акустичні /в. акустические/ [acoustic w.] — пружні збурення, що розповсюджуються у твердому, рідкому і газоподібному середовищах. Розповсюдження х. а. в середовищі викликає виникнення механічних деформацій стиснення і зсуву, які переносяться з однієї точки в іншу; при цьому має місце перенесення енергії пружної деформації при відсутності потоку речовини (за виключенням особливих випадків, наприклад, акустичної течії). Важливий різновид х. а. — хвилі акустичні поверхневі. Див. також хвилі пружні.

Х. акустичні поверхневі /в. акустические поверхностные/ — пружні хвилі, що розповсюджуються вздовж вільної поверхні твердого тіла або вздовж межі твердого тіла з іншими середовищами і загасають при віддаленні від межі. Х. а. п. ультра- і гіперзвукового діапазонів широко застосовуються для створення мікроелектронних схем оброблення електричних сигналів в акустоелектроніці.

Х. гіперзвукові /в. гиперзвуковые/ [hypersonic w.] (від грец. префікса *ὑπερ*..., що означає підвищення, надмірність) — високочастотна частина хвиль пружних — від 10^9 до 10^{12}–10^{13} Гц. За фізичною природою х. г. нічим не відрізняються від хвиль ультразвукових, проте із-за наявності більш високих частот (менших довжин хвиль) більш суттєвою стає взаємодія х. г. з квазічастинками в середовищі — електронами провідності, тепловими фононами, магнонами і т. ін. Властивості х. г. дозволяють використовувати їх для дослідження стану речовини, особливо у фізиці твердого тіла, а також для створення акустичних ліній

затримки в діапазоні надвисоких частот електромагнітних хвиль та пристроїв акустоелектроніки і акустооптики.

Х. довгі (кілометрові) /в. длинные (километровые)/ [long w-s] — радіохвилі в діапазоні 1 — 10 км. Д. х. піддаються дифракції, порівняно слабо поглинаються земною поверхнею і можуть розповсюджуватися поверхневим променем на відстані до 3000 км. В іоносфері вони загасають сильніше, проте можуть відбиватися від шару E і розповсюджуватися просторовим променем на великі відстані. Радіохвилі цього діапазону як носії інформації, окрім великої дальності розповсюдження, мають порівняно постійну напруженість поля в пункті прийому протягом доби і року, що забезпечує стійкість зв'язку. Ці хвилі застосовують також для зв'язку під водою, де погано розповсюджуються хвилі більш високих частот. Недоліком довгохвильової радіолінії є погана випромінююча здатність антен, їхні великі розміри, що сягають декількох сотень метрів, високий рівень атмосферних і промислових завад і мала пропускна здатність.

Х. електромагнітні /в. электромагнитные/ [electromagnetic w-s] — збурення електромагнітного поля, що розповсюджується в просторі з кінцевою швидкістю в залежності від властивостей середовища. У вакуумі е. х. розповсюджуються зі швидкістю світла (біля 300000 км/с). Е. х. характеризуються частотою коливань, потужністю і поляризацією. В залежності від довжини хвилі (частоти коливань) розрізняють такі види х. е.: радіохвилі ($>$ 0,1 мм) (див. також діапазон радіохвиль), випромінювання оптичне (від 1 мм до 1 нм), випромінювання рентгенівське (від 0,1 мкм до 1 пм) і гамма-проміння ($<$ 0,1 нм).

Х. звукові /в. звуковые/ [sound w.] — поздовжні хвилі пружні, що розповсюджуються в твердих тілах, рідинах і газах та суб'єктивно сприймаються системою слуховою людини та органами слуху тварин. Людина чує звук в діапазоні частот від 16 Гц до 20 кГц. Джерелами звуку можуть бути будь-які явища, що викликають локальну зміну тиску або механічної напруги. Розповсюдження з. х. характеризується в першу чергу швидкістю звуку. В ряді випадків спостерігається дисперсія швидкості звуку, тобто залежність швидкості його розповсюдження від частоти. При розповсюдженні з. х. виникає поступове загасання звуку, зв'язане з необоротним перетворенням звукової енергії в інші форми (головним чином, в теплоту). Ва-

жливою характеристикою звуку є його спектр, який одержують у результаті розкладання звуку на окремі гармонічні коливання. Енергетичною характеристикою звукових коливань є інтенсивність звуку, яка залежить від амплітуди звукового тиску, а також від властивостей самого середовища і від форми хвилі. Суб'єктивною характеристикою звуку, зв'язаною з його інтенсивністю, є гучність звуку, що залежить від частоти. Найбільшу чутливість вухо людини має в діапазоні частот 1–5 кГц. В техніці для прийому з. х. застосовують, головним чином, перетворювачі акустоелектричні: в повітрі — мікрофони, в воді — гідрофони, в земній корі — геофони.

Х. інфразвукові /в. инфразвуковые/ [infrasonic w-s] (від лат. infra — нижче, під) — хвилі акустичні з частотами нижче межі чутних людиною частот. За верхню межу інфразвуку приймають частоти 16–25 Гц, а нижню межу не визначено. Х. і. містяться в шумі атмосфери і моря; їхнє джерело — турбулентність атмосфери і вітер, грозові розряди (грім), вибухи, гарматні постріли; в земній корі — струси і вібрації від найрізноманітніших джерел. Для інфразвукових хвиль характерне мале поглинання в різноманітних середовищах, внаслідок чого він може розповсюджуватися на дуже далекі відстані. Це дозволяє визначати місця сильних вибухів або положення стріляючої гармати, прогнозувати цунамі, досліджувати верхні шари атмосфери, властивості водного середовища.

Х. іоносферна /в. ионосферная/ [ionospheric m.] — радіохвиля, що розповсюджуються в результаті переломлення її в іоносфері і відбиття від земної поверхні. Переломлення радіохвиль на цій чи іншій висоті іоносфери залежить від частоти радіохвиль і кута падіння (кута, що відраховується від вертикальної лінії в точці падіння) на відповідний шар іоносфери. Із збільшенням кута падіння хвилі збільшується пологість траєкторії променя в іоносфері та зменшується концентрація електронів (іонів), необхідна для повернення променя на Землю. Мінімальне значення кута падіння, при якому можливе відбиття радіохвиль від іоносфери, називається критичним. Коефіцієнт переломлення зменшується із збільшенням частоти, тобто хвилі довгі переломлюються сильніше, ніж короткі, а для УКХ переломлення недостатнє для повернення хвиль на Землю і вони виходять у космічний простір. За рахунок багатократного переломлення радіохвиль

в іоносфері і відбиття від земної поверхні х. і. може розповсюджуватися на великі відстані, аж до огинання Землі. При такому розповсюдженні хвилі на земній поверхні, виникають зони мовчання, в які не попадають відбиті хвилі. В зонах прийому виникає інтерференція хвиль, що пройшли різний шлях від випромінювача і мають різні фази. Випадковий характер зміни фази приводить до випадкової зміни амплітуди сумарної хвилі, яка називається завмиранням або федінгом. Ступінь поглинання радіохвиль в атмосфері збільшується при підвищенні густини іонізації, частоти коливань і шляху, що проходить хвиля в іоносфері. Зимою, коли концентрація електронів у зв'язку з пониженням сонячної активності зменшується, поглинання радіохвиль знижується і дальність розповсюдження збільшується.

Х. короткі /в. короткие/ [short w-s] — радіохвилі в діапазоні 10 — 100 м. При розповсюдженні х. к. дальність поверхневого променя невелика внаслідок зростання поглинання енергії землею. Поле в точці прийому створюється в основному за рахунок переломлення в різноманітних шарах іоносфери. В результаті флуктуації густини та висоти шарів і взаємодії променів, на х. к. спостерігаються глибокі завмирання і навіть повне зникнення зв'язку протягом одиниць і десятків секунд. Для забезпечення цілодобового зв'язку в умовах добової зміни іоносфери необхідно здійснювати періодичну зміну частот. Визначення оптимальних частот здійснюється спеціальними службами спостереження іоносфери за результатами вертикального і вертикально-скісного зондування її радіоімпульсами. Найбільш сприятливі умови проходження хвиль вдень — в діапазоні 10–25 м, а вночі — 35–70 м. В діапазоні х. к. на напруженість поля і характер її зміни в точці прийому впливають інші явища, такі як "спалах" на Сонці, розсіювання хвиль на дрібних неоднорідностях іоносфери, поворот площини поляризації. Х. к. дозволяють забезпечити зв'язок на дуже великі відстані при порівняно малих потужностях передавача і габаритах антени, а також малий вплив атмосферних і промислових завад. Вони застосовуються для зв'язку, радіонавігації, радіомовлення.

Х. поверхнева (земна) /в. поверхностная (земная)/ [surface w.] — радіохвиля, що поширюється в безпосередній близькості від поверхні Землі і частково огинає її поверхню в результаті дифракції.

Х. просторова /в. пространственная/ [space (spatial) w.] — радіохвиля, що поширюється вгору під

кутом до горизонту. Х. п. поділяються на прямі, тропосферні і іоносферні.

Х. пружна /в. упругая/ [elastic w.] — пружне збурення, що розповсюджується у твердому, рідинному і газоподібних середовищах, наприклад, хвилі, що виникають у земній корі при землетрусах, хвилі звукові і ультразвукові в рідинах, газах і твердих тілах. При розповсюдженні х. п. в середовищі, виникають механічні деформації стискування і зсуву, які переносяться хвилею з однієї точки середовища в іншу. При цьому має місце перенесення пружної деформації при відсутності потоку речовини. Всяка гармонічна х. п. характеризується амплітудою зміщення часток середовища і його напрямом, коливальною швидкістю часток, змінними механічною напругою і деформацією, частотою коливань часток середовища, довжиною хвилі, фазовою і груповою швидкостями, а також законом розподілу зміщень і напруг уздовж фронту хвилі. Діапазон частот х. п. простягається від малих часток Гц до 10^{13} Гц. Х. п. знаходять надзвичайно широке застосування: низькочастотні х. п. використовуються в сейсмології (для реєстрації землетрусів) і в сейсмічній розвідці. Х. п. кілогерцового діапазону застосовуються в гідролокації і при дослідженнях океану. П. х. ультра- і гіперзвукового діапазонів застосовуються у фізиці, акустоелектроніці, у промисловості, медицині та інших галузях.

Х. пряма /в. прямая/ [direct w.] — радіохвиля, що поширюється прямолінійно в атмосфері і космосі.

Х. середні (гектометрові) /в. средние (гектометровые)/ [medium w-s] — радіохвилі в діапазоні 100–1000 м. Можуть розповсюджуватися поверхневими і просторовими променями. Енергія х. с. поглинається земною поверхнею сильніше, ніж енергія довгохвильових, тому дальність зв'язку поверхневим променем складає приблизно 500–1500 км. При розповсюдженні просторовим променем прийом сигналів можливий до 4000 км. Умови розповсюдження х. с. суттєво змінюються в залежності від години доби. В нічний час за рахунок переломлення в іоносфері дальність розповсюдження вища, ніж в денні, коли переважають поверхневі хвилі. В цьому діапазоні спостерігаються завмирання в результаті інтерференції земних і поверхневих або просторових хвиль з різноманітними шляхами розповсюдження, високий рівень атмосферних і промислових завад. Антени в діапазоні х. с. за рахунок більшої близькості їхніх геометричних розмірів до довжин

хвиль мають більший коефіцієнт підсилення, ніж антени діапазону довгих хвиль. Х. с. використовуються для радіомовлення і зв'язку, на флоті і в авіації.

Х. тропосферна /в. тропосферная/ [tropospheric w.] — радіохвиля, що поширюється в тропосфері — приземній неоднорідній частині атмосфери не вище 10–12 км від поверхні Землі. У тропосфері здійснюється розсіювання, а також часткове викривлення траєкторії і відбиття радіохвиль від неоднорідностей тропосфери.

Х. ультразвукова /в. ультразвуковая/ [ultrasound w., ultrasonic w., supersonic w.] (від. лат ultra — за, понад, по той бік, за межами) — хвиля акустична з частотами приблизно від $(1{,}5–2)\cdot10^4$ Гц (15–20 кГц) до 10^9 Гц (1 ГГц). В залежності від специфічних особливостей генерації, прийому, розповсюдження і застосування, діапазон частот х. у. поділяють на три піддіапазони: х. у. низьких частот ($1{,}5\cdot10^4$–10^5 Гц), середніх частот (10^5–10^7 Гц) та високих частот (10^7–10^9 Гц). У. х. застосовуються в акустоелектроніці, гідроакустиці, промисловості, медицині і т. ін.

Х. ультракороткі (УКХ) /в. ультракороткие (УКВ)/ [ultrashort (very short) w-s. (VSW)] — радіохвилі в діапазоні від 1 м до 10 м. В діапазоні х. у. (метрових і більш коротких) практично відсутня дифракція. Вони розповсюджуються в межах прямої видимості, в тому числі відбиваються від землі і тропосфери із утратою частини енергії на поглинання. Радіохвилі в цих діапазонах є основними носіями інформації в мережах телекомунікацій. Це зумовлено рядом особливостей х. у.: широкий частотний діапазон, який забезпечує можливість передавання великого обсягу інформації, в тому числі шляхом використання широкосмугових каналів; низький рівень атмосферних і промислових завад, що дозволяє використати приймальні пристрої з високою чутливістю, що підвищує дальність прийому; незначний вплив станційних завад на роботу інших радіосистем унаслідок обмеженості їхнього радіуса видимості; можливість створення невеликих антен з вузькою діаграмою спрямованості, що дозволяє здійснювати радіозв'язок при відносно малій потужності передавальних пристроїв. Основний недолік х. у. — суттєво велике поглинання їх в атмосфері, в тому числі природними осадками (дощем, снігом, градом), і, як наслідок, відносно мала дальність розповсюдження.

ХЕШ-КОД /хэш-код/ [hash code] — результат застосування хеш-функції до повідомлення.

ХЕШ-ФУНКЦІЯ /хэш-функция/ [hash function] — функція, яка відображає двійкове слово довільної довжини у двійкове слово фіксованої довжини, тобто відображення $(0,1)^n \xrightarrow{f} (0,1)^k$, де $n = 1, 2, ...\infty$, k фіксоване, має ефективний алгоритм обчислення та задовольняє наступним вимогам. По-перше, за допомогою обчислень неможливо знайти за даним виходом функції відповідне вхідне значення або "вхід", по-друге, за даним входом за допомогою обчислень неможливо знайти другий вхід, хеш-функція від якого збігалася б з першим.

Х.-Ф. колізістійка /х.-ф. колизистойкая/ [collision resistance h. f., strong collision resistance h. f.] — те ж, що хеш-функція сильна.

Х.-Ф. сильна /х.-ф. сильная/ [strong h. f.] — хеш-функція слабка, яка додатково має наступну властивість: на основі обчислення неможливо знайти два $x \neq \acute{x}$ такі, що $f(x) = f(\acute{x})$. Тобто ми вільні у виборі як одного, так і іншого вхідного значення. Інша назва хеш-функція колізістійка.

Х.-Ф. слабка /х.-ф. слабая/ [weak h. f.] — хеш-функція, яка задовольняє двом вимогам: по-перше, на основі обчислень неможливо знайти за даним виходом функції відповідне вхідне значення або "вхід", тобто за даним $y = f(x)$ на основі обчислення неможливо знайти x. По-друге, за даним входом на основі обчислення неможливо знайти другий вхід, хеш-функція від якого збігалася б з першим, тобто за даним x на основі обчислення неможливо знайти $x \neq \acute{x}$ такий, що $f(x) = f(\acute{x})$. Інша назва — хеш-функція, стійка до визначення обраного прообразу.

Х.-Ф., стійка до визначення обраного прообразу /хэш-ф., стойкая к определению выбранного прообраза/ [and-preimage resistance h. f., weak collision resistance h. f.] — те ж, що слабка хеш-функція.

ХОЛЕРИК /холерик/ [choleric subject] (лат. cholericus, від грец. $\chi\text{ø}\lambda\varepsilon\rho\iota\kappa\acute{o}\varsigma$ — хворий на жовчну хворобу) — людина із сильним, рухливим, але неврівноваженим типом вищої нервової діяльності. Див. також темперамент.

ХОСТ /хост/ [host] — комп'ютер, на якому працює мережний протокол, наприклад, TCP/IP. Х. має

деяке прикладне програмне забезпечення, призначене для передавання і приймання пакетів. Він обмінюється даними з іншими х.-комп'ютерами, і значна частина діяльності в Інтернеті зумовлена керуванням інформаційними потоками між х.-комп'ютерами. Типовими прикладами х. можуть бути: маршрутизатори, комп'ютери персональні, сервери, проксі-сервери, шлюзи і т. ін.

Ц

ЦЕНТР /центр/ [center] (лат. centrum, від грец. *κέντρøν* — стрекало, осереддя) — 1) Середня частина чогось. 2) Зосередження великих і важливих сил (наприклад, науковий ц., промисловий ц. і т. ін.).

Ц. генерації ключів /ц. генерации ключей/ — див. центр розподілу ключів.

Ц. інформаційний /ц. информационный/ [information c.] — постійний чи тимчасово діючий орган, який здійснює обслуговування інформаційне по колу заздалегідь визначених питань. Зазвичай під ц. і. розуміється спеціалізована установа, що організує і координує роботу прямо чи побічно підпорядкованих йому інформаційних підрозділів.

Ц. інформаційних бойових дій /ц. информационных боевых действий/ [information battle c.] — військова частина (підрозділ), призначений для створення засобів ведення війни інформаційної на підтримку операцій; планування компаній, придбання і випробовування обладнання, захисту штабів від інформаційного нападу. З цією метою центр навчає, споряджає і розгортає групи реагування, розробляє і підтримує бази даних і програми прикладні, проводить аналіз уразливості електронних систем своїх військ (сил).

Ц. інформаційно-обчислювальний /ц. информационно-вычислительный/ [information and computing c.] — центр обчислювальний, що має інформаційну систему автоматизовану і забезпечує як інформаційне обслуговування користувачів, так і вирішення широкого кола обчислювальних задач.

Ц. комп'ютерної безпеки Національний /ц. компьютерной безопасности Национальный/ [National Computer Security C.] — підрозділ Агентства національної безпеки, призначений для підтримки і стимулювання розповсюдження захищених систем в закладах Федерального уряду. Центр також здійснює коорди-

націю в галузі аналізу і розробки систем з гарантованим захистом.

Ц. мережної інформації Інтернету /ц. сетевой информации Интернета/ [Internet Network Information C. (InterNIC)] — центр, призначений для реєстрації імен доменів Інтернету і керування базою даних цих імен.

Ц. обчислювальний /ц. вычислительный/ [computation (computer, computing) c.] — 1) Науково-дослідний заклад, який займається розробкою забезпечення програмного ЕОМ, методів вирішення прикладних задач в різноманітних галузях *науки*, науки, техніки, управління. Ц. о. надає також послуги з виконання обчислювальних робіт зовнішнім замовникам. 2) Заклад, призначений для виконання складних і трудомістких обчислювальних робіт з допомогою ЕОМ.

Ц. передавання ключів /ц. передачи ключей/ [Key Translation C. (KTC)] — об'єкт системи захисту, якому довірено передавати ключі між абонентами, які мають з ц. п. к. спільний ключ.

Ц. розподілу ключів /ц. распределения ключей/ [Key Distribute C. (KDC)] — об'єкт системи захисту, який генерує (чи отримує з будь-якого іншого джерела) та розповсюджує ключі електронним або ще будь-яким чином. Якщо для розповсюдження ключів використовується *методи захисту інформації криптографічні*, то у абонентів системи та ц. р. к. повинні бути відповідні ключі для таємного зв'язку.

Ц. сертифікації ключів /ц. сертификации ключей/ [key sertification c.] — об'єкт системи захисту, який проводить автентифікацію ключів за допомогою механізму *підпису цифрового* або будь-яким іншим чином.

Ц. ситуаційний /ц. ситуационный/ — постійний чи тимчасово діючий орган, призначений для колективного прийняття рішень, як правило, в надзвичайних ситуаціях.

ЦИКЛ /цикл/ [cycle, loop] (від грец. *κύκλøς* — круг, коло, круговерть) — сукупність взаємопов'язаних явищ, процесів, робіт, яка створює закінчене коло дій протягом певного проміжку часу.

Ц. життєвий інформації /ц. жизненный информации/ — період існування інформації, починаючи з її створення до споживання.

ЦИФРА /цифра/ [digit] — графічний знак, призначений для зображення кількісних величин.

Ц. контрольна /ц. контрольная/ [check d.] — цифра, що доповнює блок даних, які передаються, і дозволяє контролювати за певним алгоритмом їхню достовірність.

ЦІЛІСНІСТЬ /целостность/ [integrity] — 1) Внутрішня єдність, зв'язаність усіх частин чого-небудь, єдине ціле. 2) В обчислювальній техніці — стан даних або комп'ютерної системи, в якій дані та програми використовуються встановленим чином, що забезпечує: стійку роботу системи; автоматичне відновлення у випадку виявлення системою потенційної помилки; автоматичне використання альтернативних компонентів замість тих, що вийшли з ладу.

Ц. адміністративна /ц. административная/ [mandatory i.] — послуга безпеки, яка забезпечує цілісність інформації відповідно до принципів керування доступом довірчого.

Ц. бази даних /ц. базы данных/ [database i.] — стан бази даних, коли всі значення даних правильні в тому сенсі, що відображають стан реального світу (в межах заданих обмежень по точності та часовій узгодженості) і підпорядковуються правилам взаємної несуперечливості. Підтримка ц. б. д. включає перевірку цілісності і відновлення з будь-якого неправильного стану (див. *відновлення баз баз даних*), яке може бути виявлено; це входить у функції адміністратора бази даних.

Ц. даних /ц. данных/ [data i.] — стан, при якому дані, що зберігаються в комп'ютері, в точності відповідають даним у вихідних документах; властивість, що має відношення до набору даних і означає, що дані не можуть бути змінені або зруйновані без санкції на доступ. Ц. д. вважається збереженою, якщо дані не спотворені і не зруйновані (стерті).

Ц. довірча /ц. доверительная/ [discretionary i.] — послуга безпеки, яка забезпечує цілісність інформації відповідно до принципів адміністративного керування доступом.

Ц. інформації /ц. информации/ [information i.] — властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і (або) процесом. Інформація зберігає

цілісність, якщо дотримуються встановлені правила її модифікації (видалення).

Ц. об'єкта /ц. объекта/ [object i.] — властивість об'єкта доступу, що характеризує його авторизований стан.

Ц. семантична /ц. семантическая/ [semantic i.] — стан даних, коли вони зберігають свій інформаційний зміст та однозначність інтерпретації в умовах випадкових впливів.

Ц. системи /ц. системы/ [system i.] — властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки.

ЦІНА /цена/ [price] — 1) Вартість товару, що виражена у грошах. 2) Грошове відшкодування за товар, послуги, плата.

Ц. інформації /ц. информации/ [p. of information] — вартість інформації, виражена у грошах. Складається із собівартості інформації та прибутку від інформації. Собівартість визначається витратами власника інформації на її одержання, наприклад: проведення досліджень в наукових лабораторіях, аналітичних центрах, групах і т. ін.; купівля інформації на ринку інформації; добування інформації за допомогою протиправних дій. Прибуток від інформації з огляду її особливостей може приймати різноманітні форми, причому вираз його у грошах не є найбільш розповсюдженою формою. В загальному випадку прибуток від інформації може бути одержаний в результаті наступних дій: продажу інформації на ринку; матеріалізації інформації в продукції з новими якостями або технології, що приносить прибуток; використання інформації для прийняття більш ефективних рішень. Остання форма прибутку від інформації не стільки очевидна, проте вона найбільш розповсюджена, тому що будь-яка діяльність людини це послідовність прийняття нею рішень.

ЦІННІСТЬ /ценность/ [value] — сукупність таких властивостей чого-небудь, як важливість, значність, необхідність.

Ц. інформації /ц. информации/ [information v.] — властивість інформації, що визначається її придатністю до практичного використання в різних галузях цілеспрямованої діяльності людини. Розповсюдже-

ння інформації та її використання приводить до зміни її цінності і ціни. З часом цінність більшості видів інформації, що циркулює у суспільстві, зменшується — інформація старіє.

Ч

ЧАС /время/ [time] — 1) Одна з основних форм існування матерії, яка виявляється в тривалості буття. 2) Тривалість існування явищ і предметів.

Ч. безконтрольної присутності противника в інформаційно-обчислювальній мережі /в. бесконтрольного присутствия противника в информационно-вычислительной сети/ — час, протягом якого системі захисту інформації мережі інформаційно-обчислювальної невідома стратегія дій противника або на дії противника нема можливості вплинути.

Ч. безпечний /в. безопасное/ [security t.-lag] — математичне сподівання часу розкриття системи захисту статистичним апробуванням можливих варіантів доступу до даних.

ЧАСТИНА /часть/ [share, parts, unit] — 1) Доля, окрема одиниця, на які підрозділяється ціле. 2) Предмет як складовий елемент якого-небудь цілого. 3) Відділ якого-небудь закладу.

Ч. предметна /ч. предметная/ — підмножина (частина реального світу), на якій визначається набір даних і методів маніпулювання з ними для вирішення конкретних завдань або досліджень.

Ч. предметна інформаційної сфери /ч. предметная информационной сферы/ — див. сфера інформаційна.

Ч. секретна /ч. секретная/ — назва кімнати або цілої споруди, спеціально призначеної і підготовленої для роботи з матеріалами вищої категорії секретності або відомостей особливої важливості. Стіни, підлога і стеля такого приміщення зроблені з особливих матеріалів, які роблять неможливим підслухування ззовні і одержання інформації за допомогою електронних засобів. В ч. с. не буває вікон. Вона обладнується різноманітною апаратурою технічного захисту інформації.

ЧАСТОТА /частота/ [frequency] — величина, що характеризує кількість коливань хвиль (періодичних

сигналів) за секунду. Частота вимірюється в герцах (Гц) — 1 Гц дорівнює одному повному коливанню за секунду. Частота також вимірюється в кілогерцах (кГц, 1000 Гц), мегагерцах (МГц, 1000 кГц), гігагерцах (ГГц, 1000 МГц) та терагерцах (ТГц, 1000 ГГц).

Ч. вельмивисокі (ВВЧ) /ч. крайне высокие (КВЧ)/ [extremely high f. (EHF)] — радіочастоти, значення частоти яких лежить у межах 30–300 ГГц.

Ч. високі (ВЧ) /ч. высокие (ВЧ)/ [very high f. (VHF)] — радіочастоти, значення частоти яких лежить у межах 3–30 МГц.

Ч. гектометрових (середніх) хвиль /ч. гектометровых (средних) волн/ — те ж, що частоти середні.

Ч. гіпервисокі (ГВЧ) /ч. гипервысокие (ГВЧ)/ [tremendously high f. (THF)] — радіочастоти, значення частоти яких лежить у межах 300–3000 ГГц.

Ч. декаметрових (коротких) хвиль /ч. декаметровых (коротких) волн/ — те ж, що частоти високі.

Ч. декаміріаметрових хвиль /ч. декамириаметровых волн/ — те ж, що частоти наднизькі.

Ч. дециметрових хвиль /ч. дециметровых волн/ — те ж, що частоти ультрависокі.

Ч. децимілліметрових хвиль /ч. децимиллиметровых волн/ — те ж, що частоти гіпервисокі.

Ч. дуже високі (ДВЧ) /ч. очень высокие (ОВЧ)/ [very high f. (VHF)] — радіочастоти, значення частоти яких лежить у межах 30–300 МГц.

Ч. дуже низькі (ДНЧ) /ч. очень низкие (ОНЧ)/ [very low f. (VLF)] — радіочастоти, значення частоти

яких лежить у межах 3–30 кГц.

Ч. звукова /ч. звуковая/ [audio f.] — частота від 20 Гц до 20 кГц.

Ч. інфранизькі (ІНЧ) /ч. инфранизкие (ИНЧ)/ [infra low f. (ILF)] — радіочастоти 300–3000 Гц.

Ч. кілометрових (довгих) хвиль /ч. километровых (длинных) волн/ — те ж, що низькі частоти.

Ч. метрових хвиль /ч. метровых волн/ [very high f. (VHF)] — те ж, що частоти дуже високі.

Ч. міліметрових хвиль /ч. миллиметровых волн/ — те ж, що частоти вельмивисокі.

Ч. міріаметрових хвиль /ч. мириаметровых волн/ — те ж, що частоти дуже низькі.

Ч. надвисокі (НВЧ) /ч. сверхвысокие (СВЧ)/ [super high f.] — радіочастоти, значення частоти яких лежить у межах 3–30 ГГц.

Ч. наднизькі (ННЧ) /ч. сверхнизкие (СНЧ)/ [extremely low f. (ELF)] — радіочастоти, значення частоти яких лежить у межах 30–300 Гц.

Ч. низькі (НЧ) /ч. низкие (НЧ)/ [low f.(LF)] — радіочастоти, значення частоти яких лежить у межах 30–300 кГц.

Ч. радіохвилі /ч. радиоволны/ [radio wave f.] — величина, що характеризує кількість коливань радіохвилі в секунду.

Ч. радіоприймача проміжна /ч. радиоприемника промежуточная/ [intermediate f.] — задана частота, в яку повинна бути перетворена в супергетеродинному приймачі частота несуча сигналу радіочастотного, що приймається, з метою ефективного підсилення і фільтрації. Якщо відбувається більше одного перетворення несучої частоти, то частоти відповідно називають: першою проміжною частотою, другою проміжною частотою і т.ін.

Ч. робоча /ч. рабочая/ [operational (operating) frequency] — несуча частота електромагнітних, звукових та інших коливань, що генеруються передавачами і випромінюються антенними пристроями радіостанцій,

РЛС, гідроакустичних та інших станцій в процесі їхньої роботи.

Ч. сантиметрових хвиль /ч. сантиметровых волн/ — те ж, що частоти надвисокі.

Ч. середні (СЧ) /ч. средние (СЧ)/ [medium f.(MF)] — радіочастоти 300–3000 кГц.

Ч. ультрависокі (УВЧ) /ч. ультравысокие (УВЧ)/ [ultra high f.(UHF)] — радіочастоти 300–3000 МГц.

Ч.-носій /ч.-носитель/ — те ж, що несуча частота.

ЧАСТОТОМІР /частотомер/ [frequency meter] — прилад, призначений для вимірювання частоти періодичних (а частіше — гармонічних) сигналів.

Ч. гетеродинний /ч. гетеродинный/ [heterodyne f. m.] — частотомір, що працює за принципом порівняння вимірюваної частоти зі зразковою (наприклад, із частотою кварцового генератора).

Ч. конденсаторний /ч. конденсаторный/ — частотомір, принцип дії якого ґрунтується на вимірюванні середнього струму розряджання або заряджання зразкового конденсатора, що перемикається із заряджання на розряджання з вимірюваною частотою.

Ч. резонансний (хвилемір) /ч. резонансный (волномер)/ [resonant f. m.] — частотомір у вигляді резонансної системи (із зосередженими або розподіленими параметрами), оснащеної індикатором резонансу та органом настроювання, градуйованим в значеннях резонансної частоти (довжини хвилі).

Ч. цифровий (електронно-лічильний) /ч. цифровой (электронно-счетный)/ [counter-type f. m., counter timer] — частотомір, що працює за принципом дискретної лічби — підрахунку кількості періодів вимірюваної частоти протягом каліброваного інтервалу часу.

ЧЕРВ'ЯК /червь/ [worm] — безхребетна тварина, яка пересувається, вигинаючи своє м'яке видовжене тіло.

Ч. мережний /ч. сетевой/ [network w.] — вірус комп'ютерний, що має властивість самостійного розповсюдження в мережах обміну інформацією та заражає елементи МОІ, функціональні сегменти МОІ або МОІ цілком. Основні етапи функціонування ч. м.: пошук в МОІ цілі впливу (у більшості випадків — ПЕОМ із відомою мережною адресою); передавання по МОІ системи керування автоматизованої свого коду на ПЕОМ,

що атакується; одержання керування в системі операційній ПЕОМ, що атакується; перехід до дій за першим етапом. Основною проблемою при функціонуванні м. ч. є одержання керування в операційній системі ПЕОМ, що атакується. Для цього необхідно визначити ідентифікатор і пароль абонента або уразливі місця механізмів захисту інформації. Тому м. ч. повинен мати спеціальний програмний модуль подолання рубежів захисту (наприклад, перехоплення паролю).

Ч. програмний /ч. программный/ [program w.] — закладка програмна, що маскується під системні засоби пошуку вільних обчислювальних ресурсів в мережі.

ЧИСЛО /число/ [number] — дійсна величина в певній системі числення.

Ч. контрольне /ч. контрольное/ [check n.] — число, що використовується для контролю достовірності даних, що передаються.

Ч. просте /ч. простое/ [prime n.] — (в термінах елементарної теорії чисел) натуральне число, яке більше 1 та ділиться націло тільки на 1 та на само себе. Див. також складене число.

Ч. просте сильне /ч. простое сильное/ [strong prime n.] — число просте p, у якого числа $p \pm 1$ мають хоча б один великий простий дільник.

Ч. псевдопросте /ч. псевдопростое/ [pseudoprime n.] — число складене, яке не визначається тестом на простоту ймовірнісним.

Ч. псевдопросте сильне /ч. псевдопростое сильное/ [strong pseudoprime n.] — число складене, яке не визначається простим тестом Мілера-Рабіна.

Ч. псевдопросте слабке /ч. псевдопростое слабое/ [ferma pseudoprime n.] — число складене, яке не визначається тестом Ферма.

Ч. складене /ч. составное/ [composite n.] — (в термінах елементарної теорії чисел) натуральне число n, яке більше 1 та ділиться націло на деяке натуральне число $1 < x < n$. Див. також число просте.

ЧІП /чип/ [chip] — кристал напівпровідника разом із нанесеною на ньому схемою інтегральною.

ЧУТКИ /слухи/ — 1) Відомості, вісті, вірогідність яких не встановлена. 2) Специфічний вид інформації,

що з'являться спонтанно із-за інформаційного вакууму серед певних прошарків населення, або спеціально будь-ким розповсюджується для впливу на суспільну свідомість. Ч. класифікуються за трьома параметрами: експресивному (у відповідності з емоційними станами, що відображені в змісті ч. і в особливостях емоційних реакцій на нього — чутки-бажання, чутки-страховиська, чутки агресивні роз'єднувальні), інформаційному (у відповідності із ступенем вірогідності ч. — абсолютно невірогідні, частково вірогідні [з елементами правдоподібності], правдоподібні) і за ступенем впливу на психіку людей: ч., що розбурхують суспільну думку, але не викликають явно вираженої антисуспільної поведінки окремих осіб або навіть цілих груп; ч., що викликають антисуспільну поведінку серед деякої частини певних соціальних груп; ч., що порушують соціальні зв'язки й організаційно-керівні відносини між людьми, викликають масові безпорядки, паніку і т. ін. Застосування ч. потребує великого мистецтва й обережності, тому що їхній зміст після початку розповсюдження виходить з-під контролю. Циркулюючи в масах, ч. дуже часто піддаються змінам, аж до того, що набувають смисл, протилежний тому, що передбачався їхніми авторами. Для того щоб інформація стала ч., необхідно щоб: інформація мала значення для об'єкта впливу (тобто прямо стосувалася його інтересів); інформація була зрозумілою усім учасникам трансляції ч.; володіння інформацією сприяло підвищенню авторитету транслятора слуху. Використання ч. в інтересах війни психологічної — розповсюдження інформації вигідної джерелу. Ч. можуть виникати також спонтанно, внаслідок неправильного сприйняття інформації, що розповсюджується зацікавленою стороною. Тоді вони можуть мати негативний ефект.

Ч. агресивні роз'єднувальні /с. агрессивные разобщающие/ — чутки, інформація в яких має за мету розлад у взаємовідносинах у середовищі противника, порушує соціальні зв'язки.

Ч.-бажання /с.-желания/ — чутки, інформація в яких має за мету викликати розчарування з причини нездійснених сподівань та деморалізувати об'єкт впливу.

Ч.-страховиська /с.-пугала/ — чутки, інформація в яких ставить за мету ініціювати у об'єкта впливу стан тривоги й невпевненості. Такими можуть бути чутки про смертельну суперзброю, якою володіє про-

тивник (тобто сторона, що розповсюджує чутку), про катастрофічну нестачу продовольства, про майбутні бомбардування, про зараження місцевості і т. ін.

ЧУТЛИВІСТЬ /чувствительность/ [sensitivity, sensitiveness, sensibility] — величина, що характеризує здатність відображати, фіксувати зовнішні впливи, зміни, прояви певного рівня.

Ч. мікрофона /ч. микрофона/ — один з основних показників мікрофона, який оцінюється коефіцієнтом перетворення тиску акустичної хвилі в рівень електричного сигналу. Так як ч. м. для різних частот акустичних коливань різна, то вона визначається на частоті найбільшої чутливості слухової системи людини, — 1000 Гц. Вимірювання проводяться для акустичної хвилі, напрямок розповсюдження якої перпендикулярний до поверхні мембрани, в вольтах або мілівольтах на Паскаль (В/Па, мВ/Па). Ч. м. залежить в основному від параметрів фізичних процесів в акустоелектричних перетворювачах і площі мембрани мікрофона. Ч. м. підвищується із збільшенням площі мембрани приблизно у квадратичній залежності.

Ч. радіоприймача /ч. радиоприемника/ [receiver s.] — мінімальна потужність або напруга на вході радіоприймача, при якій рівень сигналу і відношення сигнал/шум на його виході забезпечує нормальну роботу кінцевих пристроїв (реєстрації і індикації). Таку чутливість називають ще реальною. В діапазонах дециметрових і більш коротких хвиль чутливість вимірюють у ватах або децибелах по відношенню до рівня в 1 мВт, у спектральній густині у Вт/Гц або децибелах (по відношенню до Вт/Гц), на метрових і більш довгих — в мікровольтах (мкВ). Реальна ч. р. сучасних професійних приймачів супергетеродинних дециметрових і сантиметрових хвиль складає 10^{-12} — 10^{-15} Вт або -180 — -200 дБ по відношенню до Вт/Гц, приймачів метрових і більш довгих хвиль — 0,1–10 мкВ.

Ч. радіоприймача гранична /ч. радиоприемника предельная/ — чутливість радіоприймача, яка відповідає потужності (напрузі) вхідного сигналу, що дорівнює потужності (напрузі) шумів вхідних ланцюгів радіоприймача. Інформація корисного сигналу потужністю менше потужності шумів радіоприймача настільки сильно ними спотворюється, що передавання інформації можливе тільки при кодуванні її зава-

достійкими кодами.

Ч. радіоприймача порогова /ч. радиоприемника пороговая/ — чутливість радіоприймача, визначена мінімальним рівнем радіосигналу на його вході при рівних рівнях корисного сигналу і шуму на виході радіоприймача.

Ч. радіоприймача, обмежена підсиленням /ч. радиоприемника, ограниченная усилением/ — чутливість радіоприймача, визначена мінімальним рівнем радіосигналу на його вході, необхідним для одержання заданого рівня сигналу на виході радіоприймача. Заданим рівнем сигналу на виході радіоприймача можуть бути номінальні вихідні потужність або напруга на опорі навантаження.

Ч. радіоприймача, обмежена шумами /ч. радиоприемника, ограниченная шумами/ — чутливість радіоприймача, визначена мінімальним рівнем радіосигналу на його вході при заданому відношенні рівнів корисного сигналу і шуму і заданому рівні корисного сигналу на виході радіоприймача.

Ч. фотографічного матеріалу /ч. фотографического материала/ — властивість світлочутливого шару фотографічного матеріалу хімічно змінюватися внаслідок дії світла, в результаті чого створюється приховане зображення, яке після проявлення перетворюється у видиме. Ч. ф. м. вимірюється в умовних одиницях ISO (раніше в одиницях ГОСТу), в США і багатьох інших країнах — в одиницях ASA, в Німеччині — в DINах.

Ш

ШАНТАЖ /шантаж/ [blackmail] (франц. chantage — вимагання) — 1) Погроза розголошення компрометуючих або начебто компрометуючих відомостей з метою одержання якихось вигод. 2) Операція інформаційно-психологічної війни, спрямована на створення умов, при яких об'єкт шантажу ставиться в ситуацію, коли відмова від виконання умов, поставлених суб'єктом впливу, може реально спричинити неприйнятні для об'єкта наслідки. За метою умовно можна виділити ш., спрямований на: одержання грошей; одержання зброї, наркотиків, засобів пересування і т.ін.; спонукання об'єкта до здійснення або відмови від

здійснення деяких дій. За змістом на: політичний, економічний, психологічний, змішаний. Практика показує, що для об'єкта немає ніяких гарантій реалізації обіцянок суб'єкта, навіть якщо він абсолютно повністю виконав усі його вимоги. З іншої сторони, відмова від виконання вимог шантажиста також не дає ніяких гарантій, що від приведе свої погрози в дію.

ШАФА /шкаф/ [cabinet] — пристрій у вигляді ящика з дверцятами, що має певне призначення.

Ш. металева /ш. металлический/ — конструкція захисту об'єктів інженерна, призначена для зберігання документів із невисоким грифом конфіденційності, цінних речей, невеликих сум грошей. Надійність ш. м. визначається тільки міцністю металу і секретністю замка.

ШАХРАЙСТВО /мошенничество/ [fraud] — обман, шахрайські дії з корисною метою.

Ш. в стільникових мережах /м. в сотовых сетях/ [fraud] — неправомочний та навмисний доступ абонента до послуг зв'язку з метою особистої або колективної вигоди. Форми прояву ш. можуть бути різноманітними. Це і зловживання довірою компанії-оператора, у тому числі перепродажа ефірного часу, різноманітного роду переробки стільникових апаратів, підробка ідентифікаторів, викрадення апаратів з наступною їх переробкою.

Ш. з контрактом /м. с контрактом/ [subscription f.] — надання невірних даних при укладанні контракту, використання послуг у кредит з наміром не сплачувати за них.

Ш. з украденим телефоном /м. с украденным телефоном/ [stolen phone f.] — несанкціоноване використання вкраденого або загубленого апарата стільникового зв'язку.

Ш. процедурне /м. процедурное/ [procedural f.] — неправомочне використання роумінгу та інших бізнес-процедур (наприклад білінгу) з метою зменшення оплати послуг зв'язку.

Ш. технічне /м. техническое/ [technical f.] — неправомочне виготовлення телефонних апаратів стільникового зв'язку або платіжних телефонних карток з фальшивими ідентифікаторами абонентів, номерів та платіжних відміток.

Ш. хакерське /м. хакерское/ [hacking f.] — проникнення хакерів в комп'ютерну систему захисту для

видалення механізмів захисту або переконфігурування системи для своїх цілей.

ШИФР /шифр/ [cipher, code, pressmark] (франц. chiffre, букв. — цифра, від араб. сіфр — нуль) — сукупність обернених перетворень тексту повідомлень, які виконуються з метою схову від зловмисника (противника) інформації, яка знаходиться у повідомленні.

Ш. ADFGVX /ш. ADFGVX/ [ADFGVX с.] — представник шифру дроблення, в якому кожний символ вхідного алфавіту (латинські літери та десяткові цифри) замінюється біграмою із символів A,D,F,G,V,X, а отриманий шифртекст зашифровується шифром одиночної перестановки.

Ш. BlowFish /ш. BlowFish/ — шифр Фейстеловського типу з довжиною блока 64 біта, із перемінною довжиною ключа (до 448 біт) з 16 циклами, один алгоритм використовується і для зашифровування, і для розшифровування інформації. Алгоритм складається з двох частин: розширення ключа та шифрування. На етапі розширення ключа з основного ключа отримують кілька підключових матриць загальним розміром до 4168 байт. Крокова функція — добуток перестановок, залежних від ключа, підстановок, залежних від ключа і даних та додавання за модулем 2. Усі операції здійснюються над 32-бітними словами, що забезпечує досить високу швидкість.

Ш. CAST /ш. CAST/ — шифр Фейстеловського типу з довжиною блоку 64 біта, з довжиною ключа 64 біт, з 8 циклами, один алгоритм використовується і для зашифровування, і для розшифровування інформації. Використовує шість S-блоків розміром 8x32 біта, які використовуються в якості ключа довгострокового подібно до шифру стандарту шифрування ГОСТ 28147-89. Крокова функція — добуток підстановок, які реалізуються за допомогою S-блоків та додавання за модулем 2. CAST стійкий до лінійного та диференційного методів криптоаналізу. Модифікація шифру CAST з довжиною ключа 256 біт (CAST-256) розглядалася серед інших 15 кандидатів до стандарту AES на першому етапі оцінювання. Уряд Канади розглядає алгоритм як новий національний стандарт шифрування.

Ш. FEAL /ш. FEAL/ [FEAL (Fast data Encipherment ALgorithm)] — родина DES-подібних шифрів, базова схема якого розроблена А. Шимізу та Ш. Міагучі з японської фірми NTT. FEAL-N є шифром Фей-

стеловского типу з довжиною блока 64 біта, довжиною ключа 64 біта та змінним (N-парне ціле) числом циклів, один алгоритм використовується і для зашифровування, і для розшифровування інформації. Існують варіанти FEAL-4, FEAL-8, FEAL-16, FEAL-24, FEAL-32. Існує також варіанти FEAL-NX з довжиною блока 64 біта, довжиною ключа 128 біт та змінним (N-парне ціле) числом циклів. Ш. FEAL відіграв значну роль у розвитку диференційного та лінійного методу криптоаналізу.

Ш. IDEA /ш. IDEA/ [IDEA (International Data Encryption Algorithm)] — алгоритм шифрування, розроблений швейцарським криптологом Д.Массі та Х.Лейем (X. Lai) в 1990 році. Спочатку алгоритм носив назву PES (Proposed Encryption Standard), потім після доробки алгоритму — IPES (Improved Proposed Encryption Standard) та в 1992 році назву змінили на IDEA. В IDEA використовується новий узагальнений принцип Фейстела, в якому блок вхідного повідомлення розбивається на 4 рівних підблоки, кожний з яких використовується для модифікації трьох інших. В основу шифру покладені останні досягнення криптологічної науки, в тому числі використання комбінованих операцій з різних алгебраїчних груп. Зокрема, для побудови крокової функції використовуються операції $\oplus$, додавання за модулем 2^{16}, множення за модулем $2^{16}+1$.IDEA є блочним шифром з довжиною блока 64 біта, довжиною ключа 128 біт з 8 циклами, один алгоритм використовується і для зашифровування, і для розшифровування інформації. За думкою фахівців, на сьогодні IDEA — це один з найбільш “стійких” алгоритмів.

Ш. MARS /ш. MARS/ — шифр блоковий симетричний з довжиною блока 128 бит, змінною довжиною ключа (від 128 до 1248 біт). При розробці ставилось за мету підвищення співвідношення стійкість/швидкість. Реалізація алгоритму на мові С та мікропроцесорі Pentium-Pro 200 MG працює зі швидкістю 65 МБіт/с, на мікропроцесорі PowerPC 200 MG — 85 МБіт/с. При апаратній реалізації — в 10 разів швидше ніж на програмній. За попередніми оцінками , криптоаналіз диференційний та лінійний потребує більш ніж 2^{128} відкритих текстів. В MARS у повній мірі використовуються можливості сучасної обчислювальної техніки по виконанню швидкого множення та зсуву, що залежить від даних. При цьому, на відміну від шифру IDEA, їхня загальна кількість зменшена до 16 (замість 32). Використовуються операції множе-

ння, $\oplus$, $\boxplus$, $\boxminus$, зсуву на фіксоване число позицій та табличної заміни (1 таблиця з 512 32-бітних слів, яка іноді розглядається як 2 таблиці по 256 32-бітних слів). Внутрішня структура 32-х розрядна. Використовується мережа Фейстела 3-го типу, яка на кожному циклі використовує одне слово даних (та декілька слів ключа) для модифікації усіх трьох слів, що залишилися. В шифрі MARS також використовується ідеї "криптографічного ядра" або "змішаної конструкції", коли перші та останні цикли побудовані інакше, ніж середні. Структура шифру описується наступним чином: етап попереднього "перемішування" — додавання з ключем за модулем 2^{32}, 8 циклів безключового перетворення Фейстела 3-го типу з використанням S-блоків "у прямому проходженні"; етап "криптоядра" — 16 циклів (8 — в прямому, 8 — у зворотному) перетворення Фейстела 3-го типу; етап заключного "перемішування" — 8 циклів безключового перетворення Фейстела 3-го типу з використанням S-блоків "у зворотному проходженні" та віднімання ключа за модулем 2^{32}. Ш. MARS — один з 5 алгоритмів, з яких буде обрано алгоритм стандарту шифрування даних AES.

Ш. RC4 /ш. RC4/ — шифр потоковий симетричний із змінною довжиною ключа. Запропонований Ronald L. Rivest. (M.I.T. Laboratory for Computer Science) в 1987 році. В алгоритмі використовуються 256 байтових S-блоків, які разом з операцією додавання за модулем 256 використовуються в процедурі генерації гами з ключа. RC4 з довжиною ключа 40 біт не вважається стійким шифром.

Ш. RC5 /ш. RC5/ — симетричний шифр блоковий із змінними довжиною блока, ключа та кількістю циклів. Запропонований Ronald L. Rivest. Для перетворення даних використовуються 3 операції: додавання за модулем 2, додавання та зсув. Зсув залежить як від ключа, так і від даних. Дослідження стійкості шифру з 64-бітною довжиною блока показує необхідність використання принаймні 16 циклів шифрування.

Ш. RC6 /ш. RC6/ — симетричний шифр блоковий із змінними довжиною блока, ключа та кількістю циклів. Запропонований Ronald L. Rivest. (M.I.T. Laboratory for Computer Science) та M.J.B. Robshaw (RSA Laboratories). RC6 більш правильно було б називати RC6-$w/r/b$, де w — довжина слова в бітах, r — число циклів, b — довжина ключа в байтах. При $w = 32, r = 20$ та змінною довжиною ключа — 16, 24, 32 байт. RC6 поданий як кандидат стандарту шифрування даних AES. Реалізація алгоритму на мові C та

мікропроцесорі Pentium-Pro 200MHz виконує операцію шифрування із швидкістю 5,19 Мбайт/с при будь-якому розмірі ключа, а на мові Асемблера — 12,6 Мбайт/с. Процедура шифрування RC6 має вигляд:

Вхід:

Відкритий текст зберігається в чотирьох w-бітних регістрах A, B, C, D;

r — число циклів

w-бітні ключі на кожний цикл $S[0, \cdots, 2r+3]$.

Вихід:

Шифртекст у регістрах A, B, C, D.

Процедура:

$B = B + S[0]$

$D = D + S[1]$

for $i = 1$ **to** r **do**

{

$t = (B \times (2B + 1)) <<< \lg w$

$u = (D \times (2D + 1)) <<< \lg w$

$A = ((A \oplus t) <<< u) + S[2i]$

$C = ((C \oplus u) <<< t) + S[2i + 1]$

$(A, B, C, D) = (B, C, D, A)$

}

$A = A + S[2r + 2]$

$C = C + S[2r + 3]$, де

$+$ цілочислове додавання за модулем 2^w

$-$ цілочислове віднімання за модулем 2^w

$\oplus$ порозрядне додавання за модулем 2 w-бітних слів

$\times$ цілочислове множення за модулем 2^w

$<<<$ циклічний зсув ліворуч w-бітного слова

$>>>$ циклічний зсув праворуч w-бітного слова.

При апаратній реалізації алгоритму виконується співвідношення швидкість/розмір, що дозволяє підвищити швидкість роботи до 1,3 Гбіт/с. За попередніми оцінками, для проведення криптоаналізу диференційного та лінійного потрібно більш ніж 2^{128} відкритих текстів. Ш. RC6 — один з 5 алгоритмів, з яких буде обрано алгоритм стандарту шифрування даних AES.

Ш. SEAL /ш. SEAL/ — симетричний шифр потоковий з довжиною ключа 160 біт. SEAL не є потоковим шифром у традиційному розумінні, а є так званою сім'єю псевдовипадкових функцій. За даним 160-бітним ключем k та 32-бітним числом n SEAL генерує гаму L, довжина якої залежить від $k(n)$, але не більше 64 кБайт. Така побудова шифру забезпечує дуже цікаву та практично корисну властивість: просте отримання будь-якої позиції у послідовності ключової. Ш. SEAL побудований з використанням наступних ідей: використання S-блоків великого розміру, залежних від ключа; некомутативних арифметичних операцій (додавання та додавання за модулем 2); захист внутрішнього стану шифру за допомогою додаткового шифрування; використання різних функцій крокових на різних циклах та ітераціях алгоритму; використання для ініціалізації ключа процедури, заснованої на хеш-функції стандарту SHA. SEAL надзвичайно ефективний за швидкодією: 58 МБіт/с на мікропроцесорі Intel 486/50МГц.

Ш. SkipJack /ш. SkipJack/ — симетричний шифр блоковий з довжиною ключа 80 біт, довжина вхідного блока 64 біта, 4 режиму (подібно режимам DES), 32 цикли шифрування. SkipJack є шифром Фейстелівського типу. Алгоритм оперує з чотирма 16-бітними підблоками. В перших восьми циклах два підблоки (перший та другий) перетворюються з використанням односторонньої функції від першого й четвертого та першого підблоків відповідно. Двом іншим підблокам (третьому та четвертому) присвоюється значення відповідно другого та третього підблоків попереднього циклу шифрування. В наступних восьми циклах два підблоки

(другий та третій) перетворюються з використанням односторонньої функції від першого та першого й другого підблоків відповідно. Двом іншим підблокам (першому та четвертому) присвоюється значення відповідно четвертого та третього підблоків попереднього циклу шифрування. Після цього перші й другі вісім циклів повторюються ще раз. Характерною особливістю алгоритму є застосування в циклі шифрування операції додавання за модулем 2 із значенням лічильника номера циклу. Для побудови функції односторонньої використовуються фіксована байтова таблиця підстановок. SkipJack розроблявся як секретний алгоритм і є частиною стандарту шифрування США на криптосистеми з депонуванням ключів(Escrow Encryption Standard) більш відомий як програма Clipper. Однак 23 липня 1998 року розсекречений АНБ. Реалізований у мікросхемах Clipper та Capstone. Швидкість шифрування за алгоритмом SkipJack мікросхемою Clipper складає 15-20 МБ/с. У звіті про дослідження Skipjack групою американських криптологів, відзначається: алгоритм стійкий щодо силової (brute-force) атаки; при аналізі алгоритму на наявність криптографічних слабкостей (подібність псевдовипадковому криптографічно сильному датчикові, криптоаналіз диференційний та інші) не було виявлено криптоаналітичних атак на алгоритм; стійкість Skipjack не залежить від зберігання в секреті опису алгоритму.

Ш. TwoFish /ш. TwoFish/ — симетричний шифр блоковий з довжиною блока 128 біт, з довжиною ключа128, 192 та 256 біт з 16 циклами, один алгоритм використовується і для зашифровування, і для розшифровування інформації. Алгоритм оперує з чотирма 32-бітовими підблоками. Узагалі виконуються перетворення подібно до шифру Фейстеловского типу за винятком спеціальних операцій зсуву. Крокова функція — добуток підстановок, залежних від ключа та даних, що реалізуються за допомогою чотирьох байтових S-блоків та лінійних перестановок, заснованих на MDS-матрицях, деяких спеціальних перетворень та додавання за модулем 2. Ш. TwoFish — один з 5 алгоритмів, з яких буде обрано алгоритм стандарту шифрування даних AES.

Ш. автоключа /ш. автоключа/ [autokey c.] — шифр заміни, в якому перші символи замінюються на символи, що є сумою за модулем n з символами ключа, а інші — символами, що є сумою за модулем

n з першими символами відкритого або отриманого шифртексту. Тут n — кількість символів в алфавіті. Наприклад, текст "YOU ARE MAN" з ключем "KEY" шифрується таким чином:

$$\begin{array}{cccccccccc} Y & O & U & A & R & E & M & A & N \\ K & E & Y & Y & O & U & A & R & E \\ I & R & S & Y & F & Y & M & R & R. \end{array}$$

В більш широкому розумінні — шифр, в якому ключ формується з тексту повідомлення або шифртексту.

Ш. асиметричний /ш. ассиметрический/ [asymmetric c.] — див. криптосистема асиметрична).

Ш. атбаш /ш. атбаш/ — різновид шифру простої заміни, в якому перша буква алфавіту замінюється на останню, друга — на передостанню і так далі. Один із найперших шифрів, використовується в Біблії для шифрування слова "ВАВИЛОН" (відповідна криптограма – "СЕССАХ").

Ш. афінний /ш. афинный/ [affine c.] — підклас шифрів заміни, в якому символ (група символів) відкритого тексту перетворюється в символ шифртексту за допомогою афінного перетворення. Прикладом а. ш. є шифр, в якому кожний символ x повідомлення заміщується символом $E(x) = (ax + s) mod n$, де $0 < a < n, 0 \leq s < n$ — ключ, $(a, n) = 1$, а — кількість символів вхідного алфавіту.

Ш. безключової перестановки /ш. безключевой перестановки/ [geometric transposition keyless c.] — шифр перестановки, який утворюється просто за правилом розбиття вхідного тексту на блоки, наприклад, блок утворюють кожний k символ повідомлення. Звичайно, це реалізується за допомогою таблиць — вхідне повідомлення записується по стовпчиках таблиці, а шифрограма утворюється зчитуванням по рядках. Ключем є розмір таблиці, тому термін не є вдалим.

Ш. біграмний (диграфний) /ш. биграммный (диграфный)/ [bigram c.] — шифр заміни, в якому кожна біграма відкритого тексту замінюється на якусь біграму.

Ш. блоковий /ш. блочный/ [block c.] — див. шифрування блокове.

Ш. блоковий ітеративний /ш. блочный итеративный/ [iterative block c.] — шифр блоковий, який утворюється послідовним повторенням деякої шифруючої функції, яка називається кроковою або цикло-

вою функцією, а її застосування до блоку вхідної інформації — циклом шифрування. Ключ цикловий для кожного циклу виробляється з загального ключа. Кількість повторів шифруючої функції називається числом циклів шифру.

Ш. Вернама /ш. Вернама/ [Vernam c.] — див. шифр одноразового блокнота.

Ш. Віженера /ш. Виженера/ [Vigener c.] — різновид шифру поліалфавітної підстановки. Текст відкритий і криптограма записуються в одному і тому ж алфавіті. Кожний символ вхідного повідомлення замінюється на символ, який є результатом циклічного зсуву символів на кількість позицій, що дорівнює номерові символу ключа в алфавіті (нумерація символів алфавіту починається з 0). Така операція задається так званими таблицями Віженера. На відміну від шифру Цезаря шифрування однакових символів залежить від їхньої позиції у повідомленні. Ш. В. не є стійким до статистичного криптоаналізу. Він піддається дешифруванню за допомогою методу Казискі.

Ш. гамування /ш. гаммирования/ — див. гамування.

Ш. гомофонний /ш. гомофонный/ [homophonic c.] — шифр заміни, в якому кожний символ відкритого тексту замінюється будь-яким символом з кількох можливих (із деякої множини). Кількість елементів множини може залежати від частот символів у відкритому тексті.

Ш. Грибоєдова /ш. Грибоедова/ — різновид геометричної стеганографії. Використовувався А.С. Грибоєдовим у дипломатичному листуванні з Персії. Ключем є трафарет у якому прорізані віконця під літери. Трафарет накладається на лист, пишеться секретне повідомлення, потім дописуються розкидані по листу літери так, щоб вони складали змістовний текст.

Ш. Гросфельда /ш. Гросфельда/ — різновид шифру поліалфавітної підстановки. Ключ записується у числовому вигляді в десятковій системі. Кожна цифра ключа визначає число позицій, на яке зсувається в алфавіті символ відкритого тексту. Ключ повторюють циклічно.

Ш. дроблення (мережа підстановок-перестановок) /ш. дробления (сеть подстановок-перестановок)/ [SP-network] —- шифр композиційний, який є добутком скінченного числа шифрів підста-

новки та перестановки. Найстарішим представником цього типу шифрів є шифр ADFGVX.

Ш. заміни (підстановки) /ш. замены (подстановки)/ [substitution] — метод криптографічного перетворення, що полягає у заміні кожного символу (блоку) тексту відкритого на інший символ з того ж алфавіту відповідно до значення ключа.

Ш. ідеальний /ш. идеальный/ [provable-secure c., unconditionally secure c.] — шифр, що має криптостійкість абсолютну.

Ш. інволютний /ш. инволютный/ — шифр, для якого алгоритми зашифровування та розшифровування є однаковими.

Ш. Кардано /ш. Кардано/ — різновид шифрів перестановки, називається ще шифром решітки. Ключем є квадратні таблиці, в яких четверта частина комірок прорізана так, щоб при чотирьох поворотах трафарету вони покривали таблицю цілком. У прорізані комірки при кожному повороті записуються символи тексту відкритого. Кількість подібних решіток швидко зростає із збільшенням їхнього розміру. Ш. К. легко піддається зламу, однак його ідеї використовувалися для ускладнення шифрів підстановки.

Ш. композиційний (похідний) /Ш. композиционный (производный)/ [product c.] — шифр, який є добутком шифрів, заснованих на простих операціях заміни, перестановки, афінних перетвореннях, арифметичних операціях, операції XOR та операціях модульної арифметики. Частковим видом цих шифрів є шифр подрібнення.

Ш. контекстнозалежний /ш. контекстнозависимый/ — те ж, що шифр поліграмний.

Ш. контекстнонезалежний /ш. контекстнонезависимый/ — те ж, що шифр монограмний.

Ш. Люцифер /ш. Люцифер/ [Lucifer c.] — шифр мережі підстановок-перестановок, розроблений Х. Фейстелом на початку 1970 років, ідеї якого лягли в основу алгоритму DES. Люцифером називається також програма досліджень у галузі комп'ютерної криптографії, розпочата наприкінці 1960-х років Х. Фейстелом та У. Тучманом. Ш. Л. є 16-цикловим, з довжиною вхідного блока 128 біт, S-блоками 4x4 біта.

Ш. монограмний /ш. монограммный/ [monogram c.] — шифр заміни, в якому кожний символ вхідного

алфавіту замінюється на якийсь символ з вихідного алфавіту.

Ш. одиночної (простої) перестановки /ш. одиночной (простой) перестановки/ [simple substitution c.] — шифр перестановки, в якому блоки вхідного повідомлення переставляються за значенням ключа однократно. Реалізується в ручних криптосистемах за допомогою таблиць.

Ш. одноалфавітний (моноалфавітний) /ш. одноалфавитный (моноалфавитный)/ [monoalphabetic substitution c.] — шифр заміни, в якому правило заміни символу (символів) не залежить від позиції символу у відкритому тексті.

Ш. одноразового блокноту /ш. одноразового блокнота/ [one-time pad (OTP)] — шифр заміни з довжиною ключа, що дорівнює довжині тексту, що шифрується. Для шифрування нового тексту обирається новий ключ. Ключі обираються випадково з ключового простору. К. Шенноном доведено, що цей шифр є криптостійким у теоретико-інформаційному сенсі (див. криптостійкість абсолютна, шифр ідеальний).

Ш. перестановки /ш. перестановки/ [transposition] — метод перетворення криптографічного, що полягає у тому, що символи (блоки) вихідного повідомлення міняються місцями відповідно до значення ключа. Більш точно, якщо $M = m_1m_2m_3...m_t$ — блок довжини t вхідного повідомлення, то шифртекстом є $C = E_K(M) = m_{s(1)}m_{s(2)}m_{s(2)}...m_{s(t)}$. Ключем є інформація, необхідна для обчислення функції $s(i)$ для $i = 1, ..t$. Параметр t називається періодом шифру перестановки.

Ш. Плейфера /ш. Плейфера/ — різновид шифру поліграмної підстановки. Ключем є всі символи алфавіту, розміщені у випадковому порядкові у квадратній матриці (для англійської мови розмір матриці $5x5$, літера j, яка рідко використовується, відкидається). Відкрите повідомлення розбивають на біграми і до кожної з них застосовують наступний алгоритм. Якщо літери біграми відкритого тексту (p_1, p_2) розміщені в різних рядках та стовпчиках матриці, вони утворюють квадратну підматрицю розміром $2x2$. Кути матриці, відмінні від (p_1, p_2) утворюють символи криптограми (c_1, c_2) таким чином, що c_1 належить тому самому стовпчикові, що і p_1. Якщо (p_1, p_2) належать одному рядкові, то c_1 визначається як символ безпосередньо правий від p_1, а c_2 — безпосередньо правий від p_2(для останнього стовпчика правим є перший стовпчик).

Якщо (p_1, p_2) належать одному стовпчикові, c_1 визначається як символ безпосередньо нижчий від p_1, а c_2 — безпосередньо нижчий від p_2(для останнього рядка правим є перший рядок). Якщо $p_1 = p_2$, то між p_1 і p_2 установлюється спеціально обраний символ вхідного алфавіту та відкритий текст, що залишився, перерозбивається на біграми, після чого вище згаданий алгоритм повторюється. Існують модифікації ш. П. для випадку двох та чотирьох квадратів (див. шифр Уітстона).

Ш. подвійної перестановки /ш. двойной перестановки/ [double transposition c.] — шифр перестановки, в якому блоки вхідного повідомлення переставляються за значенням ключа два рази. При цьому розмір блоків та довжини ключів (таблиць) у першому разі відрізняється від другого (довжини ключів та блоків взаємно прості).

Ш. поліалфавітний /ш. полиалфавитный/ [polyalphabetic substitution c.] — шифр заміни, в якому правило заміни символу (символів) залежить від позиції символу у відкритому тексті.

Ш. Полібіанський квадрат /ш. Полибианский квадрат/ — різновид шифру простої заміни. Ключем є всі символи алфавіту, розміщені у випадковому порядкові у квадратній матриці (для грецької мови розмір матриці 5×5, додається символ пропуску). Кожний символ тексту відкритого замінюється на символ, нижчий від нього в тому самому стовпчикові, для нижнього рядка — на символ у першому рядку.

Ш. поліграмний /ш. полиграммный/ [polygram positionally dependent c.] — шифр заміни, в якому вхідний текст розбивається на поліграми (l-грами для деякого фіксованого $l > 1$) і кожна з них замінюється на якийсь символ чи групу символів.

Ш. потоковий /ш. поточный/ [stream c., sequence c.] — див. шифрування потокове.

Ш. простої заміни /ш. простой замены/ [simple substitution c.] — шифр заміни з довжиною ключа, що дорівнює одиниці.

Ш. роторний /ш. роторный/ [rotor c.] — варіант шифру поліалфавітної заміни, який реалізується за допомогою електромеханічних шифраторів, основою яких є шифруюче колесо — диск з ізоляційного матеріалу (гуми або бакеліту), на обох сторонах якого по периметру розміщені символи алфавіту та електричні

контакти (по одному на кожний символ алфавіту). В шифраторах роторного типу, звичайно, декілька (від чотирьох до кількох десятків) роторів. Ключ роторної системи визначається роторами, початковим зсувом кожного ротора, функціями повороту роторів. Прикладами роторних шифрів (систем) є Enigma (Німеччина), SIGAB (США), PURPLE (Японія).

Ш. симетричний /ш. симметрический/ [symmetric c.] — Див. криптосистема симетрична.

Ш. скитала /ш. скитала/ [skitala c.] — шифр перестановки, який отримав свою назву від назви стрижня, на який намотувалися свитки папірусу. Текст вхідного повідомлення пишеться вздовж скитали, а читається як звичайно. Ключем є скитала. Це один з найдавніших шифрів, використовувався ще древніми греками.

Ш. складеної перестановки /ш. составной перестановки/ — шифр перестановки, в якому до вхідного повідомлення послідовно двічі чи більше застосовується шифр перестановки з періодами $t_1, t_2, t_3, \ldots$.

Ш. стандарту шифрування DES /ш. стандарта шифрования DES/ [c. DES] — див. стандарт шифрування DES.

Ш. стандарту шифрування ГОСТ 28147-89 /ш. стандарта шифрования ГОСТ 28147-89/ — див. стандарт шифрування ГОСТ 28147-89.

Ш. Уитстона /ш. Уитстона/ — модифікація шифру Плейфера. Іноді шифр називають шифром двох квадратів. Замість одного квадрата, як у шифрі Плейфера, застосовується два квадрати, які заповнюються символами алфавіту випадково та незалежно один від одного. Перший символ біграми вхідного тексту обирають у першому квадраті, другий — в іншому. Далі шифрують, як у шифрі Плейфера, розглядаючи обидва квадрати, як один. У порівнянні до шифру Плейфера така модифікація збільшує кількість можливих ключів. Подібно до цього алгоритму поступають і у випадку чотирьох квадратів.

Ш. Фейстеловського типу (мережа Фейстела 1-го типу) /ш. Фейстеловского типа (сеть Фейстела 1-го типа)/ [Feistel c.] — ітеративний блоковий шифр, побудований за принципом, запропонованим Х. Фейстелом. За цим принципом вхідне повідомлення розбивається на блоки довжини $2 \cdot t$, кожний блок від-

критого повідомлення (L_0, R_0) для t - бітових підблоків L_0, R_0 перетворюється в блок шифртексту (L_r, R_r) за допомогою ітеративного блокового шифру з r циклами, де $r \geq 1$. Для $1 \leq i \leq r$ i-те перетворення визначається як $L_i = R_{i-1}, R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$, де K_i — цикловий ключ.

Ш. Хілла /ш. Хилла/ [Hill c.] — шифр поліграмний, в якому зашифровування (розшифровування) здійснюються за допомогою добутку матриці вхідного повідомлення (шифрограми) на матрицю ключа. Ключова матриця повинна бути невиродженою, тобто мати зворотну в векторному просторі $Z_{m,n}$, де m — число символів вхідного алфавіту, n — розмір блока шифрування.

Ш. Цезаря /ш. Цезаря/ [Caesar c.] — шифр простої заміни зі значенням ключа $k = 3$, тобто кожна літера вхідного алфавіту замінюється (циклічно) на кожну четверту, рахуючи себе першою. Інколи цю назву використовують як синонім шифрів простої заміни взагалі.

ШИФРАТОР /шифратор/ [encipherer, encrypter] — пристрій, призначений для автоматичного шифрування. Функцію з дешифрування виконує дешифратор.

Ш. комерційний /ш. коммерческий/ — шифратор, який поступає у вільний продаж.

ШИФРОВКА /шифровка/ [ciphered (coded) message] — який-небудь зашифрований текст (телеграма, лист і т. ін.). Див. також криптограма, шифрограма.

ШИФРОГРАМА /шифрограмма/ [ciphered (coded) message] — див. криптограма.

ШИФРСИСТЕМА /шифрсистема/ — див. система шифрувальна.

ШИФРТЕКСТ /шифртекст/ [ciphertext] — дані, отримані у результаті зашифровування тексту відкритого.

ШИФРУВАННЯ /шифрование/ [encryption] — 1) Процес зашифровування або розшифровування. 2) Процес перетворення криптографічного даних, за допомогою якого текст відкритий перетворюється в шифртекст з метою захисту від несанкціонованого доступу.

Ш. абонентське /ш. абонентское/ [end-to-end e.] — *шифрування даних*, яке передбачається у складі або на виході джерела інформації з відповідним розшифровуванням тільки у складі або на вході кінцевого

користувача інформації.

Ш. блокове /ш. блочное/ [block e.] — спосіб шифрування, при якому кожний блок, що передається, шифрується незалежно.

Ш. даних /ш. данных/ — процес зашифровування і розшифровування.

Ш. для кінцевого користувача /ш. для конечного пользователя/ — те ж, що шифрування абонентське.

Ш. з відкритим ключем /ш. с открытым ключом/ [public key cryptography] — криптографічний метод, в якому використовуються окремі ключі для зашифровуванняі розшифровування.

Ш. інформації /ш. информации/ [data e.] — перетворення криптографічне інформації з метою її захисту від доступу несанкціонованого.

Ш. ймовірнісне /ш. вероятностное/ [probability e.] — вид шифрування, при якому відкритому текстові M ставиться у відповідність не один шифртекст C, а їхня деяка множина C_M, з якої кожний елемент $C \in C_M$ вибирається з певною ймовірністю, тобто $E(M)$ є випадкова величина, розподілена на множині C_M. Вважається, що для різних відкритих текстів $M_1 \neq M_2$ множини C_{M_1}, C_{M_2} не перетинаються. Ідея запропонована Ш. Гольдвассер та С. Мікелі. Прикладом імовірнісної криптосистеми є криптосистема Ель-Гамаля.

Ш. лінійне /ш. линейное/ [link-by-link encipherement] — *шифрування даних*, що охоплює ділянку від входу до виходу лінії зв'язку телекомунікаційної системи, характеристики якого не залежать від конкретного користувача лінії зв'язку.

Ш. методом РША /ш. методом РША/ [RSA e.] — метод шифрування, запропонований Рівестом, Шаміром і Адлеманом, при якому ключ, що використовується для зашифровування, не збігається з ключем для розшифровування (останній повинен бути відомим одержувачу); відноситься до методів шифрування з відкритим ключем.

Ш. мовної інформації цифрове /ш. речевой информации цифровое/ [voice e.] — спосіб прихову-

вання інформаційного мовної інформації, заснований на шифруванні мовної інформації, яка представлена у цифровій формі. При аналого-цифровому перетворенні амплітуда сигналу вимірюється через рівні проміжки часу, що називаються кроком дискретизації. Для того, щоб цифровий мовний сигнал мав якість не гіршу телефонного, крок дискретизації не повинен перевищувати 160 мкс, а кількість рівнів квантування амплітуди мовного сигналу — не менше 128. В цьому випадку відлік амплітуди кодується 7 бітами, швидкість передавання перевищує 43 кбіт/с, а ширина спектра дискретного двійкового сигналу дорівнює сумі смуг 14 стандартних телефонних каналів. Для передавання мови в цифровій формі стандартними телефонними каналами різко скорочують смугу мовного сигналу за допомогою пристроїв, які називають вокодерами. Шифрування мовної інформації у цифровій формі здійснюється відомими методами (заміною, перестановками, аналітичними перетвореннями, гамуванням і т. ін.) або за допомогою стандартних алгоритмів криптографічного перетворення. Перевагою ц. ш. м. і. є висока надійність закриття мовної інформації, так як перехоплений сигнал являє собою випадкову цифрову послідовність. Недоліком — необхідність використання модемів, нестійка робота пристроїв шифрування в каналах з великим загасанням сигналу і з високим рівнем завад.

Ш. необоротне /ш. необратимое/ [irreversible e.] — криптографічний процес, що полягає в детермінованому перетворенні даних до такого виду, що вихідні дані відновити неможливо, не дивлячись на точне знання методу шифрування. Такий підхід може використовуватися для захисту кодів паролів, що зберігаються в пам'яті. При цьому пароль, що пред'являється системі, спочатку кодується, а потім порівнюється із закодованим зразком. Таким чином несанкціонований доступ до таблиці паролів не дозволяє отримати доступ до самої системи.

Ш. потокове /ш. поточное/ [stream e.] — спосіб шифрування даних, при якому кожний знак шифрується незалежно.

ШЛЮЗ /шлюз/ [gateway] — апаратно-програмний засіб, що забезпечує з'єднання двох мереж з різними протоколами або середовищами передавання інформації. Ш. працюють на мережному або більш високих

рівнях. Так звані прикладні ш. (application g.) при пересиланні даних з однієї мережі в іншу виконують трансляцію протоколів. Наприклад поштовий ш. конвертує два різних протоколи пошти електронної. Іноді цей термін застосовують у ситуації, коли не потрібна трансляція протоколів, а дані просто пересилаються з однієї мережі в іншу. Ш. характеризується наявністю декількох адрес мережного рівня, наприклад, декількох IP-адрес. У IP-мережах роль шлюзу виконує маршрутизатор, що комутує канал мережі, до якого підключений персональний комп'ютер.

ШПИГУН /шпион/ [spy] — 1) Таємний агент, що займається шпіонажем. 2) Особа, що таємно слідкує за будь-ким, вистежує будь-кого.

Ш. мережний /ш. сетевой/ [network s.] — комбінований засіб зброї інформаційної, основою якого є черв'як мережний. Основні етапи функціонування ш. м.: інсталяція в пам'яті ПЕОМ, що атакується; очікування запиту з віддаленої атакуючої ПЕОМ і обмін з нею повідомленнями про готовність до атаки; передавання перехопленої інформації на атакуючі ПЕОМ і надання атакуючій ПЕОМ контролю над ПЕОМ, що атакується. Основні функції ш. м.: перехоплення і передавання інформації, що вводиться з клавіатури на атакуючу ПЕОМ (подолання системи захисту інформації, порушення конфіденційності інформації); перехоплення й передавання екранної інформації на атакуючу ПЕОМ (порушення конфіденційності інформації); перехоплення й передавання на атакуючу ПЕОМ інформації про ПЕОМ, що атакується, наприклад, про тип операційної системи, параметри ПЕОМ, програми, що виконуються (ведення розвідки комп'ютерної); передавання контролю над ПЕОМ, що атакується, атакуючому комп'ютерові. Результатом такого передавання можуть бути віддалений запуск програм, знищення або модифікація інформації та інші впливи деструктивні.

ШПІОНАЖ /шпионаж/ [espionage] (від нім. Spion — шпигун, яке походить від spähen — вистежувати) — передача, викрадення або збирання з метою передавання іноземній державі або її агентурі відомостей, що складають державну або воєнну таємницю, або відомостей, що складають службову або комерційну

таємницю підприємств (шпіонаж промисловий, шпіонаж технологічний).

Ш. комп'ютерний /ш. компьютерный/ [computer e.] — приєднання до комп'ютерів без відома власників з метою зняття або ушкодження даних, що містяться в них.

Ш. промисловий /ш. промышленный/ [industrial e.] — сукупність операцій таємних, які здійснюються корпораціями або державами у відношенні інших корпорацій або держав; наприклад, збирання інформації про конкурентів, викрадення патентної інформації і навіть акти саботажу у формі викривлення даних або послуг.

Ш. технологічний /ш. технологический/ [technological e.] — напрям діяльності розвідки з добування відомостей та інформації про технологічні процеси. Ефективний на короткочасних етапах розвитку економіки, так як високі темпи науково-технічного прогресу дозволяють швидку зміну технологій.

ШТАМП ЧАСУ /временной штамп/ [time stamp] — час створення або модифікації даних.

ШУМИ /шумы/ [noises] — 1) Звуки з неясно вираженою тональністю. 2) Випадкові завади в каналі зв'язку, які спотворюють повідомлення. Якість інформації, що одержують, залежить від завадозахищеності і завадостійкості засобів зв'язку, з однієї сторони, і від кількості нерелевантних даних, введених до складу повідомлення, з іншої сторони (шуму інформаційного).

Ш. інформаційні /ш. информационные/ [information n.] — 1) Див. шуми. 2) В комунікативістиці — різного роду трансляції та тексти (від зведень новин до рекламних кліпів), що здійснюють негативний вплив на вдачу та культуру суспільства. З ш. і. також пов'язують процеси наростання перевантажень комунікаційних.

ШУМОПЕЛЕНГУВАННЯ /шумопеленгация/ — виявлення та визначення координат плаваючих засобів за їхніми шумами. Інша назва — пасивна гідролокація.

Щ

ЩУП /щуп/ [probe] — назва різних приладів, за допомогою яких виявляють, зондують що-небудь.

Щ. міжмережний пакетний /щ. межсетевой пакетный/ [Packet Internet Groper (PING)] — утиліта, для тестування програмного забезпечення протоколу PCP/IP. Вона спрямовує сервера декілька пакетів, а потім оцінює час затримки відповіді і процентне співвідношення пакетів, що пройшли та загубилися. Утиліта здатна відображати буфер маршрутизації пакетів, які прибувають, що дозволяє виявляти проблеми задіяних мережних ресурсів, а також указувати розмір пакетів, їхньої кількість і тривалість паузи перед відправкою наступного пакета.

Я

ЯВКА /явка/ [secret address] — конспіративна зустріч; місце, приміщення, де відбувається або має відбутися така зустріч.

Я. запасна /я. запасная/ — заздалегідь обговорене місце таємної зустрічі, яке використовується в тому випадку, якщо у звичайному місці зустріч за будь-яких причин не відбулася.

Я. сліпа /я. слепая/ — зустріч співробітника розвідки з будь-ким (особливо з агентом) у той час і у тому місці, яке вказує останній. В таких випадках завжди є ризик того, що співробітник розвідки попаде у пастку або наразиться на спробу перевербування.

ЯДРО /ядро/ [kernel, nucleus] — 1) Резидентна частина керуючої програми, що завантажується у фіксовану область основної пам'яті і здійснює функції керування системою. 2) Загальна частина множини варіантів однієї й тієї ж мови.

Я. безпеки /я. безопасности/ [security k.] — компонента системи безпеки, яка інтегрує механізми захисту згідно з визначеною моделлю безпеки.

Я. важкооборотної функції /я. труднообратимой функции/ [hard-core predicate] — предикат $B : D \to /0,1/$ важкооборотної функції $f : D \to D$, такий, що для обчислення $B(x)$ для кожного $x \in D$ існує ефективний (алгоритм поліноміальний), а для обчислення $B(x)$ лише за відомим $f(x)$ для більшості

елементів $x \in D$ не існує ефективного (поліноміального) алгоритму.

Я. захисту /я. защиты/ [security k.] — частина комплексу засобів захисту, в якій зосереджений мінімально необхідний набір механізмів, що реалізують правила розмежування доступу.

ЯКІСТЬ /качество/ [quality, factor, Q-factor] — 1) Сукупність суттєвих ознак, властивостей, особливостей, що відрізняють предмет або явище від інших, та надають йому визначеність. 2) Те чи інше явище, ознака, що визначають позитивність будь-чого.

Я. відтворення сигналу /к. воспроизведения сигнала/ — показник радіоприймача, який оцінюється величиною спотворень сигналу, викликаних невідповідністю амплітудно-частотної і фазової характеристик, діапазону динамічного приймача поточним характеристикам сигналу. Спотворення можуть бути частотними, фазовими і нелінійними.

ЯЩИК /ящик/ [box] — вмістилище чого-небудь, як правило чотирикутної форми.

Я. білий /я. белый/ [white b.] — в техніці обчислювальній — програмний модуль, набір даних або пристрій, про внутрішню структуру і зміст яких існує часткова або повна інформація.

Я. поштовий /я. почтовый/ [mail b.] — в архітектурі відкритих систем — сукупність повідомлень і запитів на них, що зберігаються в пам'яті ЕОМ у вигляді черг.

Я. чорний /я. черный/ [black b.] — 1) В техніці обчислювальній — програмний модуль, набір даних або пристрій, інформація про внутрішню структуру і зміст яких відсутня повністю, але відомі специфікації вхідних і вихідних даних. 2) Секретний пристрій або обладнання, призначене для ведення розвідки радіоелектронної.

Література

1. Абдеев Р.Ф. Философия информационной цивилизации. — М.: ВЛАДОС, 1994. — 336 с.
2. Английский толковый словарь по кибернетике и прикладной математике. — М.: Издательство МГУ, 1986. — 184 с.
3. Анин Б., Петрович А. Радиошпионаж. — М,:“Международные отношения”, 1996. — 448 с.
4. Банкет В.Л. и др. Защита информации в системах телекоммуникации. — О.: Изд-во УГАС, 1997. — 95 с.
5. Бармен Скотт. Разработка правил информационной безопасности.: Пер. с англ. — М.: Издательский дом “Вильямс”, 2002. — 208 с.
6. Вакин С.А., Шустов Л.Н. Основы радиопротиводействия и радиотехнической разведки. М.: Сов. радио, 1968. — 272 с.
7. Вартанесян В.А. Радиоэлектронная разведка. — М.: Воениздат, 1991. — 254 с.
8. Вартанесян В. А., Гойхман Э. Ш., Рогаткин М. И. Радиопеленгация. — М.: Воениздат, 1966. — 248 с.
9. Введение в криптографию/Под общ. ред. В.В. Ященко. — 2-е изд., испр. — М.: МЦНМО: “ЧеРо”, 1999. — 272 с.
10. Вербіцький О.В. Вступ до криптології. — Л.: Видавництво науково-технічної літератури, 1998. — 247 с.
11. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия / Под ред. акад. Б. П. Смагоринского — М.: Право и Закон, 1996. — 182 с.
12. Виноградов А.Ф., Пешков А.Ф. Современные фотоаппараты — СПб.:BHV-Санкт-Петербург, 1998. — 256 с.
13. Гайкович В., Першин А. Безопасность электронных банковских систем. —М.: Единая Европа, 1994. — 364 с.
14. Ганенко О.Ю. Защита информации. Основи информационного управления. СПб.: Изд. дом “Сентябрь”, 2001. — 228 с.
15. Генне О.В. Мошенничество в сотовых сетях //Защита информации. Конфидент. — 2001. — N5. — С. 41–43.
16. Глазов Б.И. Способ классификации и моделирования информационных отношений сотрудничества и соперничества//Военная мысль. — 1998. N1. — С. 48–55.

17. Глазов Б.И., Ловцов Д.А. Информационная борьба как система отношений в информационной среде//Военная мысль. — 1997. — N5. — С. 36–41.

18. Горохов П.К. Информационная безопасность. Англо–русский словарь. — М.: Радио и связь, 1995.— 224 с.

19. ГОСТ 16325-76. Машины вычислительные электронные цифровые общего назначения. Общие технические требования. Приложение 2. Методика определения производительности ЭВМ общего назначения. — М.: Изд-во стандартов, 1976. — С. 14–28.

20. ГОСТ 28147-89. Государственный стандарт СССР. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования — М.: Изд–во официальное, 1989. — 26 С.

21. ГОСТ 34.310-95. Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. — К.:ГОССТАНДАРТ Украины, 1998. — 15 С.

22. ГОСТ 34.311-95. Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. Функция хэширования. — К.:ГОССТАНДАРТ Украины, 1998. — 10 С.

23. Грешневиков А.Н. Информационная война. — М.: Русскій міръ, Рыбинск: Рыбинское подворье, 1999. — 400 с.

24. Гринберг А.С., Горбачев Н.Н., Тепляков А.А. Защита информационных ресурсов государственного управления: Учеб. пособие для вузов. — М.: ЮНИТИ-ДАНА, 2003. — 327 с.

25. Гриняев С.Н. Интеллектуальное противодействие информационному оружию. Серия “Информатизация России на пороге XXI века”. — М.: СИНТЕГ, 1999. — 232 с.

26. Дежин Е.Н. Информационная война по взглядам китайских военных аналитиков//Военная мысль. — 1999. — N6. — С. 73—76.

27. Демин В.П., Куприянов А.И., Сахаров А.В. Радиоэлектронная разведка и радиомаскировка. — М.: Изд-во МАИ, 1997. — 156 с.

28. Драбкин А.Л., Зузенко В.Л., Кислов А.Г. Антенно-фидерные устройства. — М.: Советское радио, 1974. — 536 с.

29. ДСТУ 2226–93. Автоматизовані системи. Терміни та визначення.

30. ДСТУ 2860–94. Надійність техніки. Терміни та визначення.

31. ДСТУ 2462–94. Сертифікація. Основні поняття. Терміни та визначення.— К.: Держстандарт України, 1994. — 24 с.

32. ДСТУ 2874–94. Системи оброблення інформації. Бази даних. Терміни та визначення.

33. ДСТУ 2938–94. Системи оброблення інформації. Основні поняття. Терміни та визначення.

34. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.

35. Жаринов К.В. Терроризм и террористы/Под общ. ред. А.Е. Тараса. — Мн.: Харвест, 1999. — 606 с.

36. Защита от радиопомех/ Под ред. Максимова М.В. — М.: Сов. радио, 1976. — 496 с.

37. Защита программного обеспечения: Пер. с англ./Д. Гроувер, Р. Сатер, Дж. Фипс и др./Под ред. Д. Гроувера. — М.: Мир, 1992. — 286 с.

38. Зегжда Д.П., Ивашко А.М. Как построить защищенную информационную систему/Под научной редакцией Зегжды Д.П. и Платонова В.М. — СПб: Мир и семья-95, 1997 — 312 с.

39. Землянова Л.Д. Зарубежная коммуникативистика в преддверии информационного общества: Толковый словарь терминов и концепций. М.: — Изд-во Моск. ун-та, 1999. — 301 с.

40. Зима В.М., Молдовян А.А., Молдовян Н.А. Компьютерные сети и защита передаваемой информации. — Спб.: Изд-во Спб. ун-та, 1998. — 328 с.

41. Информатика: Энциклопедический словарь для начинающих / Сост. Д.А. Поспелов. — М.: Педагогика-Прес, 1994. — 352 с.

42. Информационная безопасность России и современные международные отношения. Швец Д.Ю. — М.: “Мир и безопасность”, 2001, — 176 с.

43. Кандыба В.М. Тайны психотронного оружия. — Спб.: Издательский Дом “Невский проспект”, 1998. — 414 с.

44. Карачун В.Я. та ін. Російсько-український словник з інформатики та обислювальної техніки (з показником українських термінів). — К.: “Рось”, 1994. — 361 с.

45. Клопов В.А., Мотуз О.В. Основы компьютерной стеганографии //Конфидент. — 1997. — N4. — С. 43–48.

46. Коваленко М.М. Комп’ютерні віруси і захист інформації. К.: Наукова думка, 1999. – 269 с.

47. Козирський В., Шендеровський В. Українсько–англійський–німецько–російський словник фізичної лексики. — К.: Видавництво “Рада”, 1996. — 934 с.

48. Комов С.А. Информационная борьба в современной войне: вопросы теории//Военная мысль. — 1996. — N3. — С. 76–80.

49. Комов С.А. О концепции информационной безопасности страны//Военная мысль. — 1994. — N4. — С. 12–17.

50. Комов С.А. О методологии оценки эффективности информационной борьбы//Военная мысль. — 1997. — N5. — С. 42–44.

51. Комов С.А. О способах и формах ведения информационной борьбы//Военная мысль. — 1997. — N4. — С. 18–22.

52. Комп’ютерний словник / Пер. з англ. В. О. Соловйова. – К.: Україна, 1997. – 470 с.

53. Конхейм А.Г. Основы криптографии / Пер. с англ. — М.: Мир, 1987. — 412 с.

54. Копылов В.А. Информационное право: Учебное пособие. — М.: Юристъ, 1997. — 472 с.

55. Коссак О., Кравець Р. Англо-український та українсько-англійський словник-довідник з телекомунікацій / Лінгв. ред. О. Микитюк. — Львів: СП "БаК", 1996. — 248 с.

56. Костин Н.А. Общие основы теории информационной борьбы//Военная мысль. — 1997. — N7. — С. 44–50.

57. Крысько В.Г. Секреты психологической войны (цели, задачи, методы, формы, опыт)/Под общ. ред. А.Е. Тараса. — Мн.: Харвест, 1999. — 448 с.

58. Кузьминов Т.В. Криптографические методы защиты информации. — Новосибирск: Наука. Сиб. предприятие РАН, 1998.—194 с.

59. Куликовский Л.М., Мотов В.В. Теоретические основы информационных процессов. — М.: Высшая школа, 1987. — 246 с.

60. Лисичкин В.А., Шелепин Л.А. Третья мировая (информационно-психологическая) война. — М.: Институт социально-психологических исследований АСН. — 1999.—304 с.

61. Лукашкин А.Н. Программные закладки в контексте угроз системам военного назначения //Защита информации. Конфидент. — 2003. — N1. — С. 88–95.

62. Мазуров В.А. Тайна: государственная, коммерческая, банковская, частной жизни. Уголовно-правовая защита: Учебное пособие / Под научн. рек. д-ра юрид. н., проф. С.В.Землюкова — М.: Издательско-торговая корпорация "Дашков и K^o", 2003. — 156 с.

63. Малашин М.С., Каминский Р.П., Борисов Ю.Б. Основы проектирования лазерных локационных систем. — М.: Высшая школа, 1983. — 207 с.

64. Математика. Большой энциклопедический словарь/ Гл.ред. Ю.В.Прохоров. — 3–е изд. — М.: Большая Российская энциклопедия, 1998. — 848 с.

65. Мафтик С. Механизмы защиты в сетях ЭВМ. — М.: Мир, 1993. — 216 с.

66. Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через INTERNET. Под научной редакцией проф. Зегжды П. Д. — СПб.: "Мир и семья–95", — 296 с.

67. Мелик-Гайказян И.В. Информационные процессы и реальность. — М.: Наука. Физматлит, 1998. — 192 с.

68. Мельников В.В. Защита информации в компьютерных системах. — М.: Финансы и статистика; Электроинформ, 1997. — 368 с.

69. Мелюхин И.С. Информационное общество: истоки, проблемы, тенденции развития. — М.: Изд-во Моск. ун-та, 1999. — 208 с. — (21 век: информация и общество).

70. Могилевский В.Д. Методология систем: вербальный подход/Отд-ние экон. РАН; науч.-ред. совет изд-ва “Экономика”. — М.: ОАО “Издательство “Экономика””, 1999. — 251 с. — (Системные проблемы России).

71. Моисеенков И. Основы безопасности компьютерных систем // Компьютер Пресс. — 1991. — N11. — С. 7–21.

72. Найк Д. Стандарты и протоколы Интернета/Пер. с англ. — М.: Издательский отдел “Русская Редакция” ТОО “Channel Trading Ltd.”, 1999. — 384 с.

73. Нанс Б., Компьютерные сети/Пер. с англ. — М.: БИНОМ, 1996. — 400 с.

74. НД ТЗІ 1.1–002–99. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу.

75. НД ТЗІ 1.1–003–99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.

76. НД ТЗІ 2.5–005–99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

77. Новий тлумачний словник української мови у чотирьох томах. — К.: Видавництво “Аконіт”, 1998.

78. Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений/Российская академия наук. Институт русского языка им. В. В. Виноградова. - 4–е изд., дополненное. — М.: Азбуковник, 1997. — 944 с.

79. Организация и современные методы защиты информации: Информационно-справочное пособие. — М.: 1996. — 370 с.

80. Палий А.И. Радиоэлектронная борьба: (Средства и способы подавления и защиты радиоэлектронных систем). — М.: Воениздат, 1981. — 320 с.

81. Першиков В.И., Савенков В.М. Толковый словарь по информатике. — 2–е изд., доп. — М.: Финансы и статистика, 1995. — 544 с.

82. Петраков А.В. Основы практической защиты информации. — М.: Радио и связь, 1999. — 368 с.

83. Петраков А.В., Лигутин В.С. Утечка и защита информации в телефонных каналах. 2–е изд., исправл. и доп. — М.: Энергоатомиздат, 1997. — 304 с.

84. Пирумов В.С., Родионов М.А. Некоторые аспекты информационной борьбы в военных конфликтах//Военная мысль. — 1997. — N7. — С. 45–49.

85. Плэтт В. Стратегическая разведка. Основные принципы. — М.: Издательский Дом “ФОРУМ”, 1997. — 376 с.

86. Пожидаев Д. Информационная война в планах Пентагона//Зарубежное военное обозрение. — 1996. — N2. С. 2–4.

87. Поздняков А.И. Информационная безопасность личности, общества, государства//Военная мысль. — 1993. — N10. — С. 13–18.

88. Политехнический словарь/Редкол.; А.Ю.Ишлинский (гл.ред) и др.— 3–е изд., перераб. и доп. — М.: “Большая Российская энциклопедия”, 1998. — 656 с.

89. Полмар Н., Аллен Т.Б. Энциклопедия шпионажа/Пер. с англ. В. Смирнова. — М.: КРОН-ПРЕСС, 1999. — 816 с. — Серия “Экспресс”.

90. Расторгуев С.П. Информационная война. — М.: Радио и связь, 1998. — 416 с.

91. Родионов М.А. К вопросу о формах ведения информационной борьбы//Военная мысль. — 1998. — N2. — С. 67–70.

92. Російсько-український математичний словник / Уклад.: В.Я. Карачун, О.О. Карачун, Г.Г. Гульчук. — К.: Вища шк., 1995. — 258 с.

93. Російсько-український словник наукової термінології: Математика. Фізика. Техніка. Науки про Землю і Космос / В.В. Гейченко, В.М. Завірюхіна, О.О. Зеленюк та ін. — К.: Наукова думка, 1998. — 892 с.

94. Секреты и ложь. Безопасность данных в цифровом мире / Б.Шнайер. — СПб.: Питер, 2003. — 368 с.

95. Слипченко В.И. Война будущего. — М.: Московский общественный научный фонд; ООО “Издательский центр научных и учебных программ”, 1999. — 92 с. — (Серия ”Научные доклады”, выпуск 88.)

96. Словарь по кибернетике / Под ред. В.М. Глушкова. — К.: Главная редакция УСЭ, 1979. — 624 с.

97. Словарь терминов “Безопасность компьютерных систем”//Конфидент. — 1994. — N1.— С. 93–106.

98. Словарь терминов “Безопасность компьютерных систем”//Конфидент. — 1995. — N5. — С. 101–106.

99. Словарь терминов “Безопасность компьютерных систем”//Конфидент. — 1995. — N6. — С. 85–88.

100. Словник іншомовних слів / За ред. О.С. Мельничука. — К.: Головна редакція УРЕ, 1974. — 776 с.

101. Справочник по основам радиолокационной техники /Под ред. В.В. Дружинина. — М.: Воениздат, 1967. — 768 с.

102. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Учеб. пособие. — М.: ИНФРА-М, 2001. — 304 с.

103. Стрелецкий А. Средства электронной войны сухопутных войск США// Зарубежное военное обозрение. — 1999. — N8. — С. 24—28.

104. Сяо Д., Керр Д., Медник С. Защита ЭВМ. — М.: Мир, 1982. —263 с.

105. Тайли Э. Безопасность персонального компьютера/Пер. с англ. — Мн.: ООО “Попурри”, 1997. — 480 с.

106. Теория и практика обеспечения информационной безопасности/Под ред. П.Д. Зегжды. — М.: Издательство Агентства “Яхтсмен”, 1996. — 192 с.

107. Толковый словарь по вычислительным системам под ред. В. Иллингуорта. —М.: Машиностроение, 1989. — 568 с.

108. Толковый словарь по основам информационной деятельности. — К.: УкрИНТЭИ, 1995. — 252 с.

109. Торокин А.А. Основы инженерно–технической защиты информации. — М.: Издательство "Ось–89", 1998. — 336 с.

110. Уолкер Б.Дж., Блейк Я.Ф. Безопасность ЭВМ и организация их защиты. —М.: Связь, 1980. — 142 с.

111. Физический энциклопедический словарь/ Гл. ред. А.М. Прохоров. — М.: Сов. энциклопедия, 1983. — 928 с.

112. Халипов В.Ф. Власть: Кратологический словарь. — М.: Республика, 1997. — 431 с.

113. Хорев А.А.Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Учебное пособие. М.: Гостехкомиссия России, 1998. — 320 с.

114. Хорошко В.О. та ін. Термінологічний довідник з питань технічного захисту інформації. — Київ, 1998. — 135 с.

115. Хоффман Л.Д. Современные методы защиты информации. — М.: Сов. радио, 1980. — 264 с.

116. Цыганков В.Д., Лопатин В.Н. Психотронное оружие и безопасность России. Серия "Информатизация Росии на пороге XXI века". — М.: СИНТЕГ, 1999. — 152 с.

117. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — М.: Изд-во ТРИУМФ,2002. — 816 с.

118. Экономическая разведка и контрразведка. Практическое пособие. — Новосибирск: 1994. — 414 с.

119. Энциклопедия кибернетики в 2-х том./ Отв. ред. В.М. Глушков. — К.: Гл.ред. Укр. сов. энциклопедии, 1974.

120. Энциклопедия промышленного шпионажа/Ю.Ф. Каторин, Е.В. Куренков, А.В. Лысов, А.Н. Остапенко/под общ. ред. Е.В. Куренкова.— С.-Петербург: ООО "Издательство Полигон", 1999. — 512.

121. Common Criteria for Information Technology Security Evaluation. National Institute of Standards and Technology & National Security Agency (USA), Communication Security Establishment (Canada), UK IT Security and Certification Scheme (United Kingdom), Bundesamt fur Sichereit in der Informationstechnik (Germany), Service Central de la Securite des Systemes (France), National Communications Security Agency (Netherlands). Version 2.1. August 1999.

122. Denning D.E. Cryptography and data security. — M.: Addison-Wesley, 1982. — 393 p.

123. Department of Defense Trusted computer system evaluation criteria, December 1985 (Orange Book).

124. Glossary of infosec and infosec related terms. — Information System Security Organization, IDAHO State University, August 1996,Volume 1,2.

125. Glossary of computer security terms. — NCSC-TG-004, 21 October, 1988.— 55 p.

126. International Organization for Standardization, ISO JTC1/CS27 N 1090, EPHOS: Security services, Project Document, April 1995.

127. International Standard ISO/IEC 7498, Information processing systems — Open Systems Interconnections — Basic Reference Models.

128. International Standard ISO/IEC 9594-8. Information technology —Open Systems Interconnections — The Directory — Part 8: Authentication framework. — First edition. — P. 12–15.

129. ISO 7498-2: 1989 Information processing systems. — Open Systems Interconnection. — Basic Reference Model. — Part 2: Security Architecture. — First edition. —15.02.1989. — 32 p.

130. International Standard ISO/IEC 2382-08, Information technology — Security techniques. — Vocabulary. — 16.07.1996. — 35 p.

131. International Standard ISO/IEC 11770-1. Information technology — Security techniques — Key management — Part1: framework. — 22 p.

132. National Institute of Standards and Technology (NIST). Publication XX: Announcement and Specification for a Digital Signature Standard (DSS). — 1992. — August 19.

133. T. Ritter Ritter's crypto glossary and dictionary of technical cryptography // online access through WWW: http://www.io.com, last update 20 may 1998.

134. Schneier B. Applied cryptography, second edition (Protocols,algorithms and source code in C). — J.WileySons Inc., 1996.

135. Trusted network interpretation environments guideline. — NCSC, August 1990. (Red Book)