В.А. Лужецький, О.П. Войтович,
А.В. Дудатьєв

Інформаційна безпека

Information Security and Data Protection

Education and Culture
Tempus

ІНФОРМАЦІЙНА БЕЗПЕКА

Навчальний посібник

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
VINNYTSIA NATIONAL TECHNICAL UNIVERSITY

V. A. Luzhetskyi, O. P. Voytovych, A. V. Dudatyev

INFORMATION SECURITY

Approved by the scientific council of Vinnytsia National Technical University as the text-book for students with the training direction 6.030601 – Management (organisations), 6.050100 – Banking, 6.030508 – Finances and Credit, 6.030502 – Economic Cybernetics, 6.030504 – Economy of Enterprise. Proceeding № 6 of 26 February 2009.

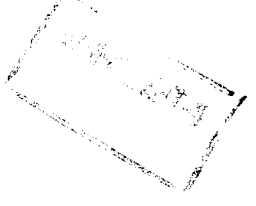
UNIVERSUM-Vinnytsia
2009

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

В.А. Лужецький, О.П. Войтович, А.В. Дудатьєв

ІНФОРМАЦІЙНА БЕЗПЕКА

Затверджено Вченою радою Вінницького національного технічного університету як навчальний посібник для студентів напрямів підготовки 6.030601 – Менеджмент (організацій), 6.050100 – Банківська справа, 6.030508 – Фінанси і кредит, 6.030502 – Економічна кібернетика, 6.030504 – Економіка підприємства. Протокол № 6 від 26 лютого 2009 р.



УНІВЕРСУМ-Вінниця
2009

УДК 658.012.8
Л 83

Рецензенти:
О. Д. Азаров, доктор технічних наук, професор
О. Є. Архипов, доктор технічних наук, професор
О. Г. Корченко, доктор технічних наук, професор

Рекомендовано до видання Вченою радою Вінницького національного технічного університету Міністерства освіти і науки України

V. A. Luzhetskyy, O. P. Voitovych, A. V. Dudatyev
Information Security. Textbook. –
UNIVERSUM-Vinnytsia, 2009. – 240 p.

The textbook considers the principal notions of Information security. There had been described the activities and means for legal, organizational, engineering and technical information protection at organizations and enterprises.

For students with training directions "Management", "Banking", "Financing and credit", "Economic Cybernetics", "Economy of the Enterprise" and for those interested in information security.

Лужецький В. А., Войтович О. П., Дудатьєв А. В.
Л 83 Інформаційна безпека : навчальний посібник. — Вінниця: УНІВЕРСУМ-Вінниця, 2009. — 240 с.
ISBN 978-966-641-297-6

У посібнику розглядаються основні поняття інформаційної безпеки. Описуються заходи та засоби правового, організаційного та інженерно-технічного захисту інформації в організаціях та підприємствах.

Для студентів напрямів підготовки «Менеджмент», «Банківська справа», «Фінанси і кредит», «Економічна кібернетика», «Економіка підприємства» та для всіх, хто цікавиться інформаційною безпекою.

УДК 658.012.8

ISBN 978-966-641-297-6

ЗМІСТ

CONTENTS

ПЕРЕДМОВА

Можна стверджувати, що на сучасному етапі розвитку людства відсутня полеміка щодо оцінки важливості інформації як такої. Ні в кого не виникає питань чи сумнівів з приводу її місця чи ролі. В постіндустріальному суспільстві матеріальні ресурси поступово втрачають свою вагомість, натомість цінність нематеріальних – інформаційних ресурсів зростає. Більше того, - сьогодні їм беззаперечно належить визначальна роль у суспільстві. Ми вже не живемо у світі машин, - ми живемо у світі ідей. Зрозуміло, що носієм і практичним реалізатором ідей є людина. Саме тому більш вагомим капіталом стає персонал підприємств і організацій. Часто втрата підприємством з якихось причин тандему працівник-інформація призводить не те що до проблем з роботою підприємства, а до ризику його існування взагалі.

Інформаційна ера внесла суттєві зміни у способи виконання обов'язків представниками значної кількості професій. Тепер середнього рівня фахівець з нетехнічною освітою може виконувати складні завдання, які раніше були під силу висококваліфікованому програмісту. Сьогодні співробітники різного формату підприємств мають у своєму розпорядженні стільки оперативної інформації, скільки ніколи не мали. А тому вони найбільш схильні до різних маніпуляцій з інформаційними масивами і тому саме вони повинні знати про свою відповідальність за їх втрату чи витоки за межі дозволеного.

Доступ до інформації більше не обмежується тільки вузьким колом осіб з вищого ешелону керівництва організацій. Число співробітників, що мають безпосередній доступ до комп'ютерного устаткування та інформаційних технологій, постійно зростає. Зрозуміло, чим більше користувачів отримує доступ до інформації, тим більша ймовірність виникнення можливостей для здійснення злочинів. Навмисні комп'ютерні злочини спричиняють значних збитків. Слід відмітити, що ще більших збитків підприємства зазнають від зловживань комп'ютерною технікою та помилок користувачів. А тому підприємства зобов'язані захищати свою інформацію від зовнішніх і внутрішніх загроз.

PREFACE

It is possible to assert that the modern stage of human development eliminates the disputes as for evaluation of information importance. No one questions its place or role. In the post industrial society in which the material resources gradually lose their value, the value of informational resources increases. More then that - informational resources play the determining role in the society. We do not live in the world of machines any more - we live in the world of ideas. It is clear that the man is the bearer and the practical realizer of the ideas. That is why the personnel of the enterprises and organizations becomes the most valuable capital. Very often it happens so that the loss of the tandem between the employee and information causes threat to the enterprise operation and sometimes questions its existence.

Information era made essential changes in the liabilities of different professions. The average employer with technical education may perform complicated assignments, which had previously been done by the skilled programmer. Today the stuff of different enterprises possesses large amount of on-line information. This makes it disposed to different manipulations with amounts of information and that is why they have to realize their own responsibility for its loss or drain.

Access to information is no more restricted to specific groups of people, representing the highest administration of the enterprise. Number of staff members with access to computer facilities and informational technologies is constantly increasing. It is quite obvious, that the more users get access to information, the higher is the opportunity for committing a crime. Purposeful computer crimes cause significant losses. It is necessary to note that the enterprises suffer greater losses caused by misusing computer facilities and users failures. That is why the enterprises have to protect their information against external and internal threats.

Будь-яке рішення приймається на основі наявної інформації та залежить від ступеню її достовірності. Витік закритої інформації може завдати серйозного удару будь-якій організації, її економічному стану, більше того - державі в цілому, її зовнішньополітичному іміджу, стратегічним планам на міжнародній арені тощо. Тому саме сьогодні необхідно приділяти належну увагу проблемам захисту інформації, у тому числі від несанкціонованого доступу, її цілісності та безпеки.

Основною причиною втрат чи витоку інформації, як мінімум, є недостатня освіченість користувачів у галузі інформаційної безпеки. Наявність відповідних знань ліквідує умови для виникнення інцидентів і помилок, забезпечить ефективне впровадження заходів і застосування засобів захисту інформації, сприятиме запобіганню інформаційним злочинам або вчасному виявленню підозрюваних у відповідних зловживаннях.

Якщо до недавно контроль за роботою комп'ютерних систем і мереж був турботою лише технічних та системних адміністраторів, то сьогодні він став обов'язком кожного, у тому числі нетехнічного користувача комп'ютерної техніки. Така ситуація вимагає поглиблення теоретичних знань та практичних навичок для груп нетехнічних працівників, перш за все тих, які займаються обробленням та аналізом економічної інформації.

Усвідомлюючи важливість проблем інформаційної безпеки і захисту даних, група українських фахівців підготувала міжнародний проект *JEP_27173_2006 "Information Security and Data Protection (Issues & Principles, Implementation & Management) – EU Experience in UA Universities"* за програмою ТЕМПУС Європейської Комісії.

Проект виконувався консорціумом університетів у складі технічного університету Дрездена (Німеччина) і університету Салєрно (Італія) з боку Європейського Союзу, Вінницького національного технічного університету, Одеського національного політехнічного університету та Інституту підприємництва і сучасних технологій (м. Житомир) з боку України.

В рамках виконання проекту авторами розроблений навчальний посібник *"Інформаційна безпека"*, який є першою спробою висвітлення питань з основ інформаційної безпеки для нетехнічної категорії користувачів.

Any decision is made on the basis of available information and depends on the level of its authenticity. Drain of closed information may cause serious impact to any organization, its economic state and to the state as a whole, its foreign policy image, strategic plans on international level etc. This encourages to pay adequate attention to the issues of information protection including that against an unauthorized access, its integrity and security.

The main reason for loss or drain of information is at the least the insufficient user's education in the sphere of information security. Availability of necessary knowledge eliminates conditions for incidents and errors, provides for efficient introduction of measures and using means for information protection, favors the prevention of information crimes or before-the-fact prevention of those suspected in the abuse of legal right.

The control over the operation of computer systems and nets has been previously the concern of technical and system administrators, but today it is becoming the responsibility of every user of computer facilities, including the non-technicians workers. Such a situation requires the profound theoretical knowledge and practical skills for non-technicians workers, firs of all for those, indulged in processing of economic information.

Realizing the importance of the problems of information security and data protection, the group of Ukrainian specialists have prepared the international project JEP_27173_2006 "Information Security and Data Protection (Issues & Principles, Implementation & Management) - EU Experience in UA Universities" following the European Commission program TEMPUS.

Project had been executed by the consortium of the Universities: on behalf of European Union - Technical University of Dresden (Germany), University of Salerno (Italy), and Vinnytsia National Technical University (VNTU), Odessa National Polytechnic University (ONPU), Institute of Business and Advanced Technologies (IBAT, the city of Zhytomyr) on behalf of Ukraine.

Within the frameworks of the project execution the authors developed the textbook "Information Security" which is the first attempt to highlight the issues on information security for non technical category of users.

Призначений для студентів економічних спеціальностей вищих навчальних закладів України.

Крім того, він може бути корисним викладачам економічних дисциплін, а також магістрантам, аспірантам і фахівцям, які працюють у галузі інформаційної безпеки та захисту даних.

Публікація навчального посібника була здійснена за фінансової підтримки Європейської Комісії в рамках проекту ТЕМПУС *JEP_27173_2006 "Information Security and Data Protection (Issues & Principles, Implementation & Management) – EU Experience in UA Universities"*

Навчальний посібник лише відображає погляди авторів.

Європейська Комісія не несе відповідальності за наведену в даному навчальному посібнику інформацію.

Віктор Мізерний,
координатор проекту,
проректор
Вінницького національного
технічного університету

Aimed at students of economic specialities in institutions for higher education of Ukraine.

It may also be useful for teachers of economic subjects, Master's degree students, post graduate students and specialists who work in the sphere of information security and data protection.

Printing and publishing of the textbook had been made with financial support of European Commission within the project *JEP_27173_2006 "Information Security and Data Protection (Issues & Principles, Implementation & Management) - EU Experience in UA Universities".*

The textbook reflects authors viewpoints.

European Commission is not responsible for the content of information presented in the issue.

Viktor Mizernyy,
project coordinator,
Vice Rector in
Vinnytsia National
Technical University

Що маємо – не зберігаємо,
втративши – плачемо.
К. Прутков

Сучасний світ розвивається у напрямку все більшої інформатизації як окремих галузей народного господарства, так і суспільства взагалі. Вже не можна собі уявити світ без інформаційних технологій, персональних комп'ютерів, глобальних комп'ютерних мереж та мобільного зв'язку, хоча ще 20 років тому це здавалось чимось фантастичним або дуже дорогим.

Донедавна тема захисту інформації була не для відкритої публікації та була доступна тільки фахівцям у цій галузі. І зараз там, де інформація з обмеженим доступом містить державні або військові секрети, все залишається як і раніше. Але з'явилося поняття комерційної таємниці або «інформації з обмеженим доступом, що носить конфіденційний характер».

Тому усе більше і більше людей усвідомлюють важливість безпеки інформації. Бізнесмен, економіст, юрист або лікар – у всіх них є свої особисті секрети, які ні під яким приводом вони не бажають розкривати. Тим більше, якщо справа стосується підприємств – компанії воліють приховувати й ретельно охороняти корпоративні секрети, розробки та інші конфіденційні матеріали. Отже, захист такої інформації – турбота самих підприємців, керівників банків, різних фірм і інших комерційних структур. Однак є фактом те, що багато бізнесменів, керівників комерційних структур, банків належним чином не приділяють цьому постійної уваги й починають турбуватися тільки тоді, коли вже виявлено витік інформації.

Необхідність вирішення проблем захисту інформації також зумовлена різким зростанням комп'ютерної злочинності, результат діяльності якої призводить до значних матеріальних втрат, незалежно від того чи це вірусна атака, чи шахрайство в області електронної комерції.

Дуже важливо правильно підійти до вирішення питань інформаційної безпеки, щоб не викидати «на вітер» гроші й, найважливіше, інформацію, яку було потрібно захистити. Існує таке поняття, як відношення ціна/якість, тобто людина (організація) повинна розуміти, інформацію якої вартості якою ціною вона збирається захищати. Нелогічно, якщо фінансові документи приблизної вартості X грн. будуть захищатися системою за 2X грн. Багаторічний досвід показує, що іноземні компанії вкладають до 20% своїх коштів в інформаційну безпеку свого підприємства.

INTRODUCTION

Modern world is developing in the direction of information increase in separate branches of economy and society in general. Modern world is difficult to imagine without the information technologies, personal computers, global computer nets and mobile connections, though 20 years ago it seemed to be fantasy or something very expensive.

Till recently the questions of information protection were not allowed for open issuing, available only to specialists in this sphere. Now the information with limited access which contains state or military secrets is treated as before. But there appeared the notion of commercial secret or "information with limited access which is of confidential character".

That is why more and more people realize the importance of information security. Businessman, economists, lawyers, doctor – all of them have private information which they wish to keep in secret. This becomes especially important when it comes to enterprises – the companies are willing to hide and guard corporate secrets, developments and other confidential materials. The security of such information is a concern of entrepreneurs, managers of banks, different firms and other commercial structures. The fact is however, that many businessmen, managers of commercial structures, banks, do not pay necessary and constant attention to this, starting to worry about it when the information drain – away takes place.

Necessity in solution of the problems related to information protection has also been stipulated for by an increase in computer delinquency, which results in significant material losses independent of whether this is a virus attack or swindle in the sphere of electronic commerce.

It is very important to choose the correct approach to the solution of problems of information security in order not to waste funds as well as information which had to be protected. There is the notion of relationship between price and quality, that is the person (organization) has to decide which information and at what cots has to be protected. It is not logical to protect the financial documentation of the approximate value X by the system of 2 X UHr in value. The experience shows that the foreign companies invest up to 20 % of their revenue to the information security of the enterprise.

Кожний комерційний об'єкт повинен будувати свою систему захисту інформації на концептуальній основі, виходячи із призначення об'єкта, його розмірів, умов розміщення, характеру діяльності й т.д. При розробці концепції захисту необхідно виходити з детального аналізу напрямків діяльності підприємницької структури й комплексних вимог захисту. Особливо, якщо структури застосовують у своїй діяльності засоби інформатики.

Основними напрямками забезпечення інформаційної безпеки бізнесу є:

- захист інформації про стан і рух матеріальних активів;
- захист інформації про стан нематеріальних активів і їх носіїв;
- захист засобів зберігання, оброблення й передавання інформації.

З огляду на різноманіття потенційних загроз інформації в системі обробки даних, складність структури й функцій, а також участь людини в технологічному процесі обробки інформації цілі захисту інформації можуть бути досягнуті тільки шляхом створення системи захисту інформації на основі комплексного підходу.

У посібнику розглядаються основні поняття інформаційної безпеки і концептуальні основи системи захисту інформації. Значну увагу приділено заходам та засобам законодавчого, адміністративного, організаційного та інженерно-технічного рівнів інформації. Наводяться відомості про українське та зарубіжне законодавство, основні стандарти щодо інформаційної безпеки. Для організаційного рівня описуються заходи, що стосуються роботи з персоналом, та організації служби безпеки підприємства чи установи, розглядаються правила побудови політики та програми безпеки. Для інженерно-технічного рівня описуються заходи та засоби фізичного, апаратного, програмного, криптографічного та стеганографічного видів захисту інформації та інформаційних ресурсів.

Наприкінці кожного розділу наведено контрольні питання, які призначені для перевірки студентами рівня засвоєння матеріалу в процесі самостійної роботи.

Each commercial unit has to build its information protection system on conceptual framework, proceeding from the unit target, its dimensions, layout conditions, character of activity etc. During the development of protection conception it is necessary to proceed from the detailed analysis of activities direction of entrepreneur structure and complex requirements to protection. Especially, when the units use information equipment in their activity.

Main directions in ensuring the information security are the following:

- protection of information on state and movement of material assets;
- protection of information on state of non material assets and their bearers;
- protection of storing devices, devices for processing and transference of information

Considering different potential threats to information in the system of data processing, complexity of structure and function as well as participation of a man in the technological process of information processing, the objectives of information protection may be reached only by creation of system for information protection on the base of complex approach.

The text book presents the consideration of principal notions of information security and conceptual framework of information protection system. Much attention has been paid to means and measures of legal, administrative, organizational, engineering and technical levels of information.

There had also been given information on Ukrainian and foreign legislation, main standards for the information security. For the organizational level there had been described the activities, concerning the work with personnel and organization of security service with the enterprise; there had been considered rules for building the security policy and program.

For engineering and technical level there had been described measures and means for physical, hardware, software, cryptographic, and steganographic kinds of protection of information and information resources. At the end of each part there are test questions, designed to check the level of comprehension of the material by students in the process of independent work.

У посібнику викладено методично опрацьований матеріал ряду літературних джерел, перелік яких наведено в кінці посібника. Методику викладення матеріалу апробовано під час читання лекцій і проведення практичних занять.

Автори висловлюють подяку рецензентам: доктору технічних наук, професору Азарову О. Д., доктору технічних наук, професору Архипову О. Є. та доктору технічних наук, професору Корченку О.Г. за корисні зауваження, що сприяли покращенню матеріалу посібника, а також провідному редактору Дружиніній В.О. за редагування тексту посібника.

Лужецький В. А.
Войтович О. П.
Дудатьєв А. В.

The textbook also describes methodically processed references, list of which is given at the end of the textbook. Methods for teaching this materials had been approbated during lectures and practical classes.

Authors are obliged to reviewers: Doctor of Technical Sciences, Professor O.D. Azarov, Doctor of Technical Sciences, Professor O.E. Arhypov and Doctor of Technical Sciences, Professor O.G. Korchenko for useful remarks which helped improve the textbook as well as chief editor Druzhynina V.O. for textbook editing.

V.A.Luzhetskyi
O.P. Voytovych
A.V. Dudatyev

Віднайди всьому початок,
і ти багато зрозумієш.
К. Прутков

1.1 ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Перш ніж говорити про інформаційну безпеку необхідно визначитися з поняттям **"інформація"**. Це поняття сьогодні вживається дуже широко і різнобічно. Важко знайти таку галузь знань, де б воно не використовувалося. Повсякденно під час здійснення різних видів діяльності користуються таким поняттям:

Інформація – це нові дані про людей, предмети, факти, події, явища і процеси незалежно від форми їхнього представлення.

У галузі інформаційних систем рекомендується таке означення інформації:

Інформація – це відомості, які є об'єктом зберігання, передавання і оброблення.

Відомо, що інформація може мати різну форму, зокрема, дані в комп'ютерах, листи, пам'ятні записи, досьє, формули, креслення, діаграми, моделі продукції, дисертації, судові документи й ін.

Відповідно до різноманітності поняття інформації, словосполучення "інформаційна безпека" в різних контекстах може мати різний сенс. Так, у Законі України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" наводиться таке поняття інформаційної безпеки:

Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Спеціальне законодавство в галузі безпеки інформаційної діяльності представлено низкою законів. У їхньому складі особливе місце належить базовому Закону "Про інформацію, інформатизацію і захист інформації", що закладає основи правового визначення всіх найважливіших компонентів інформаційної діяльності:

- інформації й інформаційних систем;
- суб'єктів – учасників інформаційних процесів;
- правовідносин виробників – споживачів інформаційної продукції;
- власників інформації – обробників і споживачів на основі відносин власності при забезпеченні гарантій інтересів громадян і держави.

У даному посібнику увагу буде зосереджено на процесах зберігання, оброблення і передавання інформації. Тому термін "інформаційна безпека" використовуватиметься у вузькому сенсі, як це прийнято, наприклад, в англомовній літературі.

Інформаційна безпека (ІБ) – це стан захищеності інформації від випадкових або навмисних дій природного або штучного характеру, які можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, зокрема, власникам і користувачам інформації.

Таким чином, правильний з методологічної точки зору підхід до проблем ІБ починається з виявлення суб'єктів інформаційних відносин та інтересів цих суб'єктів, пов'язаних з використанням **інформаційних систем (ІС)**. Загрози інформаційній безпеці – це зворотна сторона використання інформаційних технологій.

Тут необхідно зауважити, що трактування проблем, пов'язаних з інформаційною безпекою, для різних категорій суб'єктів може істотно різнитися. Для ілюстрації досить зіставити режимні державні організації і навчальні заклади. У першому випадку "хай краще все зламається, ніж ворог дізнається хоч один секретний біт", у другому – "немає у нас жодних секретів, аби все працювало". Отже, інформаційна безпека не зводиться виключно до захисту від несанкціонованого доступу до інформації, це поняття принципово ширше.

Фахівцем з інформаційної безпеки, як і знавцем футболу, вважає себе кожен другий користувач (не рахуючи кожного першого).

"Закони Мерфі для інформаційної безпеки" А.В. Лукацький

Суб'єкт інформаційних відносин може постраждати (зазнати збитки та/або одержати моральний збиток) не тільки від несанкціонованого доступу, але й від поломки системи, що викликала перерву в роботі. Більш того, для багатьох відкритих організацій власне захист від несанкціонованого доступу до інформації стоїть за важливістю зовсім не на першому місці.

Повертаючись до питань термінології, відзначимо, що термін **"комп'ютерна безпека"** (як еквівалент або замінник ІБ) є дуже вузьким. Комп'ютери – тільки одна із складових інформаційних систем, і хоч наша увага буде зосереджена в першу чергу на інформації, яка зберігається, обробляється і передається за допомогою комп'ютерів, її безпека визначається всією сукупністю складових і, в першу чергу, найслабкішою ланкою, якою в переважній більшості випадків виявляється людина.

Згідно з визначенням інформаційної безпеки, вона залежить не тільки від комп'ютерів, але й від інфраструктури, що її підтримує, до якої можна віднести системи електро-, водо- і теплопостачання, кондиціонери, засоби комунікацій і, звичайно, обслуговуючий персонал. Ця інфраструктура має самостійну цінність, але нас цікавитиме лише те, як вона впливає на виконання інформаційною системою своїх функцій.

Звернемо увагу, що у визначенні ІБ перед іменником "втрати" знаходиться прикметник "неприйнятний". Очевидно, застрахуватися від усіх видів втрат неможливо, тим більше неможливо зробити це економічно доцільним способом, коли вартість захисних засобів і заходів не перевищує розмір очікуваних втрат. Значить, з чимось доводиться миритися і захищатися слід тільки від того, з чим змиритися ніяк не можна. Іноді такими неприпустимими витратами є нанесення шкоди здоров'ю людей або стану навколишнього середовища, але частіше поріг неприйнятності має матеріальний (грошовий) вираз, а метою захисту інформації стає зменшення розмірів втрат до припустимих значень.

1.2 ОСНОВНІ ЗАДАЧІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Інформаційна безпека – це багатогранна галузь діяльності, в якій успіх може принести тільки систематичний, комплексний підхід.

Основними задачами інформаційної безпеки є:

- забезпечення доступності інформації;
- забезпечення цілісності інформації;
- забезпечення конфіденційності інформації;
- забезпечення вірогідності інформації;
- забезпечення юридичної значимості інформації, представленої у вигляді електронного документа;
- забезпечення невідстежуваності дій користувача.

Доступність – це властивість інформаційного об'єкта щодо одержання його користувачем за прийнятний час.

Інформаційні системи створюються для отримання певних інформаційних послуг. Якщо з тих чи інших причин надати ці послуги користувачам стає неможливо, це, очевидно, завдає збитку всім суб'єктам інформаційних відносин. Тому, не протиставляючи доступність решті аспектів, ми виділяємо її як найважливіший елемент інформаційної безпеки.

Особливо яскраво основна роль доступності виявляється в різного роду системах управління виробництвом, транспортом тощо. Зовні менш драматичні, але також вельми неприємні наслідки – і матеріальні, і моральні – може мати тривала недоступність інформаційних послуг, якими користується велика кількість людей (продаж залізничних та авіаквитків, банківські послуги тощо).

Хвилинна зупинка Лондонської фондової біржі через внутрішні неполадки інформаційної системи призвела до багатомільйонних втрат. cnews.ru

Цілісність – це властивість інформаційного об'єкта зберігати свою структуру і/або зміст у процесі передавання і зберігання.

Розрізняють цілісність *статичну* (тобто незмінність інформаційних об'єктів) і *динамічну* (стосується коректного виконання складних дій (транзакцій). Засоби контролю динамічної цілісності застосовуються, зокрема, при аналізі потоку фінансових повідомлень з метою виявлення крадіжки, переупорядковування або дублювання окремих повідомлень.

Міністерство оборони Великобританії веде розслідування з приводу порушення безпеки. Газета The Times пише, що всі повідомлення електронної пошти з ряду баз британських військово-повітряних сил потрапляють на російський сервер.

Inopressa.ru

Цілісність є найважливішим аспектом ІБ в тих випадках, коли інформація служить "керівництвом до дії". Рецептура ліків, зміст медичних процедур, набір і характеристики комплектуючих виробів, хід технологічного процесу – все це приклади інформації, порушення цілісності якої може призвести до небажаних наслідків. Неприємно і спотворення офіційної інформації, будь то текст закону або сторінка Web-сервера якої-небудь урядової організації.

Конфіденційність – це властивість інформації бути доступною тільки обмеженому колу користувачів інформаційної системи, в якій циркулює дана інформація.

Конфіденційність – найбільш опрацьований у нашій країні аспект інформаційної безпеки. На жаль, практична реалізація заходів щодо забезпечення конфіденційності сучасних інформаційних систем пов'язана із серйозними труднощами. По-перше, відомості про технічні канали витоку інформації є закритими, тому більшість користувачів позбавлено можливості мати

уявлення про потенційні ризики. По-друге, на шляху призначеної для користувача криптографії, як основного засобу забезпечення конфіденційності, стоять численні законодавчі перепони і технічні проблеми.

Вірогідність – це властивість інформації, яка полягає у строгій приналежності об'єкту, що є її джерелом, або тому об'єкту, від якого ця інформація прийнята.

Юридична значимість – це властивість інформації, представленої у вигляді електронного документа, мати юридичну силу.

З цією метою суб'єкти, що мають потребу в підтвердженні юридичної значимості переданого повідомлення, домовляються про прийняття деяких атрибутів інформації, що описують її здатність бути юридично значимою. Дана властивість інформації особливо актуальна в системах електронних платежів, де здійснюється операція з пересилання коштів.

Невідстежуваність – це здатність користувача робити деякі дії в інформаційній системі непомітно для інших об'єктів.

Актуальність даної вимоги виникла завдяки появі таких понять, як електронні гроші й Internet-banking. Так, для авторизації доступу до електронної платіжної системи користувач повинен надати деякі відомості, що однозначно його ідентифікують. У процесі розвитку даних систем може з'явитися реальна небезпека, що, наприклад, усі платіжні операції будуть контролюватися, тим самим виникнуть умови для тотального стеження за користувачами інформаційних систем.

Наприкінці 2007 року більш ніж 13 тис. користувачів соціальної мережі Facebook заявили про своє незадоволення новою рекламною моделлю цієї мережі. Їх занепокоїв той факт, що завдяки цільовій рекламі інформація про їхні покупки стала відомою їхнім друзям.
http://telnews.ru

Існує кілька шляхів вирішення проблеми неможливості стеження:

- заборона за допомогою законодавчих актів будь-якого тотального стеження за користувачами інформаційних систем;
- застосування криптографічних методів для підтримки неможливості стеження.

Інформаційна безпека може розглядатися не тільки стосовно деяких конфіденційних відомостей, але і стосовно здатності інформаційної системи виконувати задані функції.

Інформаційна безпека в рамках забезпечення працездатності ІС **повинна забезпечувати захист від:**

- порушення функціонування інформаційної системи шляхом впливу на інформаційні канали, канали сигналізації, керування і віддаленого завантаження баз даних, комутаційного устаткування, системне і прикладне програмне забезпечення;
- несанкціонованого доступу до інформаційних ресурсів і від намагань використання ресурсів мережі, що призводять до витоку даних, порушення цілісності мережі й інформації, зміни функціонування підсистем розподілу інформації, доступності баз даних;
- руйнування засобів захисту, що вбудовуються, і зовнішніх засобів;
- неправомірних дій користувачів і обслуговуючого персоналу мережі.

Пріоритети серед перерахованих задач інформаційної безпеки визначаються індивідуально для кожної конкретної ІС і залежать від вимог, що висуваються безпосередньо до інформаційних систем.

Якщо повернутися до аналізу інтересів різних категорій суб'єктів інформаційних відносин, то майже для всіх, хто реально використовує ІС, на першому місці стоїть доступність. Практично не поступається їй за важливістю цілісність – який сенс в інформаційній послузі, якщо вона містить спотворені відомості?

З погляду державних структур захисні заходи в першу чергу покликані забезпечити *конфіденційність, цілісність і доступність інформації.*

Комерційним структурам, ймовірно, важливіше всього *цілісність і доступність* даних і послуг. На відміну від державних, комерційні організа-

ції більш відкриті і динамічні, тому ймовірні загрози для них відрізняються не тільки кількістю, але і якістю.

Для розв'язання задач забезпечення безпеки в інформаційних системах необхідно:

- захистити інформацію під час її зберігання, оброблення і передавання мережею;
- підтвердити дійсність об'єктів даних і користувачів (автентифікація сторін, що встановлюють зв'язок);
- знайти і попередити порушення цілісності об'єктів даних;
- захистити технічні пристрої і приміщення;
- захистити конфіденційну інформацію від витоку і від вбудованих електронних пристроїв знімання інформації;
- захистити програмні засоби від під'єднання програмних закладок і вірусів;
- захистити від несанкціонованого доступу до інформаційного ресурсу і технічних засобів мережі, зокрема, до засобів керування, щоб запобігти зниженню рівня захищеності інформації і самої мережі в цілому;
- організувати заходи, що спрямовані на забезпечення збереження конфіденційних даних.

Конкретна реалізація загальних принципів забезпечення інформаційної безпеки може полягати в організаційних або технічних заходах захисту інформації.

1.3 ВАЖЛИВІСТЬ І СКЛАДНІСТЬ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Інформаційна безпека є одним з найважливіших аспектів інтегральної безпеки, на якому б рівні ми не розглядали останню – національному, галузевому, корпоративному або персональному.

Для ілюстрації цього положення наведемо кілька прикладів.

- З'явилася інформація про те, що планується терористична атака на Нью-Йоркську біржу. Ціллю терористів є комп'ютерні системи, що зберігають і працюють з інформацією про торгові операції в США та Європі. Наслідки такої операції можуть призвести до кризи світового масштабу. (З інтерв'ю з М. Дюре, директором Центру інформації та документації НАТО в Україні).

- Американський ракетний крейсер "Йорктаун" був змушений повернутися в порт через численні проблеми з програмним забезпеченням, що функціонувало на платформі Windows NT. Таким виявився побічний ефект програми ВМФ США з максимально широкого використання комерційного програмного забезпечення з метою зниження вартості військової техніки.

- У лютому 2001 року двоє колишніх співробітників компанії Commerce One, скориставшись паролем адміністратора, видалили з сервера файли, що складали крупний (на декілька мільйонів доларів) проект для іноземного замовника. На щастя, була резервна копія проекту, тому реальні втрати обмежилися витратами на слідство і засоби захисту від подібних інцидентів в майбутньому. У серпні 2002 року злочинці постали перед судом.

- Британський спеціаліст з інформаційних технологій Максвелл Парсонс отримав 2,5 року ув'язнення за злам банкоматів за допомогою MP3-плеєра і спеціального програмного забезпечення. Таким чином він отримував конфіденційну інформацію про банківські рахунки клієнтів для клонування кредитних карток.

- Американські військові оголосили про створення Командного центру кіберпростору ВВС США (U.S. Air Force Cyberspace Command) для захисту країни від онлайнових загроз з Інтернету.

- Невідомі "жартівники" скористалися принципами роботи онлайнової енциклопедії Wikipedia для розповсюдження шкідливого програмного забезпечення – нової модифікації вірусу Blaster.

- Одна студентка втратила стипендію в 18 тисяч доларів в Мічиганському університеті через те, що її сусідка по кімнаті скористалася їх загальним системним входом і відправила від імені своєї жертви електронний лист з відмовою від стипендії.

При аналізі проблематики, пов'язаної з інформаційною безпекою, необхідно зважати на специфіку даного аспекту безпеки, яка полягає в тому, що ІБ є складовою частиною інформаційних технологій, – галузі, що розвивається безпрецедентно високими темпами.

На жаль, сучасна технологія програмування не дозволяє створювати безпомилкові програми, що не сприяє швидкому розвитку засобів забезпечення ІБ. Слід виходити з того, що необхідно конструювати надійні системи ІБ із залученням ненадійних компонентів (програм). У принципі, це можли-

во, але вимагає дотримання певних архітектурних принципів і контролю стану захищеності протягом усього життєвого циклу ІС.

Наведемо ще декілька цифр.

% У березні 1999 року був опублікований черговий, четвертий річний звіт «Комп'ютерна злочинність і безпека-1999: проблеми і тенденції» (Issues and Trends: 1999 CSI/FBI Computer Crime and Security Survey). У звіті наголошувалося на різкому зростанні кількості звернень у правоохоронні органи з приводу комп'ютерних злочинів (32% з кількості опитаних); 30% респондентів повідомили про те, що їх інформаційні системи були зламані зовнішніми зловмисниками; атакам через Internet піддавалися 57% опитаних; у 55% випадках наголошувалося про порушення з боку власних співробітників. Примітно, що на питання "чи були зламані ваші Web-сервери і системи електронної комерції за останні 12 місяців? " 33% респондентів відповіли "не знаю".

% У аналогічному звіті, опублікованому в квітні 2002 року, цифри змінилися, але тенденція залишилася такою самою: 90% респондентів (переважно з крупних компаній і урядових структур) повідомили, що за останні 12 місяців в їх організаціях мали місце порушення інформаційної безпеки; 80% респондентів констатували фінансові втрати від цих порушень; 44% (223 респонденти) змогли та/або захотіли оцінити втрати кількісно (загальна сума склала більше 455 млн. доларів). Найбільшого збитку завдали крадіжки і фальсифікації (більше 170 і 115 млн. доларів відповідно).

Збільшення кількості атак – це не найбільша неприємність. Гірше те, що постійно виявляються нові вразливі місця в програмному забезпеченні і, як наслідок, з'являються нові види атак.

У таких умовах системи ІБ повинні мати можливість протистояти різноманітним атакам, як зовнішнім, так і внутрішнім, атакам автоматизованим і скоординованим. Іноді напад триває частки секунди, а інколи пошук вразливих місць розтягується на години і підозріла активність практично непомітна. Метою зловмисників може бути порушення всіх складових ІБ – доступності, цілісності і конфіденційності.

1.4 ОСНОВНІ ПОЛОЖЕННЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

1.4.1 Поняття системи захисту інформації

Існуючий на теперішній час значний практичний досвід у сфері захисту інформації показує, що потрібна прозора і цілеспрямована організація процесу захисту інформаційних ресурсів. Причому в цьому повинні активно брати участь професійні фахівці, адміністрація, співробітники і користувачі, що і визначає підвищену значимість організаційної сторони питання.

Відповідно до цього захист будується на основі системного підходу до інформаційної безпеки.

Система захисту інформації – це організована сукупність спеціальних установ, засобів, методів і заходів, що забезпечують захист інформації від внутрішніх і зовнішніх загроз.

Досвід показує, що забезпечення безпеки інформації не може бути одноразовим актом. Це неперервний процес, який полягає в обґрунтуванні і реалізації найбільш раціональних методів, способів і шляхів удосконалення та розвитку системи захисту, неперервному контролі її стану, виявленні її вузьких і слабких місць, а також протиправних дій.

Безпека інформації може бути забезпечена лише при комплексному використанні всього арсеналу наявних засобів захисту в усіх структурних елементах виробничої системи і на всіх етапах технологічного циклу обробки інформації. Найбільший ефект досягається тоді, коли всі використовувані засоби, методи і заходи поєднуються в єдиний цілісний механізм – *систему захисту інформації* (СЗІ). При цьому функціонування системи повинно контролюватися, обновлятися і доповнюватися залежно від зміни зовнішніх і внутрішніх умов.

Ніяка СЗІ не може забезпечити необхідного рівня безпеки інформації без належної підготовки користувачів і дотримання ними всіх установлених правил, спрямованих на її захист.

1.4.2 Вимоги до захисту інформації

З позицій системного підходу до захисту інформації висуваються певні вимоги. Захист інформації повинен бути:

- **неперервним**. Ця вимога виникає з того, що зловмисники тільки і шукають можливість, як би обійти захист інформації, що цікавить їх;
- **плановим**. Планування здійснюється шляхом розробки кожною службою детальних планів захисту інформації у сфері її компетенції з урахуванням загальної мети підприємства (організації);

Довгий час оновлення Windows випускалися у кожний другий четвер місяця. Тому шкідливе програмне забезпечення запускалось кожну другу п'ятницю місяця, щоб до випуску оновлень заразити якомога більше комп'ютерних систем.

http://inatack.ru

- **цілеспрямованим**. Захищається тільки те, що повинно захищатися в інтересах конкретної мети, а не все підряд;
- **конкретним**. Захисту підлягають конкретні дані, що об'єктивно вимагають охорони, втрата яких може заподіяти організації певний збиток;
- **активним**. Захищати інформацію необхідно з достатнім ступенем наполегливості;
- **надійним**. Методи і форми захисту повинні надійно перекривати можливі шляхи неправомірного доступу до охоронюваних секретів, незалежно від форми їхнього представлення, мови вираження і виду фізичного носія, на якому вони закріплені;
- **універсальним**. Вважається, що залежно від виду каналу витоку або способу несанкціонованого доступу його необхідно перекривати, де б він не проявився, розумними і достатніми засобами, незалежно від характеру, форми і виду інформації;
- **комплексним**. Для захисту інформації повинні застосовуватися всі види і форми захисту в повному обсязі. Неприпустимо застосовувати лише окремі форми чи технічні засоби. Комплексний хара-

ктер захисту виникає з того, що захист – це специфічне явище, що є складною системою нерозривно взаємопов'язаних і взаємозалежних процесів, кожний з яких, у свою чергу, має безліч різних сторін, властивостей, тенденцій.

1.4.3 Вимоги до системи захисту інформації

Закордонний і вітчизняний досвід показує, що для забезпечення виконання багатогранних вимог безпеки система захисту інформації повинна задовольняти такі умови:

- охоплювати весь технологічний комплекс інформаційної діяльності;
- бути різноманітною за використовуваними засобами, багаторівневою з ієрархічною послідовністю доступу;
- бути відкритою для зміни і доповнення заходів забезпечення безпеки інформації;
- бути нестандартною, різноманітною. Вибираючи засоби захисту не можна розраховувати на непоінформованість зловмисників щодо її можливостей;
- бути простою для технічного обслуговування і зручною для експлуатації користувачами;
- бути надійною. Будь-які несправності технічних засобів є причиною появи неконтрольованих каналів витоку інформації;
- бути комплексною, мати цілісність, що означає, що жодна її частина не може бути вилучена без втрат для всієї системи.

До системи безпеки інформації висуваються також певні вимоги:

- чіткість визначення повноважень і прав користувачів на доступ до певних видів інформації;
- надання користувачу мінімальних повноважень, необхідних йому для виконання дорученої роботи;
- зведення до мінімуму кількості спільних для декількох користувачів засобів захисту;
- облік випадків і спроб несанкціонованого доступу до конфіденційної інформації;

- забезпечення оцінювання ступеня конфіденційної інформації;
- забезпечення контролю цілісності засобів захисту і негайне реагування на вихід їх з ладу.

1.4.4 Види забезпечення системи захисту інформації

Система захисту інформації як будь-яка система повинна мати певні види власного забезпечення, спираючись на які вона буде виконувати свою цільову функцію. Враховуючи це, СЗІ повинна мати:

- **правове забезпечення**. Сюди входять нормативні документи, положення, інструкції, посібники, вимоги яких є обов'язковими в рамках сфери їх дій;
- **організаційне забезпечення**. Мається на увазі, що реалізація захисту інформації здійснюється певними структурними одиницями – такими, як служба захисту документів; служба режиму, допуску, охорони; служба захисту інформації технічними засобами; інформаційно-аналітична діяльність і ін.;
- **апаратне забезпечення**. Передбачається широке використання технічних засобів як для захисту інформації, так і для забезпечення діяльності власне СЗІ;
- **інформаційне забезпечення**. Воно містить у собі відомості, дані, показники, параметри, які лежать в основі розв'язання задач, що забезпечують функціонування системи. Сюди можуть входити як показники доступу, обліку, зберігання, так і системи інформаційного забезпечення розрахункових задач різного характеру, пов'язаних з діяльністю служби забезпечення безпеки;
- **програмне забезпечення**. До нього належать різні інформаційні, облікові, статистичні і розрахункові програми, що забезпечують оцінювання наявності і небезпеки різних каналів витоку і шляхів несанкціонованого проникнення до джерел конфіденційної інформації;
- **математичне забезпечення**. Припускає використання математичних методів для різних розрахунків, пов'язаних з оцінюванням не-

безпеки технічних засобів зловмисників, зон і норм необхідного захисту;

- **лінгвістичне забезпечення**. Сукупність спеціальних мовних засобів спілкування фахівців і користувачів у сфері захисту інформації;
- **нормативно-методичне забезпечення**. Сюди входять норми і регламенти діяльності органів, служб, засобів, які реалізують функції захисту інформації, різного роду методики, що забезпечують діяльність користувачів при виконанні своєї роботи в умовах жорстких вимог захисту інформації.

Задовольнити сучасні вимоги до забезпечення безпеки підприємства може тільки система безпеки.

Система безпеки – це організована сукупність спеціальних установ, служб, засобів, методів і заходів, що забезпечують захист життєво важливих інтересів особистості, підприємства і держави від внутрішніх і зовнішніх загроз.

Як і будь-яка система, система інформаційної безпеки має свої мету, задачі, методи і засоби діяльності, що узгоджуються за місцем і часом, залежно від умов.

Система інформаційної безпеки ніколи не будується в строк і в межах кошторису (наслідок із закону Хеопса).

"Закони Мерфі для інформаційної безпеки" А.В. Лукацький

1.5 КОНЦЕПТУАЛЬНА МОДЕЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

На рисунку 1.1 наведено концептуальну модель безпеки інформації, яка має чотири основних складові. З одного боку, це інформація, що захищається, а з іншого – загрози цій інформації. Загрози реалізуються за допомогою певних способів доступу, але їм перешкоджає захист інформації.

Джерелами конфіденційної (секретної) інформації є:

- документи всіх видів, на будь-яких носіях (у тому числі всі види носіїв, використовуваних в обчислювальній техніці й техніці засобів зв'язку);

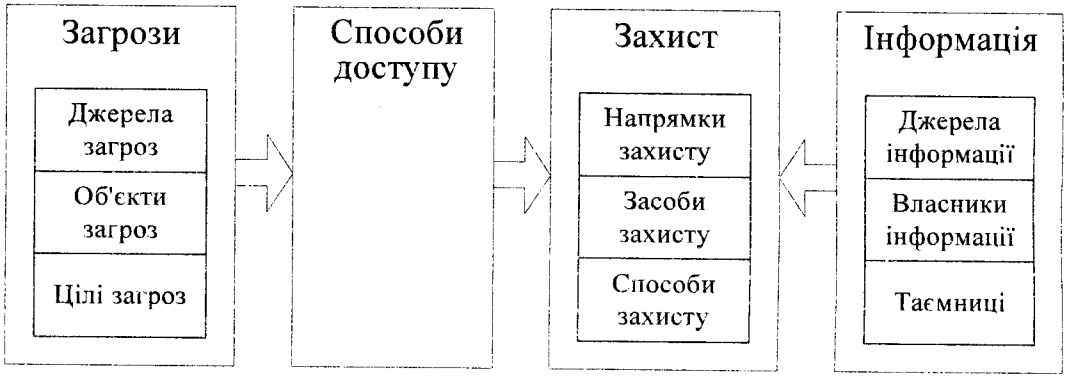


Рисунок 1.1 – Концептуальна модель безпеки інформації

- персонал (пам'ять людей), що володіє знаннями й кваліфікацією в різних галузях науки і техніки;
- організаційні одиниці - наукові, виробничі, управлінські й інші організації, що мають кадрові, технічні, виробничі, фінансові й інші можливості для вирішення певного кола проблем і завдань;
- промислові зразки (будь-які матеріальні об'єкти, створені в процесі виробництва), рецептури й технології, програмні засоби, які є результатом наукової й виробничої діяльності людей;
- науковий інструментарій (у тому числі автоматизовані системи наукових досліджень, автоматизовані робочі місця науковців і проектувальників, експертні системи і бази знань).

Можливі джерела інформації для прийняття рішень щодо забезпечення функціонування підприємства, організації, фірми та інформаційні потоки наведено на рис. 1.2.

Захищають і охороняють, як правило, не всю або не будь-яку інформацію, а найбільш важливу для власника, обмеження поширення якої приносить йому якусь користь або прибуток, можливість ефективно вирішувати завдання, що стоять перед ним.

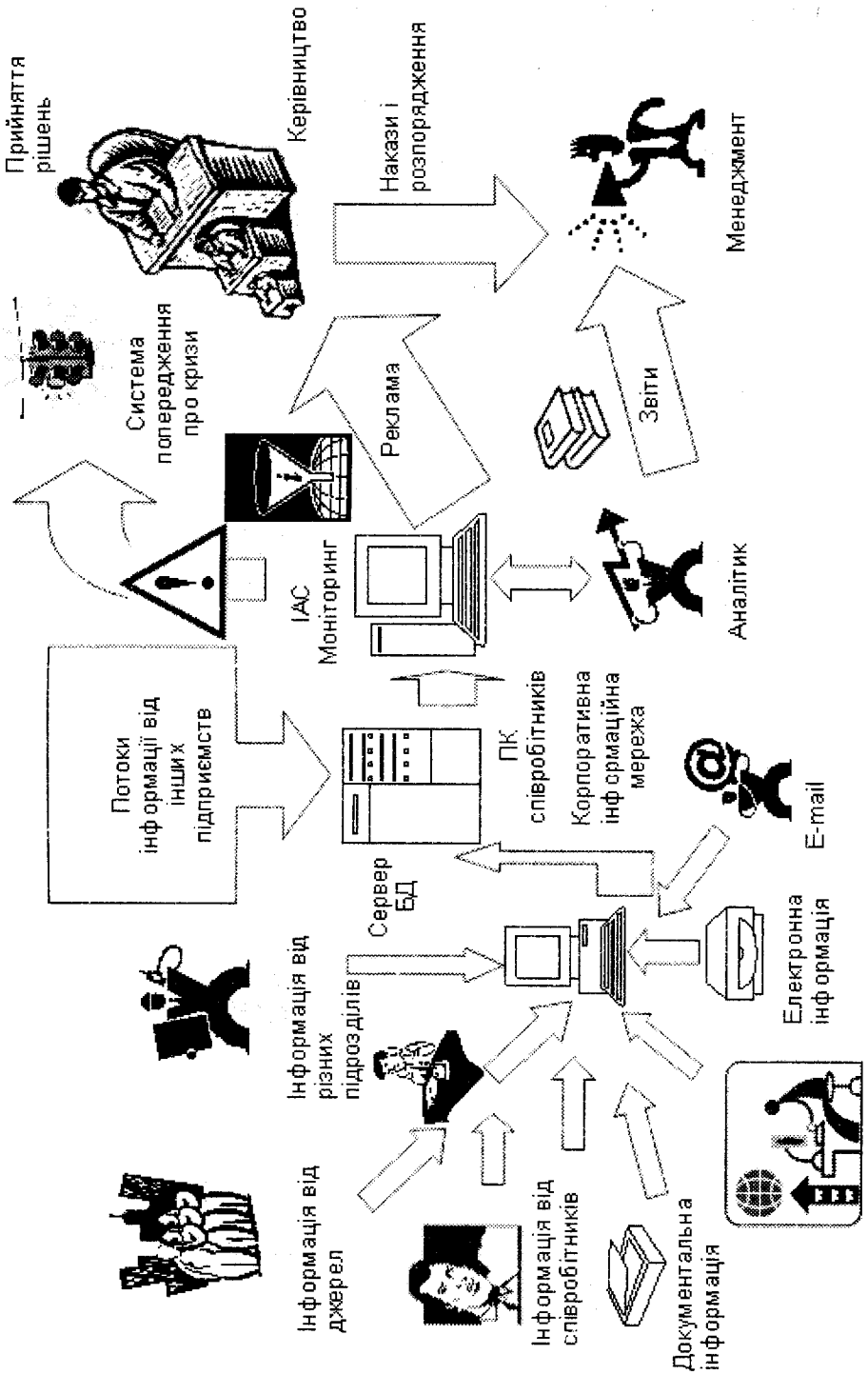


Рисунок 1.2 – Джерела інформації та інформаційні потоки

Власниками інформації, яку захищають, можуть бути:

- держава та її структури (органи);
- підприємства, товариства, акціонерні товариства (у тому числі спільні);
- громадські організації;
- громадяни.

Конфіденційна або секретна інформація поділяється на такі види:

- державна таємниця;
- комерційна таємниця;
- банківська таємниця;
- податкова таємниця;
- службова таємниця;
- професійна таємниця;
- персональні дані.

Засекречування інформації – це сукупність організаційно-правових заходів, регламентованих законами й іншими нормативними актами, щодо введення обмежень на поширення й використання інформації в інтересах її власника.

Основні принципи засекречування інформації.

1) Законність засекречування інформації. Полягає в здійсненні його строго в рамках чинних законів й інших підзаконних нормативних актів. Відступ від цього принципу може завдати серйозної шкоди інтересам захисту інформації, інтересам особистості, суспільства й держави, зокрема незаконним приховуванням від суспільства інформації, яка не вимагає засекречування, або витоку важливої інформації.

2) Обґрунтованість засекречування інформації. Полягає у встановленні шляхом експертної оцінки доцільності засекречування конкретних відомостей, імовірних економічних або інших наслідків цього акту, виходячи з балансу життєво важливих інтересів особистості, суспільства й держави. Невиправдано засекречувати інформацію, імовірність розкриття якої перевищує можливість збереження її в таємниці.

3) Своєчасність засекречування інформації. Полягає у встановленні обмежень на поширення цих відомостей з моменту їх одержання (розробки) або завчасно.

4) Підпорядкованість відомчих заходів щодо засекречування інформації загальнодержавним інтересам. Це в першу чергу стосується захисту державної таємниці. Що стосується комерційної таємниці, то підприємства наділені правами засекречування інформації, крім застережених у законі випадків.

Розсекречення конфіденційної й секретної інформації, робіт, документів, виробів – це діяльність підприємств стосовно зняття (часткового або повного) обмежень на доступ до раніше засекреченої інформації, на доступ до її носіїв, викликана вимогами законів і об'єктивних факторів: зміною міжнародної й внутрішньодержавної обстановки, появою більш досконалих видів певної техніки, зняттям виробів з виробництва, передачею (продажем) науково-технічних рішень оборонного характеру в народне господарство, продажем виробу за кордон і т.д., а також узяттям державою на себе міжнародних зобов'язань щодо відкритого обміну відомостями, які складають державну таємницю.

Інформація повинна залишатися секретною або конфіденційною доти, поки цього вимагають інтереси національної безпеки або конкурентної й комерційної діяльності підприємства.

Інформація розсекречується не пізніше строків, установлених при її засекречуванні.

Розсекреченню (розголошенню) не підлягають відомості, що стосуються особистого (неслужбового) життя громадян країни, якщо на інше немає згоди самих громадян, а у випадку їхньої смерті - їх найближчих родичів. Інший порядок такого розсекречення розглядається через суд.

Будь-яка фірма, займаючись своєю діяльністю, функціонує в деякому просторі (зовнішньому середовищі), і на її розвиток впливає ряд факторів (позитивних або негативних) як зовнішніх, так і внутрішніх. Негативні фактори часто називають факторами загроз або загрозами.

Джерелами зовнішніх загроз є:

- конкуренти;
- кримінальні структури;
- корумповані елементи держаних структур;
- природні катаклізми і техногенні катастрофи.

Внутрішні загрози створюють:

- засновники та вище керівництво;
- менеджери різних рівнів;
- персонал.

Об'єктами загроз є відомості про склад, стан і діяльність об'єкта захисту (персоналу, матеріальних і фінансових цінностей, інформаційних ресурсів).

Загрози інформації полягають у порушенні її цілісності, конфіденційності, повноти і доступності.

Джерела загроз мають на меті ознайомлення з відомостями, що охороняються, їх модифікацію в корисливих цілях і знищення для нанесення прямого матеріального збитку.

Одержати конфіденційну інформацію можна у такі способи:

- за рахунок її розголошення джерелами повідомлень;
- за рахунок витоку інформації через технічні засоби;
- за рахунок несанкціонованого доступу до повідомлень, що охороняються.

Основними напрямками захисту інформації є правовий, організаційний і інженерно-технічний захисти інформації як складові комплексного підходу до забезпечення інформаційної безпеки.

Захист інформації може бути здійснений за допомогою таких засобів:

- фізичних;
- апаратних;
- програмних;
- криптографічних;
- стеганографічних.

До **способів захисту** належать усілякі заходи, шляхи, способи і дії, що забезпечують попередження протиправних дій, їхнє запобігання, припи-

нення і протидію несанкціонованому доступу.

Концепція безпеки є основним правовим документом, що визначає захищеність підприємства від внутрішніх і зовнішніх загроз.

1.6 ЗАГРОЗИ БЕЗПЕЦІ ІНФОРМАЦІЇ

1.6.1 Джерела загроз

Знання можливих загроз, а також вразливих місць захисту, які звичайно використовують для здійснення загроз, необхідно для того, щоб вибрати найбільш економічні засоби забезпечення безпеки.

Протиправні дії з інформацією призводять до порушення її конфіденційності, цілісності і доступності, що, у свою чергу, призводить до порушення як режиму керування, так і його якості в умовах помилкової чи неповної інформації.

Загроза – це потенційна можливість певним чином порушити інформаційну безпеку.

Реалізація загрози спричиняє моральний чи матеріальний збиток, а захист і протидія загрозі покликані знизити його обсяг, в ідеалі – цілком, реально – значно чи хоча б частково. Але і це вдається далеко не завжди.

Спроба реалізації загрози називається *атакою*, а той, хто робить таку спробу, – *зловмисником (порушником)*.

З усіх атак відбудеться саме та, збиток від якої найбільший.

"Закони Мерфі для інформаційної безпеки" А.В. Лукацький

Побудова моделі зловмисника – це процес класифікації потенційних порушників за такими параметрами:

- тип зловмисника (конкурент, клієнт, розробник, співробітник компанії тощо);

- розташування зловмисника відносно об'єктів захисту (внутрішній, зовнішній);
- рівень знань про об'єкти захисту і оточення (високий, середній, низький);
- рівень можливостей доступу до об'єктів захисту (максимальні, середні, мінімальні);
- час дії (постійно, в певні часові інтервали);
- місце дії (передбачуване місце розташування зловмисника під час реалізації атаки).

Потенційні зловмисники називаються *джерелами загрози.*

Розглянемо джерела зовнішніх загроз.

Конкуренти

Фірми, що претендують на один сегмент ринку, зацікавлені в одному покупцеві, одному устаткуванні або одному приміщенні, стають конкурентами. Однією з основних ознак конкуренції є бажання, прагнення одної сторони вирішити свої завдання або задовольнити свої потреби за рахунок обмеження можливостей іншої сторони.

Конкуренція може бути чесною й несумлінною, явною й прихованою, дійсною й уявною (псевдо). Сумлінна, чесна конкуренція має на увазі цивілізовану боротьбу за покупця шляхом удосконалення продукту або технологій, підвищення якості послуг, зниження собівартості й т.п.

У тих випадках, коли конкурент використовує прийоми й методи несумлінної конкуренції, виникає реальна загроза для безпеки фірми, компанії, організації.

При аналізі потенційних і реальних можливостей фірми конкуренти серед інших факторів звертають увагу і на такі соціально-психологічні фактори:

- психологічний клімат на фірмі-конкуренті;
- специфіка кадрової політики;
- рівень виконавської дисципліни;
- творчий потенціал команди;
- стиль керівництва тощо.

Особлива увага звертається на наявність серед членів команди осіб, які незадоволені своїм становищем або взаєминами з колегами.

Збір інформації може здійснюватися як з відкритих джерел, так і оперативним шляхом. Для цього використовуються методи спостереження, опитування та вивідування. Об'єктами психологічного впливу в цьому випадку можуть стати ті співробітники фірми, які через свої психологічні якості і особистісні особливості легко піддаються чужому впливу. До цієї категорії належать особи, що:

- незадоволені своїм статусом або рівнем матеріального забезпечення;
- схильні до зловживання спиртними напоями або вживання наркотиків;
- мають дорогі хобі;
- люблять попліткувати;
- мають напружені стосунки з керівництвом або колегами;
- мають підвищену зарозумілість, честолюбство тощо.

Психологічною основою для вербування конкурентами джерела інформації серед співробітників фірми можуть стати:

- матеріальна залежність – співробітник, якого вербують, іде на контакт для того, щоб одержати гроші. Така основа використовується, якщо відомо, що співробітник має великі борги або пристрасть до азартних ігор або наркотиків;
- почуття помсти – наявність конфлікту з менеджерами або колегами, що заважає самореалізації або заняттю статусної позиції;
- залежність (шантаж) – використовується в тих випадках, коли є відомості, що компрометують співробітника в очах керівництва;
- страх (за себе або родичів) – коли представники кримінальних структур домагаються згоди на співробітництво, загрожуючи фізичною розправою.

У тих випадках, коли вербування за якихось обставин неможливе або недоцільне, використовуються методи прихованого одержання інформації. Для цього надсилаються персональні запрошення провідним співробітникам фірми для участі в конференціях, круглих столах, симпозіумах, для навчання на курсах підвищення кваліфікації тощо, де з ними працюють фахівці з вивідування.

В окремих випадках конкуренти, вступаючи у змову із представниками кримінальних структур, стають замовниками терористичних актів, роз-

бійних нападів, підпалів і погромів.

Кримінальні структури

У сучасних умовах будь-яка фірма тією чи іншою мірою зіштовхується із представниками кримінальних структур. В одних випадках це рекет, в інших – фірми-партнери та конкуренти, власниками яких є кримінальні співтовариства, а іноді – шахрайство, грабежі, розбійні напади, шантаж з боку організованих злочинних груп і злочинців-одинаків.

Найнебезпечнішою для фірм, компаній, організацій і одночасно найбільш доступною для вивчення є організована злочинність. Найменш доступні для вивчення злочинці-одинаки й випадкові злочинні групи.

Подібні структури самі виходять на контакти з комерційними фірмами. Основним мотивом взаємодії організованої злочинності з комерційними структурами є одержання грошей. Одні з них пропонують оплатити свої послуги із захисту підприємців від інших кримінальних структур і угруповань, інші – дозвіл працювати на контрольованій ними території.

Основними об'єктами злочинних зазіхань кримінальних елементів є матеріальні цінності, кошти і персонал.

Корумповані елементи контролюючих і державних структур, що займаються перевіркою

Особливе місце серед факторів зовнішньої загрози займають державні структури, що здійснюють перевірки і контроль. Самі по собі вони створені для контролю за діяльністю господарюючих суб'єктів на предмет порушення ними чинного законодавства. Однак довільне трактування їхніми співробітниками своїх прав і обов'язків може принести значну втрату фірмі. Співробітники державних контролюючих систем звикли виступати з позиції сили, що дає їм можливість, загрожуючи застосувати санкції та штрафи, змушувати бізнесмена шукати «компромісні» варіанти. З іншого боку, окремі з них виявляють прихильність до хабарів або «подарунків».

Техногенні катастрофи й природні катаклізми

Що стосується цього фактора загрози, то в першій своїй частині він у прихованій, а іноді й у явній формі нерідко містить людський фактор. Дійсно, аналіз причин катастроф свідчить про те, що серед них істотну роль гра-

ють помилкові дії операторів, неправильна експлуатація технічних засобів і просто недбалість. У ряді випадків людина сама довільно ініціює техногенні катастрофи. Подібні дії можуть бути кваліфіковані як шкідництво й навіть як терористичні акти.

Внутрішні загрози

Найчастішими і найнебезпечнішими (з погляду розміру втрат) є ненавмисні помилки штатних користувачів, операторів, системних адміністраторів і інших осіб, які обслуговують інформаційні системи.

Іноді такі помилки і є власне загрозами (неправильно введені дані або помилка в програмі, що викликала крах системи), іноді вони створюють вразливі місця, якими можуть скористатися зловмисники (звичайно такими є помилки адміністрування). За деякими даними, до 65% втрат – наслідок ненавмисних помилок.

Очевидно, найрадикальніший спосіб боротьби з ненавмисними помилками – максимальна автоматизація і суворий контроль.

Реальною загрозою існування фірми є не тільки фактори зовнішньої загрози, але й різного роду негативні процеси всередині неї.

Внутрішніми загрозами є:

- напруження, що виникають усередині команди через неправильні взаємини по вертикалі, горизонталі, незадоволеність результатами своєї праці і їх оцінкою з боку керівництва;
- нездорова конкуренція між окремими співробітниками або підрозділами;
- внутрірольові й міжролеві конфлікти;
- недостатня управлінська компетентність менеджерів різного рівня;
- низька професійна й особистісна надійність персоналу.

Відповідно до досліджень компанії Verizon, близько 18% всіх кіберзлочинів здійснюється саме інсайдерами (співробітниками). Причому збитки від дій штатних співробітників можуть бути колосальними, оскільки вони знають де шукати важливу інформацію і часто мають до неї доступ.

cnews.ru

Одним з головних суб'єктів загроз корпоративній безпеці фірми є засновники й перші особи в її керівництві. При відсутності або недостатній сформованості управлінських і лідерських якостей, слабкій поінформованості в питаннях забезпечення корпоративної безпеки, ігноруванні порад і рекомендацій фахівців з питань безпеки, при неадекватних реакціях на вимоги особистої охорони керівники самі стають фактором загрози для безпеки фірми, компанії, організації.

Найбільш типовими помилками в прийнятті управлінських рішень при забезпеченні необхідного й достатнього рівня безпеки є:

- неадекватна оцінка факторів зовнішніх й внутрішніх загроз;
- неадекватний вибір концепції організації системи безпеки;
- неадекватний рівень фінансування;
- неадекватна взаємодія з особистою охороною.

Адекватно фактори реальної й потенційної загрози можуть оцінити тільки фахівці. Тому менеджер з безпеки або керівники фірми повинні періодично консультуватися з цих питань із відповідними експертами.

Фінансування системи корпоративної безпеки розглядається більшістю керівників як непродуктивні витрати й здійснюється за залишковим принципом.

Існує група факторів загроз безпеці, що виникають як результат основної діяльності керівників і менеджерів всіх рівнів.

До них належать:

- відсутність або недостатня сформованість стратегічного мислення та цілепокладання;
- відсутність належного управлінського досвіду;
- невміння будувати свої відносини з бізнес-партнерами;
- наявність особистісних якостей, що утрудняють роботу як керівника.

Керівник великої компанії повинен бути здатним до стратегічного мислення та цілепокладання. Відсутність або недостатня розвиненість цих якостей істотно утрудняє роботу всіх управлінських систем, у тому числі й корпоративної безпеки.

Кожний менеджер компанії повинен мати необхідний рівень управлінської компетентності. Відсутність необхідного управлінського досвіду

призводить до прийняття помилкових рішень, падіння авторитету в очах підлеглих, порушення взаємин по вертикалі. Всі ці обставини істотно послабляють систему корпоративної безпеки.

При виконанні своїх функціональних обов'язків персоналу фірми, компанії, членам організації постійно доводиться вступати в особисті контакти з іншими співробітниками, клієнтами, партнерами по бізнесу, працювати з інформацією, виконувати окремі види робіт з використанням технічних і допоміжних засобів підвищеної небезпеки. При цьому будь-які несанкціоновані, помилкові, недоречні дії, порушення принципів ділового спілкування можуть стати реальним джерелом загрози для корпоративної безпеки.

Потрапивши під певний вплив, співробітники можуть стати для конкурентів або кримінальних структур джерелом відомостей, що містять комерційну таємницю, навіть не усвідомлюючи цього.

Таким чином, корпоративна безпека фірми залежить від надійності персоналу. Факторами, що визначають надійність персоналу з погляду психології, є:

- необхідний рівень професійної компетентності;
- висока виконавська дисципліна;
- стійка мотивація до діяльності в рамках даної фірми.

1.6.2 Загрози сучасним інформаційним системам

Загрози класифікуються за такими критеріями:

- **за аспектом інформаційної безпеки** (доступності, цілісності, конфіденційності), проти якого загрози спрямовані в першу чергу;
- **за компонентами інформаційних систем**, на які загрози націлені (дані, програми, апаратура, підтримувальна інфраструктура);
- **за способом здійснення** (випадкові/навмисні дії природного або техногенного характеру);
- за розташуванням джерела загрози (всередині/зовні ІС);
- **за обсягом збитку** (граничний, після якого фірма може стати банкрутом; значний, але не призводить до банкрутства; незначний, який фірма за якийсь час може компенсувати);

- **за ймовірністю виникнення** (дуже ймовірна загроза; ймовірна загроза; малоймовірна загроза);
- за характером нанесеного збитку (матеріальний; моральний).

1.6.3 Основні загрози доступності

Загрози доступності класифікуються за компонентами ІС, на які спрямовані загрози:

- відмова користувачів;
- внутрішня відмова інформаційної системи;
- відмова інфраструктури, що підтримує ІС.

Стосовно **користувачів** розглядаються такі загрози:

- небажання працювати з інформаційною системою (найчастіше виявляється, коли необхідно освоювати нові можливості і в разі розбіжності між запитами користувачів і фактичними можливостями та технічними характеристиками);
- неможливість працювати із системою через відсутність відповідної підготовки (недолік загальної комп'ютерної освіти, невміння інтерпретувати діагностичні повідомлення, невміння працювати з документацією і т.п.);
- неможливість працювати із системою через відсутність технічної підтримки (неповнота документації, нестача довідкової інформації тощо).

Основними джерелами внутрішніх відмов є:

- порушення (випадкове або навмисне) правил експлуатації;
- вихід системи зі штатного режиму експлуатації;
- помилки при (пере)конфігурації системи;
- відмови програмного і апаратного забезпечення.

Як засіб виведення системи зі штатного режиму експлуатації може використовуватися агресивне споживання ресурсів (звичайно – смуги пропускання мереж, обчислювальних можливостей процесорів або оперативної пам'яті). Для виведення систем з штатного режиму експлуатації можуть використовуватися вразливі місця у вигляді програмних і апаратних помилок.

Відома помилка в процесорі Pentium I дає можливість локальному користувачу шляхом виконання певної команди "підвісити" комп'ютер, так що допомагає тільки апаратний RESET.

Віддалене споживання ресурсів останнім часом спостерігається в особливо небезпечній формі – як скоординовані розподілені атаки, коли на сервер з безлічі різних адрес з максимальною швидкістю прямують цілком легальні запити на з'єднання та/або обслуговування.

Онлайнові казино мають значні збитки через відключення їх від мережі зловмисниками, які організовують DoS-атаки з вимогою плати за їх припинення. Сучасні міжмережеві екрани та захисні програми не спасають від розподілених нападів, коли десятки тисяч різних комп'ютерів-зомбі звертаються до сервера, порушуючи його роботу.

cnews.ru

Відмови програмного забезпечення часто провокуються впровадженням в ІС так званого шкідливого програмного забезпечення, дії якого спрямовані на:

- руйнування даних;
- руйнування або пошкодження апаратури (зокрема носіїв даних).

Стосовно інфраструктури рекомендується розглядати такі загрози:

- **порушення роботи (випадкове або навмисне) систем** зв'язку, електроживлення, водо- і/або теплопостачання, кондиціонування;
- **руйнування або пошкодження приміщень**;
- **неможливість або небажання обслуговуючого персоналу і/або користувачів виконувати свої обов'язки** (цивільні безлади, аварії на транспорті, терористичний акт або його загроза, страйк тощо).

1.6.4 Основні загрози цілісності

У більшості випадків винуватцями загроз цілісності є штатні співробітники організацій, добре знайомі з режимом роботи і заходами захисту. Це

ще раз підтверджує небезпеку внутрішніх загроз, хоча говорять і пишуть про них значно менше, ніж про зовнішні.

З метою порушення **цілісності** зловмисник (як правило, штатний співробітник) може:

- ввести неправильні дані;
- змінити дані;
- знищити дані.

Іноді змінюються змістовні дані, іноді – службова інформація.

З наведеного випадку можна зробити висновок не тільки про загрози порушення цілісності, а й про небезпеку сліпої довіри комп'ютерній інформації. Заголовки електронного листа можуть бути підроблені. Лист в цілому може бути фальсифікований особою, що знає пароль відправника. Відзначимо, що останнє можливо навіть тоді, коли цілісність контролюється криптографічними засобами. Тут має місце взаємодія різних аспектів інформаційної безпеки: якщо порушена конфіденційність, може постраждати цілісність.

Показовий випадок порушення цілісності мав місце в 1996 році. Співробітниця Oracle (особистий секретар віце-президента) подала судовий позов, звинувачуючи віце-президента корпорації в незаконному звільненні після того, як вона відкинула його залицяння. На доказ своєї правоти жінка надала електронний лист, нібито відправлений її начальником президенту, в якому було вказано час відправки. Віце-президент надав, у свою чергу, файл з реєстраційною інформацією компанії стільникового зв'язку, з якого випливало, що в указаний час він розмовляв по мобільному телефону, знаходячись далеко від свого робочого місця. Таким чином, в суді відбулося протистояння "файл проти файлу". Очевидно, один з них був фальсифікований або змінений, тобто було порушено його цілісність. Суд вирішив, що підроблювали електронний лист (секретарка знала пароль віце-президента, оскільки їй було доручено його змінювати), і позов був відхилений...

cnews.ru

Потенційно уразливі з погляду порушення цілісності не тільки дані, але і програми. Впровадження шкідливого програмного забезпечення – приклад подібного порушення.

Особливо вразливі до загроз порушення цілісності електронні магазини та їх бази даних, зміни в яких можуть призвести до значних втрат.

1.6.5 Основні загрози конфіденційності

У загальному випадку, конфіденційну інформацію можна поділити на **службову** та **предметну**.

Службова інформація (наприклад, паролі користувачів) не належить певній предметній галузі, в ІС вона грає технічну роль, але її розкриття особливо небезпечно, оскільки воно може забезпечити несанкціонований доступ до всієї інформації, зокрема предметної.

Навіть якщо інформація зберігається в комп'ютері або призначена для комп'ютерного використання, загрози її конфіденційності можуть носити некомп'ютерний і взагалі нетехнічний характер.

Багатьом людям доводиться бути користувачами не одного, а кількох інформаційних сервісів. Якщо для доступу до таких систем використовуються **багаторазові паролі** або інша конфіденційна інформація, то напевно ці дані зберігатимуться не тільки в голові, але і в записнику або на папері, які користувач часто залишає на робочому столі, а то і просто губить. І справа тут не в неорганізованості людей, а в початковій непридатності парольної схеми. Неможливо пам'ятати багато різних паролів. Рекомендації щодо їх регулярної зміни тільки погіршують стан, змушуючи застосовувати нескладні схеми чергування, або взагалі прагнути звести справу до паролів, що легко запам'ятовуються і вгадуються.

Описаний клас вразливих місць можна назвати **розміщенням конфіденційних даних у середовищі, де їм не забезпечено (часто – і не може бути забезпечено) необхідний захист**. Загроза ж полягає в тому, що хтось не відмовиться дізнатися секрети, які самі просяться в руки. Крім паролів, що зберігаються в записниках користувачів, до цього класу потрапляє передача конфіденційних даних у відкритому вигляді (у розмові, в листі, мережею), яка робить можливим перехоплення даних. Для атаки можуть використовуватися різні технічні засоби (підслуховування або прослуховування розмов, пасивне прослуховування мережі і т.п.), але ідея одна – здійснити доступ до даних у той час, коли вони найменше захищені.

Вельми небезпечною загрозою є **виставки**, на які багато організацій відправляють устаткування з виробничої мережі, з усіма збереженими на

них даними, залишаючи тим самим паролі. При віддаленому доступі вони продовжують передаватися у відкритому вигляді. Це погано навіть в межах захищеної мережі організації, а в об'єднаній мережі виставки – це дуже суворе випробування чесності всіх учасників.

Ще один приклад загрози, про яку часто забувають, – зберігання даних **на резервних носіях**. Для захисту даних на основних носіях застосовуються розвинені системи управління доступом, тоді як копії нерідко просто лежать у шафах і дістати доступ до них може багато хто.

Перехоплення даних – дуже серйозна загроза, і якщо конфіденційність дійсно є критичною, а дані передаються багатьма каналами, їх захист може виявитися достатньо складним і дорогим. Технічні засоби перехоплення доступні, прості в експлуатації, а встановити їх, наприклад на кабельну мережу, може хто завгодно, тому цю загрозу потрібно брати до уваги стосовно не тільки зовнішніх, а й внутрішніх комунікацій.

Крадіжки устаткування є загрозою не тільки для резервних носіїв, але і для комп'ютерів, особливо портативних. Часто ноутбуки залишають без нагляду на роботі або в автомобілі, іноді просто гублять.

У листопаді 2006 року виник скандал з викраденням трьох ноутбуків з персональними даними 15 тис. британських поліцейських у лондонську Скотланд Ярді. Викрадачів так і не знайшли.

cnews.ru

Небезпечною нетехнічною загрозою конфіденційності є методи **соціальної інженерії**, такі як маскарад – виконання дій під виглядом особи, що володіє повноваженнями для доступу до даних.

До неприємних загроз, від яких важко захищатися, можна віднести **зловживання повноваженнями**. На багатьох типах систем привілейований користувач (наприклад системний адміністратор) здатний прочитати будь-який (незашифрований) файл, дістати доступ до пошти будь-якого користувача і т.д.

Інший приклад – нанесення збитку при сервісному обслуговуванні. Звичайно сервісний інженер дістає необмежений доступ до устаткування і

має можливість діяти в обхід програмних захисних механізмів.

Такі основні загрози, які завдають найбільшого збитку суб'єктам інформаційних відносин.

1.6.6 Шкідливе програмне забезпечення

Одним з найнебезпечніших способів здійснення атак є впровадження в ІС шкідливого програмного забезпечення.

Шкідливе програмне забезпечення зазвичай призначено для:

- впровадження іншого шкідливого програмного забезпечення;
- отримання контролю над системою, що атакується;
- агресивного споживання ресурсів;
- зміни або руйнування програм та/або даних.

Розрізняють такі основні види шкідливого програмного забезпечення:

- **віруси** – коди, що мають здатність до розповсюдження (можливо, із змінами) шляхом впровадження в інші програми;
- **"хробаки"** – коди, здатні самостійно, тобто без упровадження в інші програми, викликати розповсюдження своїх копій в ІС і їх виконання (для активізації вірусу потрібен запуск зараженої програми);
- **троянські програми** – легальні програми, які мають незадокументовані функції, направлені, зазвичай, на перехоплення даних.

Віруси звичайно розповсюджуються локально, в межах вузла мережі; для передачі мережею їм потрібна зовнішня допомога, така як пересилання зараженого файлу. "Хробаки", навпаки, орієнтовані в першу чергу на подорожі мережею.

З усього шкідливого програмного забезпечення найбільшу увагу користувачі приділяють вірусам.

Дотримання нескладних правил "комп'ютерної гігієни" практично зводить ризик зараження до нуля. Там, де працюють, а не грають, кількість заражених комп'ютерів складає лише частки відсотка. Проте з березня 1999 року, з появою вірусу "Melissa", ситуація кардинальним чином змінилася.

"Melissa" – це макровірус для файлів MS-Word, що розповсюджується за допомогою електронної пошти в приєднаних файлах. Коли такий (заражений) приєднаний файл відкривають, він розсилає свої копії за першими 50 адресами з адресної книги Microsoft Outlook. В результаті поштові сервери піддаються атаці на доступність.

"Лабораторія Касперського" випустила звіт за перше півріччя 2006 року щодо найбільш значущих змін, подій у галузі комп'ютерної безпеки, а також зробила ряд прогнозів можливого розвитку ситуації на підставі наявної статистики.

% Троянські програми є найбільшим класом шкідливих програм, що динамічно розвивається. Зростання кількості нових модифікацій троянських програм за перші шість місяців 2006 років склало 9%. Найпопулярніші серед них Backdoor (30%), Trojan-Downloader (26%), Trojan-PSW (12%) и Trojan-Spy (13%). Така популярність зумовлена їх ключової роллю при крадіжці персональних даних користувачів при побудові бот-мереж. На відміну від шкідливих програм з самохідним функціоналом (віруси та хробаки) троянські програми повинні бути якимось чином доставлені на комп'ютер-жертву. Для цього останнім часом використовуються спам-розсилання або завантаження з допомогою так званих Exploit'ів (від англ. exploit – використовувати). Ціни кіберкримінального ринку складають $40-60 за 1000 заражень.

Однією з найнебезпечніших тенденцій є зростання кількості інцидентів, коли за допомогою певної програми зловмисники модифікують дані на комп'ютері-жертві з метою подальшого шантажу і отримання фінансової вигоди. Сценарії роботи таких програм багато в чому повторюють один одного і зводяться або до блокування нормальної роботи комп'ютера, або до блокування доступу до даних. У січні 2006 року подібного роду програми були представлені практично єдиною програмою – Trojan.Win32.Krotten.

Таким чином, дія шкідливого програмного забезпечення може бути спрямована не тільки проти доступності, але і проти інших основних аспектів інформаційної безпеки.

1.7 ІНФОРМАЦІЯ, ЩО ПІДЛЯГАЄ ЗАХИСТУ

1.7.1 Державна таємниця

Державна таємниця (секретна інформація) – вид таємної інформації, що охоплює відносини у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою.

У Законі України "Про державну таємницю" наведено такі означення основних термінів:

- **матеріальні носії секретної інформації** – матеріальні об'єкти, в тому числі фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, символів, образів, сигналів, технічних рішень, процесів тощо;
- **доступ до державної таємниці** – надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень;
- **допуск до державної таємниці** – оформлення права громадянина на доступ до секретної інформації;
- **гриф секретності** – реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації;
- **засекречування матеріальних носіїв інформації** – введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифа секретності документам, виробам або іншим матеріальним носіям цієї інформації;

- **ступінь секретності („особливої важливості", „цілком таємно", „таємно")** – категорія, яка характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою.

На кожному пакеті, в який вкладено документацію з грифом „цілком таємно", потрібно обов'язково написати „Перед читанням - спалити"

Відомості можуть вважатися державною таємницею (можуть бути засекречені), якщо:

- вони відповідають переліку відомостей, що складають державну таємницю, входять до переліку відомостей, що підлягають засекречуванню, і відповідають законодавству України про державну таємницю (принцип законності);
- доцільність засекречування конкретних відомостей встановлена шляхом експертної оцінки вірогідних економічних і інших наслідків, можливості нанесення збитку безпеці України, виходячи з балансу життєво важливих інтересів держави, суспільства і особи (принцип обґрунтованості);
- обмеження на поширення цих відомостей і на доступ до них встановлені з моменту їх здобуття (розробки) або завчасно (принцип своєчасності);
- компетентні органи і їх посадові особи прийняли відносно конкретних відомостей рішення про віднесення їх до державної таємниці і засекречування та встановили відносно них відповідний режим правової охорони і захисту (принцип обов'язкового захисту).

Державна таємниця розповсюджується на інформацію з різних галузей життєдіяльності держави.

У сфері оборони до держаної таємниці відносять інформацію:

- про зміст стратегічних і оперативних планів та інших документів бойового управління, підготовку та проведення військових операцій, стратегічне та мобілізаційне розгортання військ, а також про інші найважливіші показники, які характеризують організацію, чисельність, дислокацію, бойову і мобілізаційну готовність, бойову та

іншу військову підготовку, озброєння та матеріально-технічне забезпечення Збройних Сил України та інших військових формувань;

- про напрями розвитку окремих видів озброєння, військової і спеціальної техніки, їх кількість, тактико-технічні характеристики, організацію і технологію виробництва, наукові, науково-дослідні та дослідно-конструкторські роботи, пов'язані з розробленням нових зразків озброєння, військової і спеціальної техніки або їх модернізацією, а також про інші роботи, що плануються або здійснюються в інтересах оборони країни;
- про сили і засоби Цивільної оборони України, можливості населених пунктів, регіонів і окремих об'єктів для захисту, евакуації і розосередження населення, забезпечення його життєдіяльності та виробничої діяльності об'єктів народного господарства у воєнний час або в умовах надзвичайних ситуацій;
- про геодезичні, гравіметричні, картографічні та гідрометеорологічні дані і характеристики, які мають значення для оборони країни.

У сфері економіки, науки і техніки таємною є інформація:

- про мобілізаційні плани і мобілізаційні потужності господарства України, запаси та обсяги постачання стратегічних видів сировини і матеріалів, а також зведені відомості про номенклатуру та рівні накопичення, про загальні обсяги поставок, відпуску, закладення, оновлення, розміщення і фактичні запаси державного резерву;
- про використання транспорту, зв'язку, потужностей інших галузей та об'єктів інфраструктури держави в інтересах забезпечення її безпеки;
- про плани, зміст, обсяг, фінансування та виконання державного замовлення для забезпечення потреб оборони і безпеки;
- про плани, обсяги та інші найважливіші характеристики видобутку, виробництва та реалізації окремих стратегічних видів сировини і продукції;
- про державні запаси дорогоцінних металів монетарної групи, коштовного каміння, валюти та інших цінностей; операції, пов'язані з виготовленням грошових знаків і цінних паперів, їх зберіганням,

охороною і захистом від підроблення, обігом, обміном або вилученням з обігу; а також про інші особливі заходи фінансової діяльності держави;

- про наукові, науково-дослідні, дослідно-конструкторські та проектні роботи, на базі яких можуть бути створені прогресивні технології, нові види виробництва, продукції та технологічних процесів, що мають важливе оборонне чи економічне значення або суттєво впливають на зовнішньоекономічну діяльність та національну безпеку України.

У сфері зовнішніх відносин до таємної відносять інформацію:

- про директиви, плани, вказівки делегаціям і посадовим особам з питань зовнішньополітичної і зовнішньоекономічної діяльності України, спрямовані на забезпечення її національних інтересів і безпеки;
- про військове, науково-технічне та інше співробітництво України з іноземними державами, якщо розголошення відомостей про це завдаватиме шкоди національній безпеці України;
- про експорт та імпорт озброєння, військової і спеціальної техніки, окремих стратегічних видів сировини і продукції.

У сфері державної безпеки та охорони правопорядку до таємної належить інформація:

- про особовий склад органів, що здійснюють оперативно-розшукову діяльність;
- про засоби, зміст, плани, організацію, фінансування та матеріально-технічне забезпечення, форми, методи і результати оперативно-розшукової діяльності, про осіб, які співпрацюють або раніше співпрацювали на конфіденційній основі з органами, що проводять таку діяльність;
- про склад і конкретних осіб, що є негласними штатними працівниками органів, які здійснюють оперативно-розшукову діяльність;
- про організацію та порядок здійснення охорони адміністративних будинків та інших державних об'єктів, посадових та інших осіб, охоро-

на яких здійснюється відповідно до Закону України "Про державну охорону органів державної влади України та посадових осіб";

- про систему урядового та спеціального зв'язку;
- про організацію, зміст, стан і плани розвитку криптографічного захисту секретної інформації, зміст і результати наукових досліджень у сфері криптографії;
- про системи та засоби криптографічного захисту секретної інформації, їх розроблення, виробництво, технологію виготовлення та використання;
- про державні шифри, їх розроблення, виробництво, технологію виготовлення та використання;
- про організацію режиму секретності в органах державної влади, органах місцевого самоврядування, на підприємствах, в установах і організаціях, державні програми, плани та інші заходи у сфері охорони державної таємниці;
- про організацію, зміст, стан і плани розвитку технічного захисту секретної інформації;
- про результати перевірок, здійснюваних, згідно із законом, прокурором у порядку відповідного нагляду за додержанням законів, та про зміст матеріалів дізнання, досудового слідства та судочинства з питань охорони інформації, що належить до державної таємниці;
- про інші засоби, форми і методи охорони державної таємниці.

Конкретні відомості можуть бути віднесені до державної таємниці за ступенями секретності "особливої важливості", "цілком таємно" та "таємно" лише за умови, що вони належать до категорій, зазначених вище, і їх розголошення завдаватиме шкоди інтересам національної безпеки України.

Для набирання тексту секретних документів на роботу запрошується друкарка, що не вміє читати.

Служба працевлаштування

Забороняється віднесення до державної таємниці будь-яких відомостей, якщо цим будуть звужуватися зміст і обсяг конституційних прав та свобод людини і громадянина, завдаватиметься шкода здоров'ю та безпеці населення.

Не відносять до державної таємниці інформацію:

- про стан довкілля, про якість харчових продуктів і предметів побуту;
- про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, які сталися або можуть статися і загрожують безпеці громадян;
- про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;
- про факти порушень прав і свобод людини і громадянина;
- про незаконні дії органів державної влади, органів місцевого самоврядування та їх посадових осіб;
- інша інформація, яка відповідно до законів та міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України, не може бути засекречена.

1.7.2 Комерційна таємниця

Комерційна таємниця – це відомості, що не є державною таємницею, зв'язані з виробництвом, технологіями, фінансами, процесами управління та іншою діяльністю організацій чи фірм, розголошення, витік і несанкціонований доступ до яких може завдати шкоди їх інтересам.

Дуже важливо правильно і вчасно визначити, які відомості слід віднести до комерційної таємниці.

Як інформацію, що становить комерційну таємницю, варто розглядати науково-технічну, технологічну, виробничу, фінансово-економічну або іншу інформацію (у тому числі складову секретів виробництва (ноу-хау), що має дійсну або потенційну комерційну цінність через її невідомість третім особам, до якої немає вільного доступу на законній підставі та стосовно якої власником уведений режим комерційної таємниці.

Комерційна таємниця охороняється за сприяння держави.

Основними суб'єктами права на комерційну таємницю є власники комерційної таємниці та їх правонаступники.

Власники комерційної таємниці – фізичні (незалежно від громадянства) і юридичні (комерційні і некомерційні організації) особи, що займаються підприємницькою діяльністю і мають монопольне право на інформацію, яка складає для них комерційну таємницю.

Правонаступники – це фізичні і юридичні особи, яким через службовий стан, за договором або на іншій законній підставі (у тому числі як спадок) відома інформація, яка складає комерційну таємницю іншої особи.

Для охорони комерційної інформації організації необхідно:

1) визначити перелік інформації, що становить комерційну таємницю;

2) обмежити доступ до такої інформації шляхом установлення порядку обігу цієї інформації та контролю за дотриманням такого порядку;

3) організувати облік осіб, які одержали доступ до інформації, що становить комерційну таємницю, і (або) осіб, яким таку інформацію було надано або передано;

4) урегулювати відносини з використання інформації, що становить комерційну таємницю, із працівниками на підставі трудових договорів і з контрагентами на підставі цивільно-правових договорів;

5) нанести на документи, що містять комерційну таємницю, гриф «комерційна таємниця» з указанням власника цієї інформації (для юридичних осіб – повне найменування й місце знаходження, для індивідуальних підприємців – прізвище, ім'я, по батькові громадянина, що є індивідуальним підприємцем, і місце його проживання);

6) призначити відповідальних за схоронність комерційних відомостей і за дотримання «таємного» режиму.

Найбільш секретні папери в офісі з міркувань безпеки рвуться не менше ніж на дві частини (їх рвали б і менше ніж на дві частини, тому що ледарі, але не вдається) і викидаються в кошик так, що їх легко прочитати, просто кинувши на них погляд.

"Посібник з комп'ютерної безпеки й захисту інформації"
Карл Абрахам Шкафиц II

Будь-які заходи щодо захисту інформації повинні бути обґрунтовані з фінансової точки зору. Конфіденційність не може коштувати дорожче тих відомостей, які захищаються. Тому перш ніж уводити режим комерційної таємниці, керівництву фірми за участю бухгалтерії й провідних спеціалістів потрібно оцінити економічний ефект, що його дасть засекречування інформації (величину потенційного прибутку або відверненого збитку), і порівняти його з можливими втратами від її відкритого використання.

При цьому потрібно визначити:

1) які саме відомості мають потребу в захисті;

2) кого вони можуть зацікавити, і яку цінність мають для конкурентів;

3) які елементи інформації є найбільш важливими й уразливими;

4) як довго відомості, що становлять комерційну таємницю, будуть актуальними;

5) у що обійдеться захист інформації з фінансової та організаційної точок зору;

6) коло співробітників, що мають право доступу до такого роду відомостей і здійснюють роботу з ними;

7) які умови роботи будуть необхідні й достатні для забезпечення конфіденційності відповідної категорії відомостей.

Інформація, розголошення якої може нанести фірмі збиток, багато в чому залежить від профілю її діяльності. Однак є узагальнений перелік даних, можливий витік яких фахівці із захисту інформації рекомендують припиняти в першу чергу.

У сфері фінансів:

1) дані бухгалтерського, податкового й управлінського обліку;

2) планові й фактичні показники фінансово-господарської діяльності;

3) відомості про особисті доходи кожного працівника;

4) відомості про стан банківських рахунків і проведених фінансових операцій;

5) відомості про рентабельність виробництва;

6) відомості про боргові зобов'язання підприємства, у тому числі про розміри й умови отриманих кредитів і позик;

7) механізм ціноутворення (прямі витрати, накладні витрати, норма прибутку);

8) відомості про ефективність імпорту й експорту (у тому числі розрахунки експортної й імпортної вартості товарів, робіт, послуг);

9) відомості про участь підприємства в статутних капіталах інших організацій.

У ринкових взаєминах:

1) оригінальні методи маркетингових досліджень;

2) результати вивчення ринку, оцінки стану та перспектив розвитку ринкової кон'юнктури;

3) відомості про ринкову стратегію фірми та про оригінальні методи просування товарів;

4) проекти прайс-листів та умови надання знижок;

5) відомості про передбачувані закупівлі, про отримані замовлення й про обсяг взаємних поставок за довгостроковими договорами;

6) відомості про підприємство як про торговельного партнера;

7) дані про всіх контрагентів, ділових партнерів і конкурентів підприємства, яких немає у відкритих джерелах;

8) зміст торговельних угод, які за домовленістю сторін уважаються конфіденційними;

9) відомості про підготовку до торгів, аукціонів і про їх результати.

У сфері керування підприємством і забезпечення безпеки:

1) відомості про механізм підготовки, прийняття й виконання управлінських рішень;

2) відомості про проведення, порядок денний та результати службових нарад;

3) відомості про підготовку й результати переговорів з діловими партнерами підприємства;

4) відомості про організацію захисту комерційної таємниці, про охоронну систему підприємства, про комерційну таємницю, передану партнерам (отриману від партнерів) на довірчій основі або за договорами;

5) стан програмного й комп'ютерного забезпечення фірми;

6) зміст завдань на відрядження (якщо відрядження носять конфіден-

ційний характер).

У сфері виробництва:

1) відомості про структуру виробництва, виробничі потужності, типи і розміщення устаткування, запаси сировини, матеріалів, комплектуючих і готової продукції;

2) напрямки й обсяги інвестицій, планові та звітні дані про введення об'єктів в експлуатацію;

3) планові економічні показники;

4) плани розширення або згортання виробництва різних видів продукції і їх техніко-економічні обґрунтування;

5) відомості про нові матеріали й технологію їх застосування, про комплектуючі вироби, які надають продукції нові якості;

6) відомості про модернізації відомих технологій, що дозволяють підвищити конкурентоспроможність продукції.

У науково-технічній діяльності:

1) відомості про цілі, завдання і програми перспективних досліджень;

2) матеріали про незареєстровані відкриття, винаходи й раціоналізаторські пропозиції;

3) конструкційні характеристики створюваних виробів і параметри розроблюваних технологічних процесів (габарити, компоненти, режими обробки й т.п.);

4) особливості конструкторсько-технологічних рішень і дизайнерського оформлення, які можуть змінити рентабельність виробів;

5) умови експериментів і характеристика устаткування, на якому вони здійснювалися;

6) використовувані методи захисту від підробки товарних знаків.

Зрозуміло, що наведений список не є обов'язковим або вичерпним. Залежно від конкретних умов роботи підприємства його можна скоротити або доповнити. При цьому потрібно спрогнозувати, які негативні наслідки виникнуть, якщо та або інша інформація «піде на сторону». Результатом безтурботності можуть стати:

1) розрив (або погіршення) ділових відносин з партнерами;

2) зрив переговорів, втрата вигідних контрактів;

3) невиконання договірних зобов'язань;

4) необхідність проведення додаткових ринкових досліджень;

5) відмова від рішень, що стали неефективними через розголос інформації, і, як наслідок, фінансові втрати, пов'язані з новими розробками;

6) втрата можливості запатентувати продукт або продати ліцензію;

7) зниження цін або обсягів реалізації;

8) втрата авторитету або ділової репутації фірми;

9) більш жорсткі умови одержання кредитів;

10) труднощі з постачання та придбання устаткування тощо.

Одним з компонентів комерційної таємниці може бути «ноу-хау».

«Ноу-хау»- це відомості про рішення у будь-яких сферах практичної діяльності (техніці, економіці, організації тощо), що допускають їх практичне використання та є придатними для участі в економічному обігу через невідомість та недоступність невизначеному колу осіб.

Пропоноване рішення може бути як результатом нової розробки, так і вже накопичених з часом знань, досвіду, навичок.

На відміну від інших видів інформації, що можуть становити комерційну таємницю, «ноу-хау» полягає у вирішенні практичної задачі, у рекомендації до дії, воно не має чисто пізнавального або інформаційного характеру, це має бути рішення, що допускає здійснення. Так, наприклад, не можна назвати «ноу-хау» систематизовану інформацію, клієнтську базу, яка, проте, цілком може бути захищена як комерційна таємниця.

«Ноу-хау» – це охоронювані в режимі комерційної таємниці результати інтелектуальної діяльності, які можуть бути передані іншій особі та використані нею на законній підставі, у тому числі:

- неопубліковані науково-технічні результати, технічні рішення, методи, способи використання технологічних процесів та пристроїв, які не забезпечені патентним захистом відповідно до законодавства або за рішенням особи, яка володіє такою інформацією на законній підставі;

- знання та досвід в області реалізації продукції і послуг, відомості про кон'юнктуру ринку, результати маркетингових досліджень;
- комерційні, методичні або організаційно-управлінські ідеї та рішення.

Термін «ноу-хау» походить від англійського виразу «know how» або «знаю як [зробити]». Вперше термін «know-how» з'явився у 1916 році в США у рішенні в судовій справі «Дізенд проти Брауна» і з того часу почав широко вживатися у всьому світі, став звичним в економічному обігу.

У міжнародній практиці та актах, а також в законодавстві іноземних країн, найчастіше вживається термін «trade secret», який, як правило, перекладають як «торговий секрет».

1.7.3 Банківська таємниця

Банківська таємниця — це відомості про банківські операції з рахунками і операції в інтересах клієнтів, про рахунки і вклади своїх клієнтів і кореспондентів, а також відомості про клієнтів і кореспондентів, розголошування яких може порушити право останніх на недоторканність приватного життя.

Основними об'єктами банківської таємниці є:

1) таємниця банківського вкладу – відомості про всі види вкладів клієнта в кредитній організації;

2) таємниця приватного життя клієнта або кореспондента – відомості, що складають особисту, родинну таємницю і охороняються законом як персональні дані цього клієнта або кореспондента;

3) таємниця банківського рахунку – відомості про рахунки клієнтів і кореспондентів і дії з ними в кредитній організації (про розрахунковий, поточний, бюджетний, депозитний, валютний, кореспондентський і тому подібні рахунки, про відкриття, про закриття, переведення, переоформлення рахунків тощо);

4) таємниця операцій з банківським рахунком – відомості про прийняття і зарахування грошових коштів, що надходять на рахунок клієнта, ви-

конання його розпоряджень з перерахування і видачі відповідних сум з рахунку, а також про здійснення інших операцій і операцій з банківським рахунком, передбачених договором банківського рахунка або законом.

На сьогодні основоположним документом, який визначає правовий режим банківської таємниці в Україні, є Закон України "Про банки і банківську діяльність" № 2121-14 в редакції від 7 грудня 2000 року.

Згідно з цим законом до банківської таємниці певного банку також належить інформація про клієнтів інших банків, яка може стати відомою з документів, угод та операцій клієнта банку.

Законом віднесено до банківської таємниці інформацію про організаційно-правову структуру юридичної особи - клієнта банку, її керівників, напрями діяльності.

Також банківську таємницю складає інформація зі звітності окремого банку, за винятком тієї, що підлягає опублікуванню, а саме: дата реєстрації, кількість балансових філій, кількість працюючих на кінець року, кількість рахунків, валюта балансу, обсяг кредитного портфеля, обсяг вкладів громадян, капітал банку, сплачений статутний фонд, сума доходів, сума витрат, прибуток, рентабельність власного капіталу у відсотках.

Режим конфіденційності деякого обсягу інформації про банк, яка складає банківську таємницю, має строковий, а не абсолютний характер – припинення режиму конфіденційності даної інформації пов'язується із настанням певної події в часі, а саме: на такій стадії ліквідації банку, як призначення ліквідатора, відомості про фінансове становище банку перестають бути конфіденційними чи становити банківську таємницю. Однак решта відомостей, що становлять банківську таємницю, зберігають режим конфіденційності.

1.7.4 Податкова таємниця

Податкову таємницю становлять будь-які відомості про платника податків, отримані податковим органом, органами внутрішніх справ, органом державного позабюджетного фонду й митним органом , за винятком відомостей:

1) розголошених платником податків самостійно або з його згоди;

2) про ідентифікаційний номер платника податків;

3) про порушення законодавства про податки й збори й міри відповідальності за ці порушення;

Відповідно до Кодексу щодо запобігання ухилення від податків, прийнятого в 2006 році, забороняється не повідомляти податковому інспектору будь-яку інформацію, яку б ви не хотіли доводити до його відома, хоча ви і не зобов'язані повідомляти йому інформацію, яку ви не проти йому повідомити

http://blog.yurist-online.com

4) надаваних податковим (митним) або правоохоронним органам інших держав відповідно до міжнародних договорів (угод), однієї зі сторін яких є Україна, про взаємне співробітництво між податковими (митними) або правоохоронними органами (у частині відомостей, наданих цим органам).

1.7.5 Службова таємниця

Службова таємниця – конфіденційна інформація, що захищається згідно із законом, стала відомою в державних органах і органах місцевого самоврядування лише на законних підставах і через виконання їх представниками службових обов'язків, а також службова інформація про діяльність державних органів, доступ до якої обмежений законом або через службову необхідність.

До основних об'єктів таємниці належать такі види інформації:

- службова інформація про діяльність державних органів, доступ до якої обмежений законом з метою захисту державних інтересів: військова таємниця; таємниця слідства (дані попереднього розслідування або слідства); судова таємниця (таємниця наради суддів, вміст дискусій і результатів голосування закритої наради Конституційного суду України, матеріали закритого судового засідання або через службову необхідність, порядок вироблення і ухвалення рішення, організація внутрішньої роботи і т.п.);
- конфіденційна інформація, що стала відомою через виконання службових обов'язків посадовою особою державних органів і

органів місцевого самоврядування: комерційна таємниця, банківська таємниця, професійна таємниця, а також конфіденційна інформація про приватне життя особи.

Інформація службової таємниці повинна відповідати критеріям охороноздатності права:

- бути віднесеною законом до службової інформації про діяльність державних органів, доступ до якої обмежений згідно із законом або через службову необхідність;
- бути конфіденційною інформацією службового характеру (чужою таємницею) іншої особи (комерційна таємниця, банківська таємниця, таємниця приватного життя, професійна таємниця);
- не бути державною таємницею і не входити до переліку відомостей, доступ до яких не може бути обмежений;
- бути отриманою представником державного органу і органу місцевого самоврядування лише через виконання службових обов'язків у випадках і порядку, встановлених законом.

Інформація, що не відповідає цим вимогам, не може вважатися службовою таємницею і не підлягає правовій охороні.

Відомості, які не можуть бути віднесені до службової інформації обмеженого поширення:

- відомості з актів законодавства, що встановлюють правовий статус державних органів, організацій, суспільних об'єднань, інформація про права, свободи і обов'язки громадян, порядок їх реалізації;
- відомості про надзвичайні ситуації, небезпечні природні явища і процеси; екологічна, гідрометеорологічна, гідрогеологічна, демографічна, санітарно-епідеміологічна та інша інформація, необхідна для забезпечення безпечного існування населених пунктів, виробничих об'єктів, громадян і населення в цілому;
- відомості з описів структур органів виконавчої влади, їх функцій, напрямів і форм діяльності, інформація про їх адресу і місце розташування;
- інформація про порядок розгляду заяв фізичних і юридичних осіб;

- відомості про виконання бюджету і використання інших державних ресурсів, про стан економіки і потреби населення;
- інформація з документів відкритих фондів бібліотек і архівів, інформаційних систем організацій, необхідна для реалізації прав, свобод і обов'язків громадян.

1.7.6 Професійна таємниця

Професійна таємниця – інформація, що захищається згідно із законом, довірена або така, що стала відомою особі виключно через виконання нею своїх професійних обов'язків, не пов'язаних з державною або муніципальною службою, поширення якої може завдати збитку правам і законним інтересам власника інформації або іншої особи (довірителя), що довірила ці відомості, які не є державною або комерційною таємницею.

Інформація професійної таємниці за критеріями охороноздатності права відповідає таким вимогам:

- інформація не належить до відомостей, що складають державну і комерційну таємницю;
- інформація стала відомою або була довірена особі лише через виконання нею своїх професійних обов'язків;
- інформація стала відомою або була довірена особі, що не перебуває на державній або муніципальній службі (інакше інформація вважається службовою таємницею);
- заборонено поширення довіреної або такої, що стала відомою, інформації, яка може завдати збитку правам і законним інтересам довірителя.

Відповідно до цих критеріїв виділяють такі об'єкти професійної таємниці.

1. **Лікарська таємниця** – інформація, що містить:

- відомості про факт звертання за медичною допомогою, про стан здоров'я, діагнози захворювання та інші відомості, отримані при обстеженні і лікуванні громадянина;

- відомості про здійснення штучного запліднення та імплантацію ембріона, а також про особу донора;
- відомості про донора і реципієнта при трансплантації органів і (або) тканин людини;
- відомості про наявність психічного розладу, факти звертання за психіатричною допомогою і лікування в установі, що надає таку допомогу, а також інші відомості про стан психічного здоров'я громадянина;
- інші відомості в медичних документах громадянина.

2. **Нотаріальна таємниця** – відомості, довірені нотаріусові у зв'язку із здійсненням нотаріальних дій.

3. **Адвокатська таємниця** – інформація, повідомлена адвокатові громадянином у зв'язку з наданням йому юридичної допомоги.

4. **Таємниця зв'язку** – таємниця листування, телефонних переговорів, поштових, телеграфних і інших повідомлень.

5. **Таємниця усиновлення** – відомості про усиновлення дитини, довірені на законній підставі іншим особам, окрім суддів, що винесли ухвалу про усиновлення, і посадових осіб, що здійснюють державну реєстрацію цього усиновлення.

6. **Таємниця страхування** – відомості про страхувальника, застраховану особу, стан їх здоров'я, а також про майновий стан цих осіб, отримані страховиком в результаті своєї професійної діяльності.

7. **Таємниця сповіді** – відомості, довірені громадянином священнослужителеві на сповіді.

1.7.7 Персональні дані

У Європі для охорони і захисту права на недоторканність приватного життя в умовах автоматизованої обробки особистих даних про громадян більше 25 років тому був введений інститут захисту персональних даних. Більш ніж в 20 європейських державах ухвалені національні закони про персональні дані, у ряді країн введені незалежні уповноважені із захисту персональних даних, у всіх країнах Європейського Союзу з 1998 р. створено єди-

ну уніфіковану систему захисту персональних даних, зокрема в секторі телекомунікацій.

Персональні дані – інформація (зафіксована на будь-якому матеріальному носієві) про конкретну людину, яка ототожнена або може бути ототожнена з нею.

До персональних даних можуть бути віднесені відомості, використання яких без згоди суб'єкта персональних даних може завдати шкоди його честі, гідності, діловій репутації, доброму імені, іншим нематеріальним благам і майновим інтересам:

- біографічні і пізнавальні дані (у тому числі про обставини народження, усиновлення, розлучення);
- відомості про сімейний стан (у тому числі про родинні стосунки);
- відомості про майновий, фінансовий стан (окрім випадків, прямо встановлених в законі);
- особисті характеристики (у тому числі, особисті звички і схильності);
- відомості про стан здоров'я.

Суб'єктами права тут виступають:

- особи, яких стосуються відповідні дані, та їх спадкоємці;
- утримувачі персональних даних – органи державної влади і органи місцевого самоврядування, юридичні і фізичні особи, що здійснюють на законних підставах збір, зберігання, передачу, уточнення, блокування, знеособлення, знищення персональних даних (баз персональних даних).

Для персональних даних і роботи з ними передбачені такі правила:

- персональні дані мають бути отримані і оброблені законним чином на підставі чинного законодавства;
- дані вносяться до бази персональних даних на підставі вільної згоди суб'єкта у письмовій формі, за винятком випадків, прямо встановлених в законі;
- персональні дані повинні накопичуватися для точно визначеної та законної мети, не використовуватися в протиріччі з цією метою і

не бути надлишковими стосовно неї. Не допускається об'єднання баз персональних даних, зібраних тримачами в різних цілях, для автоматизованої обробки інформації;

- персональні дані, що надаються тримачем, мають бути точними; у разі потреби вони повинні оновлюватися;
- персональні дані повинні зберігатися не довше, ніж цього вимагає мета, і підлягати знищенню після досягнення цієї мети;
- персональні дані охороняються в режимі конфіденційної інформації, що виключає їх випадкове або несанкціоноване руйнування або випадкову втрату, а також несанкціонований доступ до даних, їх зміну, блокування або передачу;
- встановлюється спеціальний правовий режим використання персональних даних осіб, що обіймають вищі державні посади, і кандидатів на ці посади.

1.8 СПОСОБИ НЕПРАВОМІРНОГО ОВОЛОДІННЯ КОНФІДЕНЦІЙНОЮ ІНФОРМАЦІЄЮ

У значній частині законодавчих актів, законів, кодексів, офіційних матеріалів стосовно неправомірного оволодіння конфіденційною інформації використовуються такі поняття, як розголошення відомостей, витік інформацією і несанкціонований доступ до конфіденційної інформації.

Розголошення – це навмисні чи необережні дії з конфіденційними відомостями, що призвели до ознайомлення з ними осіб, не допущених до них.

Розголошення полягає у повідомленні, передачі, наданні, пересиланні, опублікуванні, втраті та в інших формах обміну і дій з діловою і науковою інформацією.

Реалізується розголошення *формальними і неформальними каналами* поширення інформації.

До **формальних комунікацій** належать ділові зустрічі, наради, переговори і тому подібні форми спілкування: обмін офіційними діловими і науковими документами засобами передачі офіційної інформації (пошта, телефон, телеграф і ін.).

Неформальні комунікації – це особисте спілкування (зустрічі, листування й ін.); виставки, семінари, конференції й інші масові заходи, а також засоби масової інформації (газети, інтерв'ю, радіо, телебачення й ін.).

Як правило, причиною розголошення конфіденційної інформації є недостатнє знання співробітниками правил захисту комерційних секретів і нерозуміння необхідності їх ретельного дотримання. Отут важливо відзначити, що суб'єктом у цьому процесі виступає джерело (власник) секретів, що охороняються.

Необхідно враховувати такі особливості інформації. Інформація змістовна, осмислена, упорядкована, аргументована і доводиться найчастіше в реальному масштабі часу. Часто є можливість діалогу. Інформація орієнтована у певній тематичній галузі і документована. З урахуванням цього, для одержання інформації зловмисник може докладати практично мінімальні зусилля.

Закордонні фахівці до найбільш імовірних каналів витоку конфіденційної інформації відносять такі:

- спільну діяльність із іншими фірмами;
- проведення переговорів;
- екскурсії й відвідування фірми;
- рекламу, публікації в пресі, інтерв'ю;
- консультації фахівців з інших фірм, що одержують доступ до документації й виробничої діяльності даної фірми;
- фіктивні запити про можливість роботи у фірмі, укладання з нею угод, здійснення спільної діяльності;
- розсилання окремим співробітникам фірми різних анкет й опитувальників під виглядом наукових або маркетингових досліджень;
- приватні бесіди зі співробітниками фірми, нав'язування їм незапланованих дискусій з різних проблем.

Витік – це безконтрольний вихід конфіденційної інформації за межі організації чи кола осіб, яким вона була довірена

Канал витоку інформації – це шлях від джерела конфіденційної інформації до зловмисника, за допомогою якого останній може одержати доступ до відомостей, що охороняються.

Для утворення каналу витоку інформації необхідні певні просторові, енергетичні і часові умови, а також наявність на стороні зловмисника відповідної апаратури прийому, обробки і фіксації інформації.

Взаємодію об'єкта (фірма, організація) і суб'єкта (конкурент, зловмисник) в інформаційному процесі з протилежними інтересами можна розглядати з позиції активності в діях, що призводять до оволодіння конфіденційними відомостями.

У цьому випадку можливі такі ситуації:

- власник (джерело) не вживає ніяких заходів для збереження конфіденційної інформації, що дозволяє зловмиснику легко одержати відомості, які його цікавлять;
- джерело інформації строго дотримується заходів інформаційної безпеки, тоді зловмиснику доводиться докладати значних зусиль для здійснення доступу до відомостей, що охороняються, використовуючи для цього всю сукупність способів несанкціонованого проникнення;
- проміжна ситуація – це витік інформації технічними каналами, коли джерело ще не знає про це (інакше він вжив би заходи захисту), а зловмисник легко, без особливих зусиль може їх використовувати у своїх інтересах.

Можливі канали витоку інформації поділяються на такі групи.

Перша група. Канали, пов'язані з доступом до елементів системи обробки даних, але такі, що не потребують зміни компонентів системи. До цієї групи належать канали, що утворюються за рахунок:

- дистанційного прихованого відеоспостереження або фотографування;

- застосування пристроїв підслуховування;
- перехоплення електромагнітних випромінювань і наведень і т.д.

Друга група. Канали, пов'язані з доступом до елементів системи й зміною структури її компонентів. До даної групи належать:

- спостереження за інформацією з метою її запам'ятовування в процесі оброблення;
- розкрадання носіїв інформації;
- збір виробничих відходів, що містять оброблювану інформацію;
- навмисне зчитування даних з файлів інших користувачів;
- читання інформації, що залишається на носіях після виконання завдань;
- копіювання носіїв інформації;
- навмисне використання для доступу до інформації терміналів зареєстрованих користувачів;
- маскування під зареєстрованого користувача шляхом викрадення паролів і інших реквізитів розмежування доступу до інформації, використовуваної в системах обробки;
- використання для доступу до інформації так званих «люків», «дірок» і «лазівок», тобто можливостей обходу механізму розмежування доступу, що виникають внаслідок недосконалості загальносистемних компонентів програмного забезпечення (операційних систем, систем керування базами даних і ін.) і неоднозначності мов програмування, застосовуваних в автоматизованих системах обробки даних.

Третя група. Канали, що утворюються за рахунок:

- незаконного підключення спеціальної реєструвальної апаратури до пристроїв системи або ліній зв'язку (перехоплення модемного й факсимільного зв'язку);
- злочинної зміни програм таким чином, щоб ці програми поряд з основними функціями обробки інформації здійснювали також несанкціоноване збирання і реєстрацію цінної інформації;
- злочинного виведення з ладу механізмів захисту.

Четверта група. До складу цієї групи входять:

- несанкціоноване одержання інформації шляхом підкупу або шантажу посадових осіб відповідних служб;
- одержання інформації шляхом підкупу та шантажу співробітників, знайомих, обслуговуючий персонал або родичів, що знають про відповідну діяльність.

Несанкціонований доступ – це протиправне навмисне оволодіння конфіденційною інформацією суб'єктом, який не має права доступу до секретів, що охороняються.

Несанкціонований доступ до джерел конфіденційної інформації реалізується різними способами: від *ініціативного співробітництва*, що полягає в активному прагненні «продати» секрети, до *використання різних засобів проникнення* до комерційних секретів.

Розглянемо типову ситуацію, яка може виникнути в будь-якій фірмі або організації.

Після того, як фінансовий документ у філії великої компанії створено, його необхідно відправити електронною поштою в головний офіс на підпис керівникові. При цьому можуть відбутися такі події:

1) Документ створено, і щасливий співробітник після роботи над ним пішов на обід. У цей час зловмисник здійснив несанкціонований доступ до персонального комп'ютера співробітника й підмінив або знищив документ.

2) Документ створено, співробітник поклав його в теку на файловому сервері корпоративної мережі й пішов додому. У цей час його конкурент або недоброзичливець, отримавши доступ до сервера, підмінив або знищив документ.

3) Документ створено, співробітник поклав його в теку на файловому сервері корпоративної мережі. Відбулася атака на корпоративну мережу компанії з боку мережі Інтернет, і всі бази даних й інші матеріали знищено.

4) Документ створено і відправлено електронною поштою або відправлено на ftp сервер у головний офіс. При передачі документа відбулося його перехоплення й підміна.

5) Документ створено, переписано на дискету й відправлено з кур'єром у головний офіс. Кур'єр за день дуже втомився й забув теку з диском в транспорті.

6) Документ створено, оброблено, і він зберігається десь на диску якогось комп'ютера. Комп'ютер «за старістю» списується й новий власник знаходить у схованих файлах річний фінансовий звіт. Він продає звіт конкурентові.

7) Комп'ютер співробітника або сервер мережі був заражений вірусом, що спричинило знищення баз даних і іншої важливої інформації.

У кожному із цих випадків компанія зазнає фінансових збитків і, якщо інформація про подію виходить за межі компанії, втрачає свою репутацію на ринку.

Наведений приклад свідчить про необхідність комплексного підходу до забезпечення інформаційної безпеки, тобто потрібен захист інформації як від розголошення, так і від витоку по технічних каналах і від несанкціонованого доступу до неї з боку конкурентів і зловмисників.

1.9 ФІЗИЧНІ КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ

Інформація передається полем або речовиною. Це або акустична хвиля (звук), або електромагнітне випромінювання, або аркуш паперу з текстом тощо. Але ні передана енергія, ні передана речовина самі по собі ніякого значення не мають, вони є лише носіями інформації. Людина не розглядається як носій інформації. Вона виступає суб'єктом відносин або джерелом.

За фізичною природою можливі такі засоби перенесення інформації:

- світлові промені;
- звукові хвилі;
- електромагнітні хвилі;
- матеріали і речовини.

Використовуючи в своїх інтересах ті або інші фізичні поля, людина створює певну систему передавання інформації. Такі системи прийнято називати *системами зв'язку*.

Будь-яка система зв'язку (система передавання інформації) складається з джерела інформації, передавача, лінії зв'язку (фізичного середовища розповсюдження сигналу), приймача і одержувача інформації. Ці системи використовуються в повсякденній практиці відповідно до свого призначення і є офіційними засобами передачі інформації, робота яких контролюється з

метою забезпечення надійної, достовірної і безпечної передачі інформації, що виключає неправомірний доступ до неї з боку конкурентів.

Проте існують певні умови, за яких можливе утворення системи передачі інформації з однієї точки в іншу незалежно від бажання об'єкта і джерела. При цьому, природно, такий канал в явному вигляді не повинен себе проявляти. За аналогією з каналом передачі інформації такий канал називають каналом витоку інформації. Він також складається з джерела сигналу, фізичного середовища його розповсюдження і приймальної апаратури на стороні зловмисника. Рух інформації в такому каналі здійснюється тільки в один бік – від джерела до зловмисника.

На рис. 1.3 наведено узагальнену схему можливих каналів витоку і несанкціонованого доступу до інформації, що обробляється в типовому одноповерховому офісі.

Зловмисник може отримати доступ до конфіденційної інформації використовуючи:

- витік за рахунок звуку в стінах і перекриттях;
- радіозакладки в стінах і меблях;
- знімання інформації за системою вентиляції;
- високочастотний канал витоку в побутовій техніці;
- лазерне знімання акустичної інформації з вікон;
- знімання акустичної інформації з використанням диктофонів;
- дистанційне знімання відеоінформації (оптика);
- знімання інформації з використанням відеозакладок;
- знімання інформації за рахунок наведень і "нав'язування";
- знімання інформації направленим мікрофоном;
- витік за рахунок побічного випромінювання термінала;
- виробничі і технологічні відходи;

В Каліфорнії доктор медицини Ральф Комінгс викинув у сміттєвий контейнер зразу декілька коробок з конфіденційними паперами.

cnews.ru

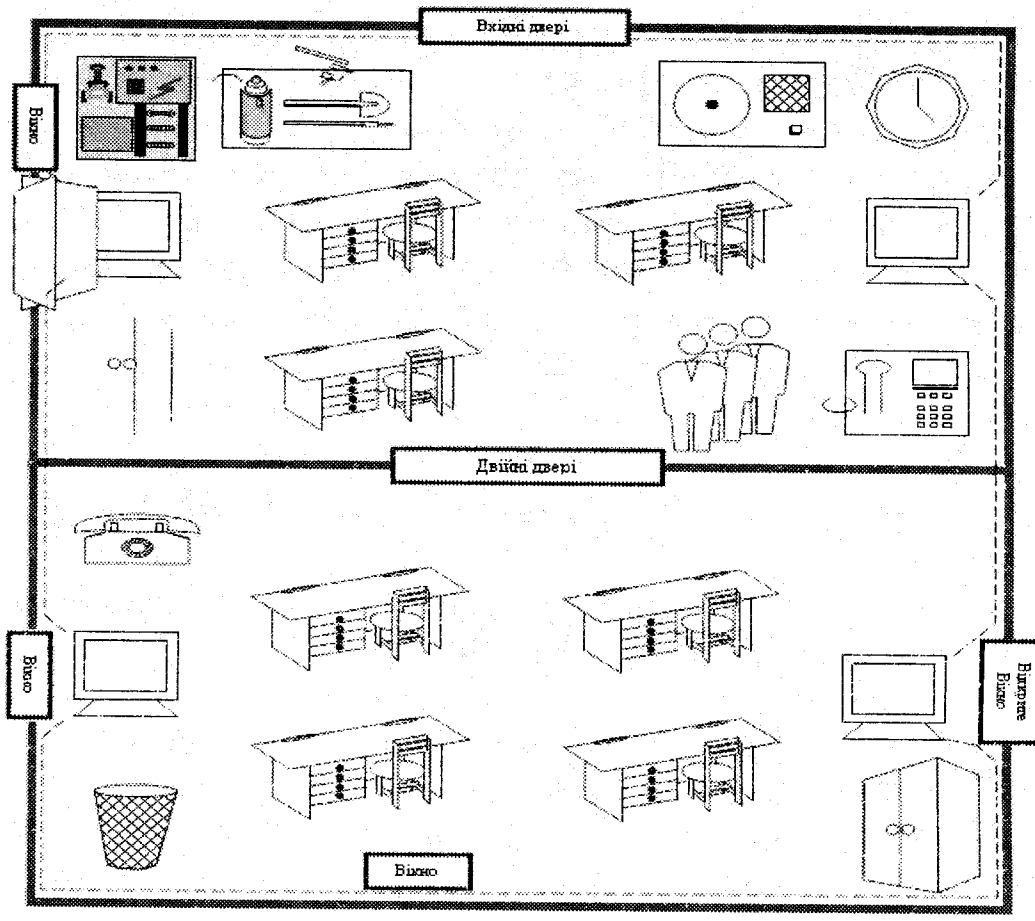


Рисунок 1.3 – Схема каналів витоку та несанкціонованого доступу до інформації в типовому одноповерховому офісі

- знімання інформації за рахунок використання "телефонного вуха";
- знімання з клавіатури і принтера через акустичний канал;
- знімання з дисплея через електромагнітний канал;
- візуальне знімання з дисплея і принтера;

При розсиланні квитанцій про державну допомогу, в яких були вказані персональні дані отримувачів, у вересні 2008 р. був зафіксований витік інформації через... принтер. При друкуванні квитанцій принтер заїло, і титульні аркуші були прикріплені до даних інших отримувачів, в результаті стався витік даних 3 тис. осіб.

cnews.ru

- наведення на лінії комунікацій і сторонні провідники;
- витік через лінії зв'язку;
- витік ланцюгами заземлення;
- витік мережею трансляції і через гучномовний зв'язок;
- витік через охоронно-пожежну сигналізацію;
- витік мережею електроживлення;
- витік мережами опалювання, газо- і водопостачання;
- внутрішні канали витоку інформації (обслуговуючий персонал);

IT-аналітик компанії Atos Origin, яка співпрацювала з британським урядом, після пива, випитого в пабі, загубив невеличку флешку. На ній зберігались коди доступу до гігантської урядової бази даних Governement Gateway (більш ніж 12 млн. записів). На деякий час базу даних довелось закрити.

cnews.ru

- розкрадання носіїв інформації;
- несанкціоноване копіювання;
- програмно-апаратні закладки в комп'ютері;
- шкідливе програмне забезпечення;
- витоки мережею Internet.

При виявленні каналів витоку інформації необхідно розглядати всю сукупність комп'ютерного обладнання, що містить технічні засоби обробки інформації, лінії зв'язку, розподільні і комутаційні пристрої, системи електроживлення, системи заземлення тощо. Слід враховувати також такі допоміжні технічні засоби і системи, як засоби відкритого телефонного, факсимільного, гучномовного зв'язку, системи охоронної і пожежної сигналізації, електрифікації, радіофікації, електропобутові прилади тощо.

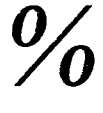
Серед каналів витоку помітну роль грають допоміжні засоби, що виходять за межі контрольованої зони, а також сторонні дроти, кабелі, металеві труби систем опалювання, водопостачання та інші струмопровідні металоконструкції, що проходять через приміщення, де встановлені основні і допоміжні технічні засоби.

Не зважаючи на значне зростання ролі автоматизованих інформаційних систем у потоках повідомлень зберігається висока (до 80%) питома вага

мовної інформації. І саме вона часом стає «ласим шматочком» для конкурента або зловмисника. Одна випадково загублена або найчастіше просто підслухана фраза - і можна втратити дохідну угоду, розоритися чи стати об'єктом шантажу.

За часів СРСР зі стін відомчих і виробничих приміщень невпинно закликали до пильності плакати: «Базіка – знахідка для шпигуна» і «Тсс! Ворог підслуховує». Сьогодні якщо не ворог, то вже конкурент підслуховує напевно. Із часів плакатно-політичної агітації й всенародної пильності необхідність захисту мовної інформація не втратила своєї актуальності. А от пильності в народу явно зменшилося. Дослідження фахівців показали, що керівництво більшості фірм (62% опитаних) не надає належного значення цій проблемі.

Існуючих каналів витоку мовної інформації досить багато, від традиційних до досить екзотичних. Зрозуміло, що далеко не завжди й не від усіх з них потрібно захищатися.



Більшість фахівців вважають основними загрозами підключення до телефонних ліній (34%) і прослуховування приміщень за допомогою мікрофонів (32%). Ще 20% побоюються прямого прослуховування мовної інформації, що циркулює в приміщенні.

Часто доводиться зустрічатися із ситуаціями, коли відвідувачі, що перебувають у приймальні, досить чітко чують усе, що відбувається в кабінеті посадової особи, співробітники в приміщенні для куріння обговорюють внутрішні справи організації, а наради проводяться в приміщеннях першого поверху при відкритих вікнах або кватирках. Виявити потрібну інформацію в подібних випадках нескладно.

Аналіз можливих каналів витоку і несанкціонованого доступу показує, що істотну їх частину складають технічні канали витоку акустичної інформації. Залежно від середовища розповсюдження акустичних коливань, способів їх перехоплення і фізичної природи виникнення інформаційних сигналів технічні канали витоку акустичної інформації поділяють на повітряні, вібраційні, електроакустичні, оптико-електронні і параметричні.

У **повітряних** технічних каналах витоку інформації середовищем розповсюдження акустичних сигналів є повітря і для їх перехоплення використовуються мініатюрні високочутливі і направлені мікрофони, які

з'єднуються з диктофонами або спеціальними мікропередавачами, їх називають акустичними закладками. Перехоплена цими пристроями акустична інформація може передаватися радіоканалом, мережею змінного струму, з'єднувальними лініями, сторонніми провідниками тощо.

Особливої уваги заслуговують пристрої, прийом інформації з яких можна здійснити із звичайного телефонного апарата. Для цього їх встановлюють або безпосередньо в корпусі телефонного апарата, або підключають до телефонної лінії в телефонній розетці. Подібні пристрої часто називають "телефонним вухом".

У **вібраційних** (або структурних) каналах витоку інформації середовищем поширення акустичних сигналів є не повітря, а конструкції будівель (стіни, стелі, підлоги), труби-конденсатори водо- і теплопостачання, каналізації та інші тверді тіла. В цьому випадку для перехоплення акустичних сигналів використовуються контактні, електронні (з підсилювачем) і радіостетоскопи (при передачі радіоканалом).

Оптико-електронний (лазерний) канал витоку акустичної інформації створюється при опромінюванні лазерним променем вібруючих в акустичному полі таких тонких відзеркалювальних поверхонь, як скло вікон, дзеркал, картин і т.п. При цьому для перехоплення мовної інформації використовуються локаційні системи, відомі як "лазерні мікрофони". Дальність перехоплення складає декілька сотень метрів.

Особливий інтерес викликає перехоплення інформації при її передачі каналами зв'язку. Як правило, в цьому випадку є вільний несанкціонований доступ до сигналів, що передаються.

Залежно від виду каналів зв'язку, технічні канали перехоплення інформації поділяються на електромагнітні, електричні та індукційні.

Електромагнітні випромінювання передавачів засобів зв'язки, що модулюються інформаційним сигналом, можуть перехоплюватися природним чином з використанням стандартних технічних засобів. Цей електромагнітний канал перехоплення інформації широко використовується для прослуховування телефонних розмов, що ведуться по радіотелефону, стільниковому телефону або по радіорелейному та супутниковому зв'язку.

Електричний канал перехоплення інформації, яка передається по кабельних лініях зв'язку, утворюється контактним підключенням до цих ліній. Цей канал найчастіше використовується для перехоплення телефонних розмов, при цьому перехоплювана інформація може бути записана на диктофон або передана по радіоканалу. Подібні пристрої, що підключаються до телефонних ліній зв'язку і містять радіопередавачі для ретрансляції перехопленої інформації, зазвичай називають *телефонними закладками.*

Сучасні індукційні сенсори здатні знімати інформацію з кабелів, які захищені не тільки ізоляцією, а й подвійною бронею із сталевої стрічки і сталевого дроту.

Останнім часом пильну увагу привертають канали витоку графічної інформації у вигляді зображень об'єктів або копій документів, які реалізуються технічними засобами шляхом спостереження за об'єктом, знімання об'єкта і копіювання документів. Залежно від умов спостереження використовуються відповідні технічні засоби, зокрема: оптика (біноклі, підзорні труби, телескопи, монокуляри), телекамери, прилади нічного бачення, тепловізори тощо. Для документування результатів спостереження здійснюється знімання об'єктів, для чого використовуються фотографічні і телевізійні засоби, відповідні умовам знімання. Для зняття копій документів використовуються електронні і спеціальні (закамуфльовані) фотоапарати. Для дистанційного знімання візуальної інформації використовують відеозакладки.

Розглянуті вище методи отримання інформації основані на використанні зовнішніх каналів витоку. Необхідно, проте, коротко зупинитися і на внутрішніх каналах витоку інформації, тим паче, що, зазвичай, їм не приділяють належної уваги.

Внутрішні канали витоку пов'язані, як правило, з адміністрацією і обслуговуючим персоналом, з якістю організації режиму роботи. З них, насамперед, слід відзначити такі канали, як розкрадання носіїв інформації, знімання інформації з погано стертих дискет, використання виробничих і технологічних відходів, візуальне знімання інформації з дисплея і принтера, несанкціоноване копіювання і тому подібне.

Номенклатура технічних засобів комерційної розвідки дуже велика, що робить завдання надійного блокування каналів витоку і несанкціонованого доступу до інформації виключно складним.

Розв'язання подібної задачі можливе тільки з використанням професійних технічних засобів і з залученням кваліфікованих фахівців.

1.10 ПОРУШНИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.10.1 Модель поводження потенційного порушника

Порушенням вважається спроба несанкціонованого доступу або блокування доступу до будь-якої частини інформації, що зберігається, обробляється і передається в ІС.

Оскільки час і місце прояву навмисного порушення передбачити неможливо, то доцільно створити деяку модель поводження потенційного порушника, припускаючи найнебезпечнішу ситуацію:

а) порушник може з'явитися в будь-який час і в будь-якому місці периметра інформаційної системи;

б) кваліфікація і поінформованість порушника може бути на рівні розробників даної системи;

в) порушнику відома інформація про принципи роботи системи;

г) для досягнення своєї мети порушник вибирає найслабшу ланку захисту;

д) порушником може бути не тільки стороння особа, але й законний користувач системи;

е) порушник діє один.

Дана модель дозволяє визначитися з вихідними даними для побудови захисту і сформулювати основні принципи її побудови.

Згідно з п. а необхідно будувати навколо предмета захисту постійно діючий замкнутий контур (чи оболонку) захисту.

Згідно з п. б властивості перешкоди, що складають захист, повинні, по можливості, відповідати очікуваній кваліфікації і поінформованості порушника.

Згідно з п. в для входу в систему законного користувача необхідна змінна секретна інформація, відома тільки йому.

Згідно з п. г підсумкова міцність захисного контуру визначається йогонайслабшою ланкою.

Згідно з п. д при наявності декількох законних користувачів корисно

забезпечити розмежування їхнього доступу до інформації відповідно до повноважень і виконуваних функцій, реалізуючи в такий спосіб принцип найменшої поінформованості кожного користувача з метою скорочення збитку у випадку, якщо має місце безвідповідальність одного з них.

Згідно з п. е як вихідна передумова вважається, що порушник один, оскільки захист від групи порушників – задача більш складна. При цьому під групою порушників розуміється група людей, що виконують одну задачу під загальним керівництвом.

Однак для різних за призначенням і принципами побудови ІС, за видом і цінністю оброблюваної в них інформації найбільш "небезпечна" модель поводження потенційного порушника також може бути різною. Для військових систем це рівень розвідника-професіонала, для комерційних систем – рівень кваліфікованого користувача і т.д. Для медичних систем, наприклад, швидше за все не потрібен захист від побічного електромагнітного випромінювання і наведень, але захист від безвідповідальності користувачів дуже необхідний. Очевидно, що для захисту інформації від більш кваліфікованого й обізнаного порушника потрібно розглянути більшу кількість можливих каналів несанкціонованого доступу (НСД) і застосувати більшу кількість засобів захисту з більш високими показниками міцності.

Виходячи з цього, при виборі вихідної моделі поводження потенційного порушника потрібен диференційований підхід. Оскільки кваліфікація порушника – поняття дуже відносне і наближене, можна взяти за основу чотири класи безпеки.

1-й клас рекомендується для захисту життєво важливої інформації, витік, руйнування чи модифікація якої можуть призвести до великих утрат для користувача. Міцність захисту повинна бути розрахована на порушника-професіонала.

2-й клас рекомендується використовувати для захисту важливої інформації при роботі декількох користувачів, що мають доступ до різних масивів даних чи формують свої файли, недоступні іншим користувачам. Міцність захисту повинна бути розрахована на порушника високої кваліфікації, але не на порушника-професіонала.

3-й клас рекомендується для захисту відносно цінної інформації, постійний несанкціонований доступ до якої шляхом її нагромадження може призвести до витоку і більш цінної інформації. Міцність захисту при цьому повинна бути розрахована на відносно кваліфікованого порушника-непрофесіонала.

4-й клас рекомендується для захисту іншої інформації, що не цікавить серйозних порушників. Однак його необхідність диктується дотриманням технологічної дисципліни обліку й обробки інформації службового користування з метою захисту від випадкових порушень у результаті безвідповідальності користувачів і деякого підстрахування від випадків навмисного НСД.

Реалізація перерахованих рівнів безпеки повинна забезпечуватися набором відповідних засобів захисту, що перекривають певну кількість можливих каналів НСД відповідно до очікуваного класу потенційних порушників. Рівень безпеки захисту усередині класу забезпечується кількісною оцінкою міцності окремих засобів захисту й оцінкою міцності контуру захисту від навмисного НСД.

1.10.2 Класифікація порушників

Однією з найпоширеніших загроз безпеці є порушники, зазвичай називані хакерами (hacker) чи зломщиками (cracker). Існує така класифікація порушників.

- **Імітатор** (masquerader). Особа, що не має права користування комп'ютером, але подолала механізм керування доступом і використовує права доступу деякого легального користувача.
- **Правопорушник** (misfeasor). Легальний користувач, що намагається одержати доступ до даних, програм чи ресурсів, не маючи на це прав доступу, або користувач, що має у своєму розпорядженні відповідні права доступу, однак використовує їх у зловмисних цілях.
- **Таємний користувач** (clandestine user). Особа, що заволоділа правами керування системою і використовує ці права для обходу засобів аудиту і керування доступом або для створення перешкод у реєстрації системних подій.

Імітаторами найчастіше бувають зовнішні користувачі, правопорушниками звичайно є внутрішні користувачі, а таємними користувачами можуть виявитися як ті, так і інші.

Справжній хакер з першого погляду на дівчину в барі знає її ім'я, номер телефону, IP-адресу та чи відкриті в неї порти.

За рівнем небезпеки атаки порушників можуть бути як незначними, так і цілком серйозними. До незначних порушень відносять спроби тих, хто намагається одержати доступ до відповідного мережевого середовища просто з особистої цікавості. До серйозних за рівнем небезпеки порушень відносять дії осіб, що намагаються читати секретні дані, виконувати несанкціоновані зміни даних чи здійснювати дії, що призводять до ушкодження системи.

З порушниками, що не мають злого наміру, можна було б примиритися, хоча і такі порушники споживають ресурси і тим самим знижують продуктивність системи для легальних користувачів. Проблема в тім, що не існує методів, які дозволяють однозначно з'ясувати, є порушник зловмисником, чи ні. Тому навіть для систем, не призначених для зберігання особливо важливих даних, має сенс тримати дану проблему під контролем.

1.10.3 Методика вторгнення

Метою порушника є одержання доступу до системи чи розширення прав, наданих йому системою на законній підставі. Для цього порушнику, як правило, потрібно роздобути інформацію, що має бути захищеною. В більшості випадків ця інформація представлена у формі пароля користувача. Знаючи пароль деякого іншого користувача, порушник може ввійти в систему під його ім'ям і одержати всі привілеї, які має цей користувач.

Зазвичай в системі є файл, що зв'язує паролі з іменами легальних користувачів. Якщо цей файл не захищений, то нескладно одержати до нього доступ і довідатися паролі, що зберігаються в ньому. Файл паролів може захищатися одним з двох способів.

Однобічне шифрування. Система зберігає пароль користувача тільки в шифрованому вигляді. Коли користувач уводить свій пароль, система шифрує введений пароль і порівнює результат з тим значенням, що зберігається у файлі паролів. На практиці система звичайно виконує однобічне (необоротне) перетво-

рення, в якому пароль служить для генерування ключа функції шифрування.

Керування доступом. Доступ до файлу паролів дозволяється лише одному або невеликій кількості користувачів.

Якщо використовується хоча б один з цих контрзаходів, то потенційному порушнику доведеться докласти значних зусиль, щоб довідатися паролі.

Відомі такі методи одержання паролів.

1. Перевірка паролів за замовчуванням для стандартних облікових записів, що поставляються із системою. Багато адміністраторів мало уваги приділяють зміні встановлених за замовчуванням значень.

2. Перебір усіх коротких паролів (від одного до трьох символів).

3. Перевірка слів із системного словника чи зі списку найбільш ймовірних паролів. Список останніх завжди можна знайти на електронних дошках оголошень хакерів.

4. Збирання інформації про користувачів, включаючи їхні повні імена, імена їхніх дружин (чоловіків) і дітей, назви картин і фотографій на робочих місцях і навіть назви їхніх улюблених книг, за якими можна судити про їхні захоплення.

5. Перевірка як паролів телефонних номерів і номерів кімнат користувачів.

6. Перевірка як паролів усіх можливих для даної області номерних знаків автомобілів.

7. Використання "троянського коня", щоб обійти обмеження доступу.

8. Підключення до лінії зв'язку між користувачем і головним вузлом.

У багатьох фірмах через постійну чехарду із забутими паролями розсудливі мережеві адміністратори вводять один-єдиний пароль для всіх користувачів. Оскільки користувачі забувають і його, пароль великими літерами написано на аркуші А4, прикріпленому до дошки оголошень.

"Посібник з комп'ютерної безпеки й захисту інформації"
Карл Абрахам Шкафиц II

Підбор паролів є ефективним методом тільки в тих випадках, коли він може виконуватися в автоматичному режимі і без загрози виявлення факту підбору пароля.

Атака, що базується на використанні "троянських коней", є достатньо ефективною, оскільки її виявлення є досить складною задачею.

Непривілейований користувач створив ігрову програму і запропонував її системному оператору для розваги у вільний час. Програма дійсно була грою, але під час роботи вона також копіювала файл паролів, що зберігався в незашифрованому вигляді і захищений лише за допомогою системи розмежування доступу, у файл користувача, що є автором програми. Оскільки гра працювала в режимі доступу привілейованого користувача, то програма могла одержати необмежений доступ до файлу паролів.

Восьмий тип атаки, що полягає в підключенні до лінії зв'язку, відносять до галузі питань забезпечення фізичного захисту системи. У випадку таких атак можливим методом протидії є шифрування в каналі зв'язку.

1.11 УМОВИ, ЩО СПРИЯЮТЬ НЕПРАВОМІРНОМУ ОВОЛОДІННЮ КОНФІДЕНЦІЙНОЮ ІНФОРМАЦІЄЮ

Неправомірному оволодінню конфіденційною інформацією сприяють такі умови:

- розголошення (зайва балакучість співробітників) – 32%;
- несанкціонований доступ шляхом підкупу і схилення до співробітництва з боку конкурентів і злочинних угруповань – 24%;
- відсутність на фірмі належного контролю і жорстких умов забезпечення інформаційної безпеки – 14%;
- традиційний обмін виробничим досвідом – 12%;
- безконтрольне використання інформаційних систем – 10%;
- наявність передумов виникнення серед співробітників конфліктних ситуацій – 8%,
- а також відсутність високої трудової дисципліни, психологічна несумісність, випадковий підбор кадрів, слабка робота кадрів у напрямку згуртованості колективу.

Серед форм і методів **несумлінної конкуренції** найбільше поширення знаходять:

- економічне придушення, що полягає у зриві угод (48%), паралізації діяльності фірми (31%), компрометації фірми (11%), шантажі керівників фірми (10%);
- фізичне придушення: пограбування і розбійні напади на офіси, склади, вантажі (73%), загрози фізичної розправи над керівниками фірми і провідними спеціалістами (22%), вбивства і захоплення заручників (5%);
- інформаційний вплив: підкуп співробітників (43%), копіювання інформації (24%), проникнення в бази даних (18%), продаж конфіденційних документів (10%), підслуховування телефонних переговорів і переговорів у приміщеннях (5%), а також обмеження доступу до інформації, дезінформація;
- фінансове придушення (інфляція, бюджетний дефіцит, корупція, розкрадання фінансів, шахрайство);
- психічний тиск (може виражатися у вигляді хуліганських витівок, загрози і шантажу).

Кожній з умов неправомірного оволодіння конфіденційною інформацією можна поставити у відповідність певні канали, способи захисних дій і класи засобів захисту чи протидії.

1.12 ІНФОРМАЦІЙНІ ЗАГРОЗИ В ГАЛУЗІ ЕКОНОМІКИ

Впливу інформаційних загроз у сфері економіки найбільш піддані:

- система державної статистики;
- кредитно-фінансова система;
- інформаційні й облікові автоматизовані системи державних органів виконавчої влади, що забезпечують діяльність суспільства й держави у сфері економіки;
- системи бухгалтерського обліку підприємств, установ і організацій незалежно від форм власності;
- системи збирання, оброблення, зберігання й передачі даних фінансової, біржової, податкової, митної й зовнішньоекономічної діяль-

ності держави, а також підприємств, установ і організацій незалежно від форм власності.

Крім того, серйозною загрозою для нормального функціонування економіки в цілому є комп'ютерні злочини, пов'язані з проникненням у комп'ютерні системи й мережі банків та інших кредитних організацій. Все це призводить до реального збитку в діяльності суб'єктів господарської діяльності, що для держави виражається в недоодержанні податкових платежів у бюджет і погіршенні економічних показників.

Увесь світ серйозно стурбований станом захисту національних інформаційних ресурсів внаслідок можливості широкого, неконтрольованого доступу до них через відкриті інформаційні мережі. Більше 80% комп'ютерних злочинів відбуваються з використанням глобальної мережі Інтернет. У звіті «Дослідження в галузі інформаційної безпеки в Росії й СНД» в 2001 році компанія «Ернст і Янг» навела дані, що відображені в табл. 1.1.

Таблиця 1.1 – Статистика загроз інформаційній безпеці

Види загроз	**Частота виявлення, %**
Вірусні атаки	43
Відмова в обслуговуванні	15
Проникнення в систему ззовні	14
Несанкціонований доступ у самій компанії	11
Викрадення комп'ютера	7
Порушення цілісності даних або мереж	5
Фінансове шахрайство	3
Викрадення комерційної інформації	2

Усі ці загрози стосуються систем електронної торгівлі.

Електронна комерція – це укладання і виконання угод в електронній формі, що спричиняє необхідність вирішення питань її правового, фінансового, організаційного, інформаційного й технічного забезпечення. Електронна торгівля містить у собі замовлення товарів і їх оплату з використанням мережі Інтернет, що є частиною електронної комерції.

У цей час одержали розвиток дві моделі глобальної електронної комерції: B2B (business-to-business) - торговельні відносини між підприємствами й B2C (business-to-customer) - торговельні відносини між підприємством і покупцем.

Електронна комерція поєднує безліч різних функцій. У ній використовуються нові технології для організації контакту покупців і продавців, методів подання, обговорення й формування замовлення, визначення умов угоди, порядку продажу товарів і послуг, а також для процесу здійснення платежів.

Процес електронної комерції в узагальненому вигляді складається з таких етапів:

- вибір продукту або послуги на сервері компанії й оформлення замовлення;
- внесення замовлення в базу даних магазину;
- перевірка доступності замовленого продукту через центральну базу даних;
- повідомлення про неможливість своєчасної поставки замовлення й про його корекцію при відсутності замовленого товару;
- підтвердження замовлення і його розміщення в базі даних на виконання при наявності замовленого товару;
- оплата клієнтом замовлення в режимі реального часу;
- поставка замовленого товару клієнтові.

Вирішення проблеми забезпечення економічної безпеки електронної комерції в першу чергу пов'язане з вирішенням питань захисту інформаційних технологій, застосовуваних у ній, тобто із забезпеченням інформаційної безпеки.

У наш час існує безліч програмних рішень для організації електронного бізнесу. В Україні розвиток електронної комерції стримується:

- недостатньо розвиненою інформаційно-комунікаційною інфраструктурою;
- її високою вразливістю для зловмисників;
- наростаючим ступенем конкурентної боротьби.

Як видно, всі перераховані перешкоди стосуються сфери інформаційної безпеки. На жаль, керівники підприємств електронної комерції належною мірою починають усвідомлювати серйозність інформаційних загроз і важливість організації захисту своїх ресурсів тільки після того, як останні піддаються інформаційним атакам.

Компанію, що здійснює електронну комерцію, на кожному етапі підстерігають такі загрози:

- підміна web-сторінки сервера електронного магазину (переадресація запитів на інший сервер), що робить доступними відомості про клієнта, особливо про його кредитні карти, стороннім особам;
- створення помилкових замовлень і різноманітні форми шахрайства з боку співробітників електронного магазину, наприклад, маніпуляції з базами даних (статистика свідчить про те, що більше половини комп'ютерних інцидентів пов'язано з діяльністю власних співробітників);
- перехоплення даних, переданих мережами електронної комерції;
- проникнення зловмисників у внутрішню мережу компанії й компрометація компонентів електронного магазину;
- реалізація атак типу »відмова в обслуговуванні» і порушення функціонування або виведення з ладу вузла електронної комерції.

У результаті реалізації таких загроз компанія втрачає довіру клієнтів, втрачає гроші від потенційних і/або недосконалих угод, порушується діяльність електронного магазину, витрачаються час, гроші й людські ресурси на відновлення функціонування.

2000-й рік був ознаменований випадками масового виходу з ладу провідних серверів електронного бізнесу, діяльність яких носить загальнонаціональний характер: Yahoo!, eBay, Amazon, Buy, CNN, ZDNet, Datek і E*Trade. Розслідування, проведене ФБР, показало, що зазначені сервери вийшли з ладу через багаторазове зростання кількості спрямованих на їх адресу запитів на обслуговування в результаті реалізованих DoS-атак. Наприклад, потоки запитів на сервер Buy перевищили середні показники в 24 рази, а граничні – в 8 разів. За різними оцінками, економічний збиток, понесений американською економікою від цих акцій, склав близько 1,5 млрд. доларів.

Звичайно, загрози, пов'язані з перехопленням переданої через Інтернет інформації, властиві не тільки сфері електронної комерції. Однак особливість її систем полягає в тому, що в них передаються і зберігаються відомості, які мають важливе економічне значення: номери кредитних карток, номери рахунків, зміст договорів і т.п.

Вирішенням проблеми інформаційної безпеки електронного бізнесу займається незалежний консорціум - Internet Security Task Force (ISTF) - громадська організація, до складу якої входять представники та експерти компаній-постачальників засобів інформаційної безпеки, електронного бізнесу і провайдери інтернет-послуг.

Консорціум ISTF виділяє такі складові інформаційної безпеки, на яких у першу чергу повинна бути зосереджена увага організаторів електронного бізнесу:

- механізм об'єктивного підтвердження ідентифікувальної інформації;
- право на персональну, приватну інформацію;
- визначення подій безпеки;
- захист корпоративного периметра;
- визначення атак;
- контроль потенційно небезпечного вмісту;
- контроль доступу;
- адміністрування;
- реакція на події.

Від захисту перерахованих складових залежить безперервність бізнесу з усіма економічними наслідками, що випливають звідси. Безпека більше не є додатковим аспектом бізнесу: адже навіть надійність системи на рівні 97% означає, що за рік для бізнесу будуть загублені 293 години.

Безумовно, забезпеченням інформаційної безпеки повинні займатися фахівці в даній галузі, але керівники органів державної влади, підприємств і установ незалежно від форм власності, відповідальні за економічну безпеку тих або інших господарських суб'єктів, повинні постійно тримати дані питання в полі свого зору.

1.13 ІНФОРМАЦІЙНА БОРОТЬБА ТА ВІЙНА

Існують певні взаємозв'язки між поняттям «інформаційна безпека» і поняттями «інформаційна боротьба» та «інформаційна війна», які останнім часом усе частіше згадуються у засобах масової інформації.

Поняття «інформаційна війна» виникло як наслідок інтенсивної інформатизації суспільства.

У даний час відбувається глобальна інформаційно-культурна і інформаційно-ідеологічна експансія Заходу, здійснювана за допомогою Інтернет і засобів масової інформації. Багато країн змушені вживати спеціальних заходів для захисту своїх громадян, своєї культури, традицій і духовних цінностей від чужого інформаційного впливу. Виникає необхідність захисту національних інформаційних ресурсів і збереження конфіденційності інформаційного обміну світовими відкритими мережами, оскільки на цьому ґрунті можуть виникати політична і економічна конфронтації держав, нові кризи в міжнародних відносинах.

«Інформаційна революція» створила абсолютно новий економічний сектор, якого раніше не було. Це провокує зростання інтенсивності конфліктів з метою захоплення та утримання переваги в даному секторі нової світової економіки. Капіталом, який грає головну роль в «інформаційній революції», є інтелектуальний капітал, перш за все в галузі інформаційних технологій. І нарешті, основний продукт цього сектора – інформація – має унікальні властивості, яких не має у інших секторів економіки. Інформація на відміну від усіх інших ресурсів придатна для багатократного використання і для багаточисельних користувачів, при цьому чим більше вона застосовується, тим більш коштовною стає. Те ж саме можна сказати про мережі, що зв'язують різні джерела інформації.

Поняття «інформаційна боротьба» найповніше розкривається в таких взаємопов'язаних означеннях:

Інформаційна боротьба – це об'єктивно існуюча форма прояву відносин між суб'єктами при вирішенні ними завдань, що містять елементи конфліктності різної природи на інформаційному рівні.

Інформаційна боротьба – це наука про механізми, прийоми, методи і засоби інформаційного протиборства.

Інформаційна боротьба – це комплекс заходів, спрямованих на вирішення завдань, що стоять перед суб'єктом, методами і засобами боротьби.

Існування інформаційної боротьби обумовлене як існуванням інформації, так і природністю процесу її використання, її властивостей для вирішення різних завдань. Із визначення інформаційної боротьби випливає, що вона, за своєю суттю, неагресивна. До її методів і засобів вдаються, наприклад, з метою обґрунтування доцільності впровадження у виробництво певних технологічних рішень. Як об'єктивно існуючий феномен інформаційна боротьба має свої цілі, завдання, закономірності, способи, методи і засоби її ведення.

Метою інформаційної боротьби є забезпечення переваги у вирішенні певних завдань однієї сторони над іншою за рахунок досягнення вищості на інформаційному рівні. Цієї мети можна досягти різними шляхами.

Цілеспрямоване добування інформації про поточну ситуацію з жорсткими вимогами щодо її своєчасності, якості, обсягу, повноти і темпів оновлення, оцінювання на основі цієї інформації політичної (військово-політичної, військової, економічної, екологічної та ін.) ситуації. Вирішення цього комплексу завдань ускладнюється тим, що воно здійснюється в умовах інформаційної протидії. При цьому інформація, що аналізується, відзначається непевністю об'єктивного і суб'єктивного характеру, неповнотою щодо одних аспектів і надмірністю щодо інших, суперечливістю, наявністю частково зруйнованої та спотвореної інформації, у тому числі і дезінформації.

Цілеспрямований і комплексний вплив на свідомість, інформаційні ресурси країни на всіх етапах їхнього виробництва, поширення і використання, а також на інфосферу машинно-технічних систем протиборчої (конкуруючої) сторони з метою нав'язування «бажаних» рішень і «керування поведінкою». При цьому особливої важливості набуває не стільки руйнівна, скільки цілеспрямована впливова дія щодо спотворення змісту інформації для забезпечення своїх інтересів у різних сферах діяльності особистості, суспільства, держави.

Захист власних інформаційних ресурсів та інфосфери машинно-технічних систем від впливу на них протиборчої сторони. При цьому важливим є не тільки технічний захист інформації, спрямований в основному на забезпечення її конфіденційності, але й набуває особливої значимості захищеність змісту інформації від навмисного його спотворення або зміни і механізми виявлення дезінформації. До цього ж комплексу входять також і завдання відновлення цілісності змісту частково зруйнованої або спотвореної текстової природно-мовної інформації.

Соціальними об'єктами інформаційної боротьби є свідомість і підсвідомість індивіда, колективна свідомість соціальної групи, суспільства, держави, а також інформаційні ресурси та інфосфера машинно-технічних систем.

«Інформаційна війна» в багатьох джерелах тлумачиться як комплекс заходів і операцій, здійснюваних у конфліктних ситуаціях, коли інформація є водночас зброєю, ресурсом і ціллю. Ця війна може вестися як у воєнний, так і в мирний час.

Закономірним є питання про те, якою мірою реальна і наскільки загрожує національним інтересам інформаційна війна. Принадність використання методів і способів ведення інформаційної війни для забезпечення національних інтересів обумовлена можливістю її ведення в мирний час, економічною вигідністю, скритністю, у тому числі і безпосередніх ініціаторів війни. Досить звернути увагу на такі офіційні документи, як «Стратегія національної безпеки США на 1994 і 1996 рр.», «Національна військова стратегія Сполучених Штатів Америки, 1995 р.», у яких способи і методи ведення інформаційної війни розглядаються як один з найбільш ефективних засобів забезпечення національних інтересів США в різних регіонах світу.

Україна, в силу її геополітичного розташування, є об'єктом інтересів багатьох розвинутих держав, що зумовлює велику вірогідність втягування її в інформаційну війну.

Враховуючи вищесказане, головною інформаційною загрозою національній безпеці України є загроза інформаційного впливу іншої сторони на свідомість, підсвідомість, інформаційні ресурси та інфосферу машинно-технічних систем; нав'язування особистості, суспільству, державі бажаної (для іншої сторони) системи цінностей, поглядів, інтересів, рішень у життєво важливих сферах суспільної і державної діяльності, керування їх поведін-

кою і розвитком у бажаному для іншої сторони напрямі.

У цьому контексті особливо актуальною є проблема безпеки при інформаційно-аналітичному забезпеченні органів державного управління, її технологічних аспектів. Останнім часом сформувалося поняття «інформаційного фантома в управлінні», сутність якого полягає в істотному підвищенні ролі аналітиків і радників у державному управлінні. Від якості підготовлених ними аналітичних документів (інформаційно-аналітичних оглядів, довідок), адекватності реальній ситуації останніх залежить ефективність прийнятих на їх основі рішень державного рівня. З іншого боку, уявлення про поточну ситуацію, сформоване інформаційно-аналітичними підрозділами різних рівнів з привнесенням у нього елементів суб'єктивності, здатне до саморозвитку й, у свою чергу, впливає на розвиток процесів у суспільстві і державі. Природно, що цей вплив може бути як позитивним, так і негативним. Крім того, це уявлення може бути сформоване на інформації, що містить як спотворену і помилкову інформацію, так і цілеспрямовану дезінформацію.

Основними об'єктами дій в інформаційній війні є:

- мережі зв'язку та інформаційно-обчислювальні мережі, використовувані державними організаціями при виконанні своїх управлінських функцій;
- військова інформаційна інфраструктура, що вирішує завдання управління військами;
- інформаційні та управлінські структури банків, транспортних і промислових підприємств;
- ЗМІ (в першу чергу, електронні).

Розрізняють 7 різновидів інформаційної війни:

- командно-управлінська;
- розвідувальна;
- психологічна;
- хакерська;
- економічна;
- електронна;
- кібервійна.

Командно-управлінська (Command-and-control) війна як основний об'єкт дії розглядає канали зв'язку між командуванням і виконавцями. Перерізаючи «шию» (канали зв'язку), нападаючий ізолює «голову» від «тулуба». Вважається, що це краще, ніж просто вбивати «голову». Інтернет народився як оборонний варіант цієї війни («розосереджена шия»).

Розвідувальна війна має на меті збір важливої військової інформації і захист власної.

Електронна війна об'єктом своєї дії має засоби електронних комунікацій – радіозв'язку, радарів, комп'ютерних мереж. Її важлива складова – криптографія, що дозволяє здійснювати шифрування і розшифрування електронної інформації.

Психологічна війна – здійснюється шляхом пропаганди, «промивання мозків» й іншими методами інформаційної обробки населення. Виділяють 4 складові психологічної війни: підривання цивільного духу; деморалізація озброєних сил; дезорієнтація командування; війна культур (Kulturkampf).

Хакерська війна має метою тотальний параліч мереж, перебої зв'язку, введення помилок в дані, що пересилаються, розкрадання інформації, розкрадання послуг за рахунок несанкціонованих підключень до мереж, їх таємний моніторинг, несанкціонований доступ до закритих даних. Для досягнення цих цілей використовуються різні програмні засоби: віруси, «троянські коні», «логічні бомби» та ін.

Економічна інформаційна війна. Розглядаються дві її форми – інформаційна блокада та інформаційний імперіалізм.

Негативний вплив на людину досягається такими видами інформаційної зброї:

- засоби пропагандистсько-психологічного впливу (через пресу, телебачення, радіо, Інтернет, інші канали);

Фактично кожна заява світових лідерів, розповсюджена засобами масової інформації, спричиняє коливання на світових біржах, що призводить до коливання цін на нафту, основних показників фондових бірж тощо.

- засоби психологічного впливу (голографічні зображення в атмосфері, синтезатори голосів відомих лідерів, «вірус-вбивця» № 666 та ін.);

Під час першої війни в районі Перської затоки одночасно 15 тисяч військових бачили на небі хрест, який було створено як голографічне зображення в атмосфері. Це було сприйнято як символ «правильної» війни («Бог з нами») і швидкої перемоги.

- психотронна зброя (психотронні генератори, методи парапсихології та біоенергоінформатики, програмування поведінки (зомбування) особистості тощо);
- психотропні препарати.

Хронологія багатьох військових конфліктів останніх років включала, як правило, на початку їх розвитку етап психологічної обробки світової громадськості через ЗМІ.

При підготовці другої війни в районі Перської затоки США переконали світову громадськість у необхідності заходів, що вживаються коаліційним керівництвом. Основне навантаження в зв'язку з цим лягло на друковані видання, радіо і телебачення. Вони поширювали чутки про наявність в Іраку величезних запасів хімічної зброї, а також про плани їх можливого використання, повідомляли завищені дані про чисельність іракських озброєних сил, про підтримку режимом Хусейна ряду терористичних організацій і тому подібне.

Психотронні генератори – це пристрої, що здійснюють дію на людину шляхом передачі інформації через позачуттєве (неусвідомлюване) сприйняття.

Вже давно встановлено, що різні органи людини мають власні резонансні частоти, використовуючи які можна впливати на психофізіологічний стан індивіда або колективу людей, викликаючи у них страх, пригніченість або інші відчуття.

Психотропні препарати – це лікарські (наркотичні) засоби, які здатні викликати стан залежності, стимулювально або депресивно діяти на центральну нервову систему, викликаючи галюцинації або порушення мо-

торної функції організму, під впливом яких відбувається порушення мислення, змінюється настрій, поведінка.

Виробництво і управління, оборона і зв'язок, транспорт і енергетика, фінанси, наука і освіта, засоби масової інформації – все залежить від інтенсивності інформаційного обміну, повноти, своєчасності, достовірності інформації. Саме інформаційна інфраструктура суспільства є другою мішенню інформаційної зброї.

При цьому дія інформаційної зброї спрямована на:

- знищення, спотворення або розкрадання інформаційних масивів;
- подолання систем захисту;
- обмеження допуску законних користувачів;
- придушення інформаційного обміну в телекомунікаційних мережах;
- фальсифікацію інформації в каналах державного і військового управління;
- дезорганізацію роботи технічних засобів та комп'ютерних систем.

Усе це досягається:

- засобами програмно-математичного впливу (комп'ютерні віруси, логічні «бомби», засоби придушення комп'ютерних мереж тощо);
- засобами, заснованими на впливі полів різної природи (радіоелектронне придушення, акустична зброя, електромагнітні ураження).

Універсальність, прихованість, багатоваріантність форм програмно-апаратної реалізації, радикальність дії, можливість вибору часу та місця застосування, економічність роблять інформаційну зброю надзвичайно небезпечною, оскільки вона легко маскується під засоби захисту (наприклад, інтелектуальної власності) і навіть дозволяє вести наступальні дії анонімно, без оголошення війни.

КОНТРОЛЬНІ ПИТАННЯ

1. Охарактеризуйте поняття інформації в різних галузях діяльності.
2. Назвіть та охарактеризуйте основні задачі інформаційної безпеки.
3. Охарактеризуйте тенденції розвитку комп'ютерної злочинності.
4. Наведіть характерні приклади порушення ІБ.
5. Охарактеризуйте поняття системи захисту інформації.
6. Сформулюйте основні вимоги до захисту інформації.
7. Сформулюйте основні вимоги до системи захисту інформації.
8. Назвіть види забезпечення системи захисту інформації.
9. Назвіть основні компоненти моделі безпеки інформації.
10. Дайте означення поняття "загроза".
11. Наведіть класифікацію загроз ІБ.
12. Охарактеризуйте основні загрози доступності.
13. Охарактеризуйте основні загрози цілісності.
14. Наведіть характеристику основних загроз конфіденційності.
15. Назвіть види шкідливого програмного забезпечення.
16. Яку інформацію відносять до держаної таємниці?
17. На які сфери розповсюджується державна таємниця на інформацію?
18. Яку інформацію забороняється відносити до держаної таємниці?
19. Яка інформація складає комерційну таємницю?
20. Опишіть загрози конфіденційній інформації.
21. Назвіть дії, що призводять до неправомірного оволодіння конфіденційною інформацією.
22. Назвіть умови, що сприяють неправомірному оволодінню конфіденційною інформацією.
23. Дайте означення поняття "технічний канал витоку інформації".
24. Наведіть розповсюджені канали витоку інформації.
25. Назвіть основні електромагнітні канали витоку інформації.
26. Назвіть основні електричні канали витоку інформації.

27. Охарактеризуйте повітряні канали витоку інформації.
28. Охарактеризуйте електроакустичні канали витоку інформації.
29. Охарактеризуйте оптико-електронні канали витоку інформації.
30. Опишіть модель поводження потенційного порушника.
31. Назвіть і охарактеризуйте класи безпеки.
32. Наведіть класифікацію порушників.
33. Опишіть можливі методики вторгнення в інформаційну систему.
34. Опишіть особливості інформаційної війни.
35. Назвіть основні види інформаційної зброї.

Не знання законів не звільняє від відповідальності. Знання – може.
Народна мудрість

2.1 ОСНОВНІ ПОНЯТТЯ ЗАКОНОДАВЧОГО РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Більшість людей не здійснюють протиправних дій не тому, що це технічно неможливо, а тому, що це засуджується та/або карається суспільством, тому, що так чинити не прийнято. Тобто, для людини важливими є моральні та правові аспекти її вчинків і дій. Правовий захист інформації визначає структуру та особливості законодавчого рівня інформаційної безпеки.

На законодавчому рівні розрізняють дві групи заходів:

- заходи, спрямовані на створення і підтримку в суспільстві негативного (зокрема, із застосуванням покарань) ставлення до порушень і порушників ІБ (заходи обмежувальної спрямованості);
- заходи, що сприяють підвищенню освіти суспільства у галузі ІБ і допомагають у розробці і розповсюдженні засобів забезпечення ІБ (заходи творчої спрямованості).

На практиці обидві групи заходів важливі в рівній мірі, але окремо виділяється аспект усвідомленого дотримання норм і правил ІБ. Це важливо для всіх суб'єктів інформаційних відносин, оскільки розраховувати тільки на захист силами правоохоронних органів було б наївно. Необхідно це і тим, в чиї обов'язки входить карати порушників, оскільки забезпечити довідність при розслідуванні і судовому розгляді комп'ютерних злочинів без спеціальної підготовки неможливо.

Найважливіше (і, ймовірно, найважче) на законодавчому рівні – створити механізм, що дозволяє погоджувати процес розробки законів з реаліями і прогресом інформаційних технологій. Закони не можуть випереджати життя, але важливо, щоб відставання не було дуже великим, оскільки на практиці, крім інших негативних моментів, це веде до зниження інформаційної безпеки.

Право – це сукупність загальнообов'язкових правил і норм поводження, встановлених чи санкціонованих державою для певних сфер життя і діяльності державних органів, підприємств (організацій) і населення (окремої особистості).

Правовий захист інформації як ресурсу визнаний на міжнародному і державному рівнях, а також визначається *міждержавними договорами, конвенціями, деклараціями* і реалізується *патентами, авторським правом і ліцензіями* на її захист. На державному рівні правовий захист регулюється державними і відомчими актами.

У нашій країні такими правилами (актами, нормами) є Конституція, закони України, цивільне, адміністративне, карне право, викладені у відповідних кодексах.

Що стосується **відомчих нормативних актів**, то вони визначаються *наказами, посібниками, положеннями й інструкціями*, що видаються відомствами, організаціями і підприємствами, які діють у рамках визначених структур.

Сучасні умови вимагають і визначають необхідність комплексного підходу до формування законодавства із захисту інформації, його складу і змісту, співвіднесення його з усією системою законів і правових актів України.

2.2 ДЕРЖАВНА ІНФОРМАЦІЙНА ПОЛІТИКА УКРАЇНИ

Концептуальні засади державної політики України в інформаційній сфері формуються, виходячи з національних інтересів країни, збалансовуючи інтереси особистості, суспільства і держави.

Інтереси особистості в інформаційній сфері вимагають забезпечення конституційних прав людини і громадянина на доступ до інформації, на використання інформації при незабороненій законом діяльності в інтересах фізичного, духовного та інтелектуального розвитку особи, а також захисту інформації персонального характеру та захисту від інформації, що завдає шкоду особистості.

Інтереси суспільства в інформаційній сфері полягають у забезпеченні інтересів особистості у цій сфері, закріпленні демократії, створенні правової

соціальної держави, досягненні та підтриманні суспільної злагоди, духовного оновлення.

Інтереси держави в інформаційній сфері полягають у створенні умов для динамічного розвитку національної інформаційної інфраструктури, забезпечення конституційних прав людини і громадянина щодо отримання й використання інформації, для підтримання конституційного ладу, суверенітету, територіальної цілісності України, політичної, економічної, соціальної стабільності, гарантованого забезпечення законності й правопорядку, розвитку рівноправного і взаємовигідного міжнародного співробітництва, забезпечення інформаційної безпеки.

Концептуальні засади інформаційної політики визначають методи та форми впливу на такі об'єкти інформаційної сфери:

- система формування і використання інформаційних ресурсів;
- інформаційно-телекомунікаційна інфраструктура;
- ринок інформаційних і телекомунікаційних засобів, інформаційних продуктів і послуг;
- науково-технічні й виробничі кадри; системи забезпечення інформаційної безпеки;
- система нормативно-правового регулювання інформаційних відносин, освітні програми; міжнародне співробітництво.

Держава активно сприяє формуванню інформаційного права в Україні як сукупності норм різних галузей права, які регулюють відносини, пов'язані з інформацією, інформаційними технологіями та комунікаціями.

Інформаційне право будується на принципах інформаційної відкритості, прозорості в діяльності державних установ та інших юридичних осіб, гарантованості інформаційної безпеки особистості, суспільства, держави.

Інформаційне законодавство регулює протиріччя між потребами суспільства у розширенні вільного обміну інформацією та окремими обмеженнями на її поширення.

Інформаційне законодавство визначає процедури та умови, за яких повинен здійснюватися доступ до інформації комерційних структур, до персональної інформації та її поширення.

В Україні політика забезпечення інформаційної безпеки будується на таких засадах:

- обмеження доступу до інформаційного ресурсу є винятком із загального принципу відкритості інформації й реалізується тільки відповідно до чинного законодавства;
- відповідальність за збереження інформації, її засекречування і розсекречування персоніфікується;
- доступ до будь-якого інформаційного ресурсу так само, як і обмеження доступу, реалізується з урахуванням визначених законом прав власності на цей ресурс;
- держава формує нормативно-правову базу, регламентуючи права, обов'язки і відповідальність усіх суб'єктів, діючих в інформаційному просторі;
- суб'єкти, які збирають, накопичують і обробляють персональні дані й конфіденційну інформацію, несуть відповідальність перед законом за збереження і використання;
- держава забезпечує захист суспільства від хибної, викривленої і недостовірної інформації, що надходить через засоби масової інформації;
- держава реалізує контроль за створенням і використанням засобів захисту інформації шляхом їхньої обов'язкової сертифікації та ліцензування діяльності в галузі захисту інформації;
- держава підтримує діяльність вітчизняних виробників продуктів і технологій, засобів інформатизації та захисту інформації, вживає заходів щодо захисту внутрішнього ринку від проникнення неякісних засобів інформатизації, інформаційних продуктів і технологій;
- держава сприяє доступу громадян до світових інформаційних ресурсів, глобальних інформаційних мереж;
- держава формує і забезпечує виконання національної програми інформаційної безпеки, яка об'єднує зусилля всіх зацікавлених суб'єктів щодо створення єдиної системи інформаційної безпеки України;

- держава забезпечує цілісність інформаційного простору України;
- держава сприяє всебічному розвитку української мови як основного інструменту перетворення накопичених людством знань в інформаційний ресурс України.

Державна інформаційна політика сьогодні спрямована на забезпечення належних правових, економічних, внутрішньо- і зовнішньополітичних, організаційних та інших умов. Всі ці умови необхідні для:

- створення розвиненої та захищеної інформаційної інфраструктури України;
- розвитку міжнародного співробітництва в інформаційній сфері та утвердження України як країни з інформаційним суспільством;
- забезпечення безпеки інформаційної діяльності, життєво важливих інтересів особи, суспільства та держави в інформаційній сфері.

Суттєвим для інформаційної політики будь-якої держави є дотримання балансу інтересів особистості, суспільства і держави. Держава повинна забезпечувати відкритість та поінформованість суспільства про діяльність її органів і суспільних інститутів в інформаційній сфері.

У *сфері інформаційної безпеки* державна інформаційна політика спрямована на:

- захист населення України від інформаційної продукції, яка загрожує його фізичному, інтелектуальному, морально-психологічному здоров'ю (пропаганда жорстокості, насильства, людиноненависності, порнографії, окультизму, вплив на свідомість тощо);
- всебічне сприяння інформаційному забезпеченню правоохоронних відомств для виконання ними своїх функцій;
- охорону державної таємниці та іншої інформації з обмеженим доступом, а також здійснення державного контролю за режимом доступу до цієї інформації.

Важливою сьогодні є розробка збалансованих вітчизняних стандартів у галузі інформатизації і забезпечення інформаційної безпеки автоматизованих систем управління, інформаційних і телекомунікаційних систем загального і спеціального призначення; прийняття і реалізація державних програм підвищення рівня правової культури і комп'ютерної грамотності; створення

системи освіти і працевлаштування фахівців для забезпечення потреб інформаційної сфери.

2.3 СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Правові засади побудови, поточної діяльності та розвитку системи забезпечення ІБ України складають: Конституція України, Концепція (основи державної політики) національної безпеки України, інші законодавчі та нормативні акти, що регулюють відносини в інформаційній сфері.

Основні елементи системи забезпечення інформаційної безпеки України зображено на рис. 2.1. Повноваження та функції цих елементів такі.

Громадяни України на виборах, референдумах, через інші форми безпосередньої демократії, а також через органи державної влади та місцевого самоврядування:

- висловлюють і реалізують своє бачення національних інтересів України в інформаційній сфері, засобів їх захисту;
- привертають увагу суспільних і державних інститутів до небезпечних явищ і процесів в інформаційній сфері;
- захищають власні права та інтереси в інформаційній сфері всіма законними способами та засобами.

Верховна Рада України:

- здійснює законодавче регулювання і контроль за діяльністю органів державної влади та посадових осіб щодо виконання ними функцій і завдань у сфері інформаційної безпеки;
- ухвалює засади внутрішньої і зовнішньої політики держави в інформаційній сфері;
- затверджує державний бюджет, в якому передбачає кошти на забезпечення інформаційної безпеки України;
- схвалює національні програми розвитку інформаційної сфери;
- проводить парламентські слухання з питань забезпечення свободи слова та інформаційної безпеки України;

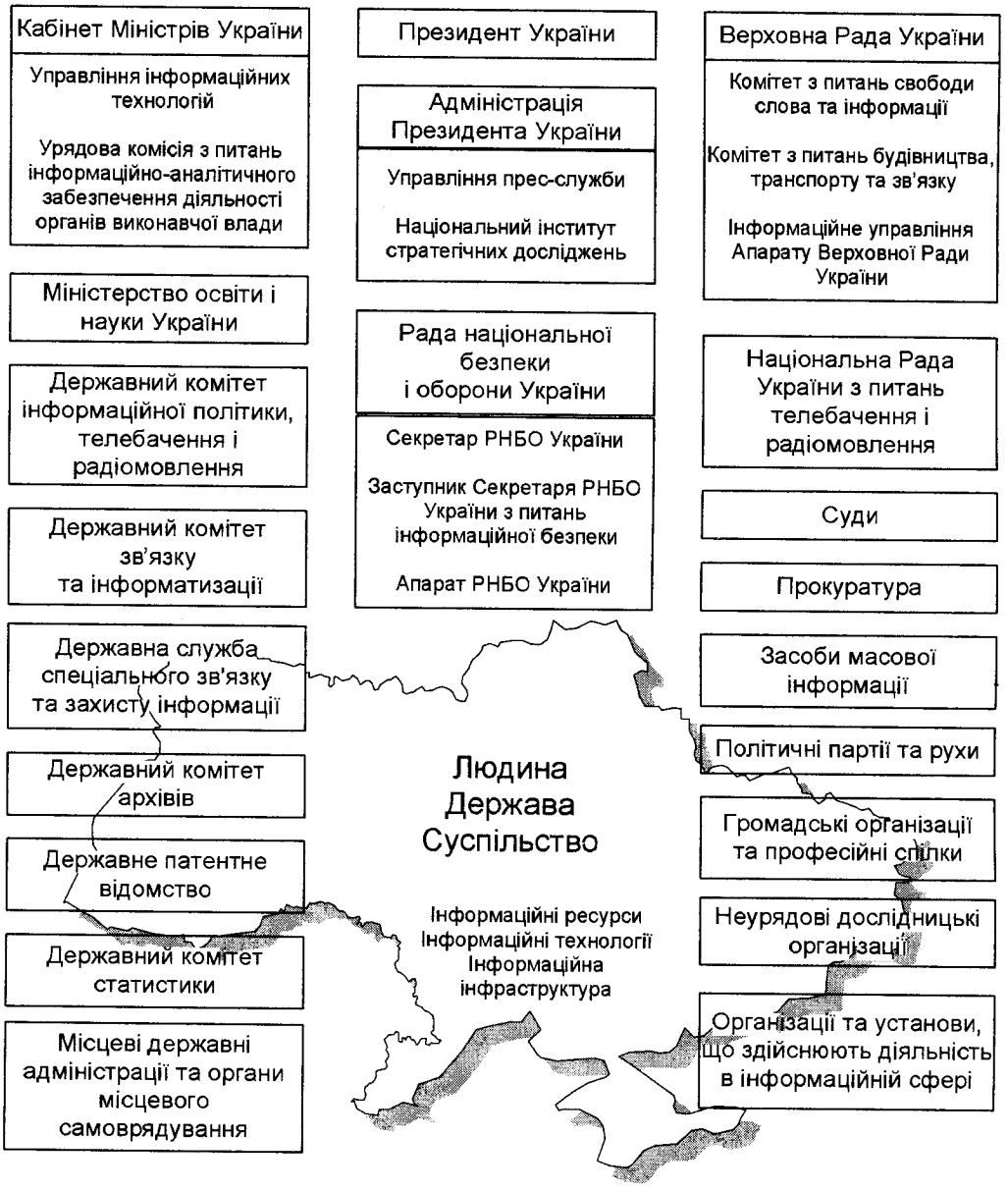


Рисунок 2.1 – Основні елементи забезпечення ІБ України

- призначає половину складу (чотири особи) Національної Ради України з питань телебачення і радіомовлення;
- дає згоду на призначення та звільнення з посади Президентом України голови Державного комітету телебачення і радіомовлення України.

Профільний парламентський Комітет з питань свободи слова та інформації готує законопроекти з питань інформаційної політики й безпеки.

Комітет з питань будівництва, транспорту і зв'язку вносить законодавчі пропозиції з питань функціонування та розвитку системи зв'язку як одного з ключових елементів інформаційної інфраструктури.

Структурним підрозділом Апарату Верховної Ради є Інформаційне управління, у складі якого діє прес-служба Верховної Ради. Зв'язки з громадськістю спікера Парламенту забезпечує прес-секретар Голови Верховної Ради України.

Президент України, в межах своїх повноважень:

- здійснює керівництво в сфері інформаційної безпеки;
- створює, реорганізовує та ліквідує органи виконавчої влади, визначає їх функції та основні завдання;
- видає укази і розпорядження, що стосуються функціонування та розвитку інформаційної сфери;
- звертається з щорічними (позачерговими) посланнями до Верховної Ради про внутрішнє і зовнішнє становище України, в т.ч. в інформаційній сфері;
- призначає (за поданням прем'єр-міністра) та звільняє з посад керівників міністерств, державних комітетів, інших центральних органів виконавчої влади, що здійснюють повноваження в інформаційній сфері: міністра освіти і науки України, голів Державного комітету інформаційної політики, телебачення і радіомовлення, Державного комітету зв'язку та інформатизації, Державного комітету архівів, Державного патентного відомства, Державного комітету статистики, президентів Національної телекомпанії України, Національної радіокомпанії України;
- призначає та звільняє з посади керівника Державної служби спеціального зв'язку та захисту інформації;
- призначає половину складу (чотири особи) Національної Ради України з питань телебачення і радіомовлення.

Адміністрації Президента України підпорядкований **Національний інститут стратегічних досліджень**, який є базовою науково-дослідною

установою аналітично-прогнозного супроводу діяльності Президента України. На Інститут покладене завдання координації наукових досліджень з питань інформаційної безпеки.

Інформування про діяльність глави держави здійснюють **прес-секретар Президента України** та **Управління прес-служби Адміністрації Президента України**.

Рада національної безпеки і оборони (РНБО) України, яку очолює глава держави, координує та контролює діяльність органів виконавчої влади у сфері інформаційної безпеки. На РНБО України покладено виконання таких функцій:

- внесення пропозицій Президентові України щодо реалізації засад внутрішньої і зовнішньої політики у сфері національної безпеки і оборони;
- координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони в мирний час;
- координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони в умовах воєнного або надзвичайного стану та при виникненні кризових ситуацій, що загрожують національній безпеці України.

Очевидно, що ці функції розповсюджуються і на сферу інформаційної безпеки. Відповідно до вказаних функцій РНБО України подає главі держави пропозиції щодо:

- визначення стратегічних національних інтересів України в інформаційній сфері, концептуальних підходів та напрямів забезпечення інформаційної безпеки;
- утворення, реорганізації та ліквідації органів виконавчої влади в інформаційній сфері;
- проекту державного бюджету за статтями, пов'язаними із забезпеченням інформаційної безпеки;
- заходів інформаційного та іншого характеру, відповідно до масштабу потенційних та реальних загроз національним інтересам України.

Апарат РНБО України здійснює поточне інформаційно-аналітичне та організаційне забезпечення діяльності РНБО України.

Апарат підпорядковується **Секретареві РНБО** України, до повноважень якого, крім іншого, віднесено підготовку пропозицій щодо перспективного й поточного планування діяльності РНБО України.

Кабінет Міністрів України:

- забезпечує державний суверенітет, здійснення внутрішньої та зовнішньої політики, виконання Конституції і законів України, актів Президента України в інформаційній сфері;
- вживає заходів щодо забезпечення прав і свобод громадян, забезпечення інформаційної безпеки України, боротьби зі злочинністю в інформаційній сфері;
- під час формування проекту бюджету передбачає виділення необхідних коштів для виконання загальнодержавних програм, спрямованих на забезпечення інформаційної безпеки України.

Урядова комісія з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади розробляє пропозиції щодо реформування системи інформаційно-аналітичного забезпечення діяльності органів виконавчої влади.

У складі Секретаріату Кабінету Міністрів України діє **Управління інформаційних технологій**. Інформування про діяльність прем'єр-міністра України здійснює його прес-секретар – керівник прес-служби.

Міністерства, інші центральні органи виконавчої влади, в межах своїх повноважень, наявних засобів бюджетного і позабюджетного фінансування, забезпечують виконання законів, указів Президента України, постанов Кабінету Міністрів України, інших органів виконавчої влади в інформаційній сфері. В кожному з цих органів діють інформаційно-аналітичні підрозділи та прес-служби.

Міністерство освіти і науки України є головним органом у системі центральних органів виконавчої влади із забезпечення реалізації державної політики в сфері освіти, наукової, науково-технічної, інноваційної діяльності та інтелектуальної власності; сприяє функціонуванню національної системи науково-технічної інформації; видає охоронні документи на об'єкти ін-

телектуальної власності, забезпечує державну реєстрацію авторського права; координує діяльність щодо трансферу технологій та прав на об'єкти інтелектуальної власності, створені повністю або частково за рахунок коштів державного бюджету.

Державний комітет інформаційної політики, телебачення і радіомовлення України вносить пропозиції щодо формування державної політики в інформаційній та видавничій сферах, забезпечує її реалізацію, здійснює управління в цих сферах, міжгалузеву координацію та функціональне управління з питань, віднесених до його відання; здійснює координацію діяльності державних засобів масової інформації, в т.ч. Національної телекомпанії України, Національної радіокомпанії України, державної телерадіокомпанії "Крим", обласних і регіональних телерадіокомпаній, видавництв; проводить аналіз і прогнозування тенденцій розвитку інформаційного простору України, здійснює заходи щодо його захисту.

Державний комітет зв'язку та інформатизації України забезпечує:

- проведення державної політики в галузі зв'язку та у сфері інформатизації, несе відповідальність за їх стан і розвиток;
- розподіл і використання радіочастотного ресурсу;
- розробляє та здійснює заходи щодо розвитку й удосконалення національної системи зв'язку;
- формування Національної програми інформатизації та її виконання.

Державний комітет архівів України:

- вносить пропозиції щодо формування державної політики у сфері архівної справи і діловодства;
- забезпечує реалізацію державної політики у сфері архівної справи і діловодства;
- здійснює управління у сфері архівної справи і діловодства, а також міжгалузеву координацію та функціональне регулювання з питань, віднесених до його відання;
- несе відповідальність за стан в архівній справі і подальший її розвиток.

Державна служба спеціального зв'язку та захисту інформації є органом державного управління в галузі забезпечення захисту державних

інформаційних ресурсів у мережах передачі даних, реалізує державну політику у сфері криптографічного та технічного захисту інформації.

Національна Рада України з питань телебачення і радіомовлення вирішує питання:

- забезпечення свободи слова та масової інформації;
- забезпечення прав телеглядачів і радіослухачів, виробників і розповсюджувачів масової звукової, візуальної та аудіовізуальної інформації;
- розробки і здійснення державної політики ліцензування телерадіомовлення;
- використання радіочастотного ресурсу держави;
- реалізації та контролю за додержанням законодавства України у сфері телебачення і радіомовлення.

Конституційний Суд України вирішує питання про відповідність законів та інших правових актів в інформаційній сфері Конституції України, дає офіційне тлумачення Конституції та законів України з відповідних питань.

Суди загальної юрисдикції здійснюють правосуддя у сфері інформаційних відносин.

Генеральна прокуратура України здійснює нагляд за дотриманням і застосуванням законів, що регулюють інформаційні відносини, порушує кримінальні справи.

Рада Міністрів Автономної Республіки Крим, обласні державні адміністрації, Київська та Севастопольська міські державні адміністрації забезпечують:

- виконання законів, указів Президента України, постанов Кабінету Міністрів України, інших органів виконавчої влади; дотримання законних прав і свобод громадян;
- виконання державних і регіональних програм в інформаційній сфері;
- реалізацію інших, наданих державою або делегованих відповідними радами, повноважень.

У державних адміністраціях діють інформаційно-аналітичні підрозділи та прес-служби.

Органи місцевого самоврядування затверджують регіональні та місцеві програми розвитку інформаційної сфери, бюджети відповідних адміністративно-територіальних одиниць (в яких передбачають кошти на виконання завдань в інформаційній сфері); виконують інші, передбачені законодавством, повноваження.

Інші державні органи та організації – Державний комітет статистики України, Державне патентне відомство України, Українське державне підприємство поштового зв'язку "Укрпошта", Концерн радіомовлення, радіозв'язку і телебачення, ВАТ "Укртелеком" тощо – здійснюють діяльність в інформаційній сфері в межах визначених функцій та повноважень.

Засоби масової інформації є важливим елементом системи забезпечення інформаційної безпеки України. ЗМІ інформують громадськість про події в Україні та світі, в т.ч. про діяльність органів державної влади; впливають на формування громадської думки; створюють своєрідні зворотні зв'язки між владою та громадськістю. Незаангажованість, активна діяльність ЗМІ є необхідною передумовою формування в Україні громадянського суспільства.

Політичні партії та рухи, громадські організації, професійні спілки, заклади академічної науки та освіти, неурядові дослідницькі організації, інші організації та установи виконують функції в системі забезпечення інформаційної безпеки України відповідно до мети і завдань їх діяльності.

Загалом, в Україні створена й функціонує структурно повна система забезпечення інформаційної безпеки. Функції та повноваження відповідних державних органів закріплено в нормативно-правових актах різного рівня – Конституції України, законах України, указах Президента України, постановах Кабінету Міністрів України, інших нормативних і відомчих актах.

2.4 ПРАВОВІ АКТИ

2.4.1 Структура правових актів

Вимоги інформаційної безпеки повинні органічно включатися в усі рівні законодавства, у тому числі й у конституційне законодавство, основні

загальні закони, закони з організації державної системи управління, спеціальні закони, відомчі правові акти й ін.

На рис. 2.2 наведено структуру правових актів, орієнтованих на правовий захист інформації.

Перший блок – **конституційне законодавство**. Норми, що стосуються питань інформатизації і захисту інформації, входять у нього як складові елементи.

Другий блок – **загальні закони, кодекси** (про власність, про надра, про землю, про права громадян, про громадянство, про податки, про антимонопольну діяльність тощо), що містять норми з питань інформатизації й інформаційної безпеки.

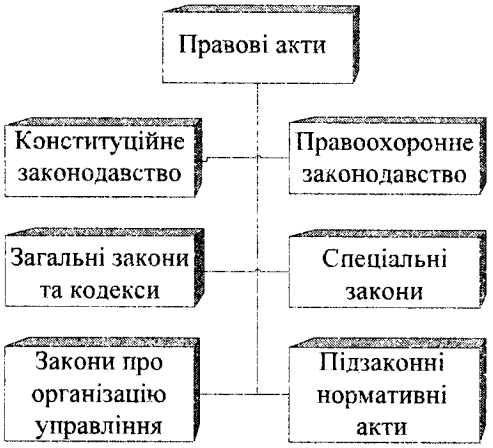


Рисунок 2.2 – Структура правових актів

Третій блок – **закони про організацію управління**, що стосуються окремих структур господарства, економіки, системи державних органів і визначають їхній статус. Вони містять окремі норми з питань захисту інформації. Поряд із загальними питаннями інформаційного забезпечення і захисту інформації конкретного органу ці норми повинні встановлювати його обов'язки з формування, актуалізації та безпеки інформації, що становить загальнодержавний інтерес.

Четвертий блок – це **правоохоронне законодавство** України, що містить норми про відповідальність за правопорушення у сфері інформатизації.

П'ятий блок – **спеціальні закони**, що цілком стосуються конкретних сфер відносин, галузей господарства, процесів. До них, зокрема, належить Закон "Про інформацію, інформатизацію і захист інформації". Саме склад і зміст цього блоку законів і створює спеціальне законодавство як основу правового забезпечення інформаційної безпеки.

Шостий блок – **підзаконні нормативні акти** з питань захисту інформації.

Спеціальне законодавство в галузі безпеки інформаційної діяльності представлено низкою законів, серед яких особливе місце належить базовому Закону "*Про інформацію, інформатизацію і захист інформації*", що закладає основи правового визначення всіх найважливіших компонентів інформаційної діяльності:

- інформації й інформаційних систем;
- суб'єктів – учасників інформаційних процесів;
- правовідносин виробників та споживачів інформаційної продукції;
- власників (джерел) інформації – обробників і споживачів на основі відносин власності при забезпеченні гарантій інтересів громадян і держави.

Цей закон визначає основи захисту інформації в системах обробки і при її використанні з урахуванням категорій доступу до відкритої інформації і до інформації з обмеженим доступом. Цей закон містить, крім того, загальні норми щодо організації і ведення інформаційних систем, зокрема банків даних державного призначення, порядку державної реєстрації, ліцензування, сертифікації, експертизи, а також загальні принципи захисту і гарантій прав учасників інформаційного процесу.

Питання правового режиму інформації з обмеженим доступом реалізуються в двох самостійних законах "Про державну таємницю" та "Про комерційну таємницю".

Крім того, цей аспект розкривається й у Цивільному кодексі статтею **"Службова і комерційна таємниця"**.

«1. *Інформація складає службову чи комерційну таємницю у випадку, коли інформація має дійсну чи потенційну комерційну*

цінність у силу невідомості її третім Особам, до неї немає вільного доступу на законній підставі і власник інформації вживає заходів щодо охорони її конфіденційності. Відомості, що не можуть складати службову чи комерційну таємницю, визначаються законом і іншими правовими актами.

2. Інформація, що складає службову чи комерційну таємницю, захищається способами, передбаченими дійсним кодексом і іншими законами.»

Друга частина статті визначає правові основи відповідальності за несанкціоноване одержання інформації чи заподіяння збитку.

"Особи, що незаконними методами отримали інформацію, яка складає службову чи комерційну таємницю, зобов'язані відшкодувати заподіяні збитки. Такий же обов'язок покладається на працівників, що розголосили службову чи комерційну таємницю всупереч трудовому договору, у тому числі контракту, і на контрагентів, що зробили це всупереч цивільно-правовому договору".

Таким чином, правовий захист інформації забезпечується нормативно-законодавчими актами, що представляють собою ієрархічну систему від Конституції до функціональних обов'язків і контракту окремого конкретного виконавця, що визначають перелік відомостей, які підлягають охороні, і міри відповідальності за їхнє розголошення.

2.4.2 Нормативно-правові документи

Нормативні документи поділяються на:

- нормативні документи із стандартизації в галузі технічного захисту інформації;
- державні стандарти та прирівняні до них нормативні документи;
- нормативні акти міжвідомчого значення, що регулюються у Міністерстві юстиції України;
- нормативні документи міжвідомчого значення технічного характеру, що реєструються органом, уповноваженим Кабінетом Міністрів України;

- нормативні документи відомчого значення органів державної влади та органів місцевого самоврядування.

Спираючись на державні правові акти і з огляду на відомчі інтереси на рівні конкретного підприємства (фірми, організації), розробляються власні нормативно-правові документи, орієнтовані на забезпечення інформаційної безпеки. До таких документів належать:

"Положення про збереження конфіденційної інформації";

"Перелік відомостей, що складають конфіденційну інформацію";

"Інструкція про порядок допуску співробітників до відомостей, що складають конфіденційну інформацію";

"Положення про спеціальне діловодство і документообіг";

"Перелік відомостей, дозволених до опублікування у відкритій пресі";

"Положення про роботу з іноземними фірмами і їхніми представниками";

"Зобов'язання співробітника про збереження конфіденційної інформації";

"Пам'ятка співробітнику про збереження комерційної таємниці".

Зазначені нормативні акти спрямовані на попередження випадків неправомірного оголошення (розголошення) секретів на правовій основі й у випадку їхнього порушення повинні вживатися відповідні заходи впливу.

2.4.3 Форми захисту інформації

Залежно від характеру інформації, її доступності для зацікавлених споживачів, а також економічної доцільності конкретних захисних заходів можуть бути обрані такі **форми захисту інформації**:

- патентування;
- авторське право;
- визнання відомостей конфіденційними;
- товарні знаки;
- застосування норм зобов'язального права.

Існують певні розходження між авторським правом і комерційною таємницею. Авторське право захищає тільки форму вираження ідеї. Комерційна таємниця стосується безпосередньо змісту. Авторське право захищає

від копіювання незалежно від конфіденційних відносин із власником. До авторського права прибігають при широкій публікації своєї інформації, у той час як комерційну таємницю тримають у секреті. Очевидно, що в порівнянні з патентом і авторським правом комерційна і виробнича таємниці є найбільш зручними, надійними і гнучкими формами захисту інформації.

Крім вищевикладених форм правового захисту і права приналежності інформації знаходить широке розповсюдження офіційна передача права на користування нею у вигляді ліцензії.

Ліцензійні дозволи надаються на певний час і на певні види товарів.

Ліцензія – це дозвіл, що видається державою на проведення деяких видів господарської діяльності, зокрема зовнішньоторговельних операцій (ввезення та вивезення) і надання права використовувати захищені патентами винаходи, технології, методики.

На всі форми захисту інтелектуальної власності є відповідні закони – "Закон про патенти", "Закон про авторське право", "Закон про комерційну таємницю", "Закон про товарні знаки" й ін.

Створюючи систему інформаційної безпеки, необхідно чітко розуміти, що без правового забезпечення захисту інформації будь-які претензії до несумлінного співробітника, клієнта, конкурента і посадової особи будуть необґрунтованими.

Якщо перелік відомостей конфіденційного характеру не доведений вчасно до кожного співробітника (природно, якщо він допущений за посадовими обов'язками) у письмовому вигляді, то співробітник, який вкрав важливу інформацію в порушення встановленого порядку роботи з нею, швидше за все розведе руками: звідки мені це знати! У цьому випадку ніякі інстанції, аж до судових, не зможуть допомогти його покарати.

Одним з напрямків правового захисту є **страхове забезпечення**. Воно призначено для захисту власника інформації і засобів її обробки як від традиційних загроз (крадіжки, стихійні лиха), так і від загроз, що виникають у ході роботи з інформацією. До них належать розголошення, витік і несанкціонований доступ до конфіденційної інформації.

Метою страхування є забезпечення страхового захисту фізичних і юридичних осіб від страхових ризиків у вигляді повного чи часткового відшкодування збитку і втрат, заподіяних стихійними лихами, надзвичайними подіями в різних галузях діяльності, протиправними діями з боку конкурентів і зловмисників шляхом виплат грошової компенсації чи надання сервісних послуг (ремонт, відновлення) при настанні страхової події.

В основі страхового законодавства лежить Закон "Про страхування", який дає таке визначення терміну "страхування":

Страхування – це відносини, що стосуються захисту майнових інтересів фізичних і юридичних осіб при настанні визначених подій (страхових випадків) за рахунок грошових фондів, які формуються зі страхових внесків, сплачуваних ними.

Цей закон покликаний гарантувати захист інтересів страхувальників, визначати єдині положення щодо організації страхування і принципи державного регулювання страхової діяльності.

2.5 ЗАХИСТ ПРАВ НА КОМЕРЦІЙНУ ТАЄМНИЦЮ ТА ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ РЕЖИМУ КОМЕРЦІЙНОЇ ТАЄМНИЦІ

Існує система засобів захисту прав на комерційну таємницю, у якій виділяються засоби цивільного, кримінального, адміністративного, трудового права.

2.5.1 Цивільно-правовий захист

Підставами для цивільно-правової відповідальності може бути порушення договірного зобов'язання або позадоговірні порушення – вчинення цивільно-правових деліктів. Договірні порушення стосуються переважно ліцензійних договорів – на них поширюються всі загальні правила про відповідальність за порушення зобов'язання.

Позадоговірний захист прав на комерційну таємницю ґрунтується на загальних положеннях про деліктну відповідальність та особливостях правового режиму комерційної таємниці як об'єкта інтелектуальної власності.

Для комерційної таємниці неможливим є такий спосіб захисту, як відновлення становища, яке існувало до порушення. Адже відомості розголошуються безповоротно, їх не можна вилучити зі свідомості особи, яка незаконно з ними ознайомилася. Відповідно, захист може полягати лише у відшкодуванні збитків та забороні продовжувати порушення.

2.5.2 Кримінально-правовий захист

Кримінальну відповідальність за діяння, пов'язані з порушенням режиму комерційної таємниці, визначено у «Кримінальному кодексі України». Передбачена відповідальність за два окремі склади злочину:

1) незаконне збирання з метою використання відомостей, що становлять комерційну таємницю;

2) незаконне використання відомостей, що становлять комерційну таємницю, якщо це спричинило істотну шкоду суб'єкту господарської діяльності.

Суб'єктивна сторона незаконного збирання характеризується прямим умислом та обов'язковою ознакою – наявністю мети: подальше розголошення або інше використання відомостей. Таким використанням може бути:

- розголошення з метою заподіяння матеріальної чи іншої шкоди;
- використання для власних потреб, наприклад, впровадження у виробництво;
- продаж чи безоплатна передача іншим суб'єктам господарювання;
- вимагання винагороди чи вчинення певних дій за повернення чи нерозголошення зібраних відомостей.

Такий злочин відносять до злочинів середньої тяжкості, оскільки найбільшою санкцією (альтернативною до штрафу та обмеження волі) за його вчинення є позбавлення волі строком до 3 років.

Розголошення комерційної таємниці також матиме місце в разі його вчинення особою, яка обіймає постійно чи тимчасово на підприємствах, в

установах, організаціях незалежно від форми власності посади, пов'язані з виконанням організаційно-розпорядчих чи адміністративно-господарських обов'язків, або виконують такі обов'язки за спеціальним повноваженням. Один з таких випадків прямо вказаний у статті 23 Закону України «Про господарські товариства»:

«Посадові особи повинні зберігати комерційну таємницю та конфіденційну інформацію і несуть за її розголошення відповідальність, передбачену чинним законодавством України та установчими документами товариства».

Законодавством також прямо передбачено ряд випадків, коли обов'язок зберігати режим таємності щодо комерційної інформації покладено на осіб, які знайомляться з такою інформацією в силу своїх професійних обов'язків. Такими особами, наприклад, є:

- управитель іпотеки щодо власників сертифікатів (ст. 34 Закону «Про іпотечне кредитування, операції з консолідованим іпотечним боргом та іпотечні сертифікати»);
- страховики стосовно страхувальників (ст. 20 Закону «Про страхування»);
- брокери щодо біржових операцій їхніх клієнтів (ст. 16 Закон «Про товарну біржу»);
- аудитори і аудиторські фірми (ст. 23 Закону «Про аудиторську діяльність») та ін.

2.5.3 Адміністративно-правовий захист

Вчинення дій, визначених Законом «Про захист від недобросовісної конкуренції» як недобросовісна конкуренція, громадянами, які займаються підприємницькою діяльністю без створення юридичної особи, тягне за собою накладення адміністративного стягнення згідно із законодавством (ст. 23 Закону). Кодексом України про адміністративні правопорушення (ст. 164-3) встановлено відповідальність за отримання, використання, розголошення комерційної таємниці з метою заподіяння шкоди діловій репутації або майну іншого підприємця у вигляді накладення штрафу від дев'яти до вісімнадцяти

неоподатковуваних мінімумів доходів громадян (17 грн. з 1996 року; тобто штраф у розмірі від 153 до 306 грн.).

Вчинення «господарюючими суб'єктами – юридичними особами та їх об'єднаннями» дій, визначених Законом «Про захист від недобросовісної конкуренції» як недобросовісна конкуренція, тягне за собою накладання на них Антимонопольним комітетом України, його територіальними відділеннями штрафів у розмірі до 3% виручки від реалізації товарів, виконання робіт, надання послуг господарюючого суб'єкта за останній звітний рік, що передував року, в якому накладається штраф. У разі, якщо обчислення виручки господарюючого суб'єкта неможливе або виручка відсутня, штрафи, зазначені у частині першій цієї статті, накладаються у розмірі до п'яти тисяч неоподатковуваних мінімумів доходів громадян (тобто до 85 тис. грн.).

Вчинення дій, визначених Законом «Про захист від недобросовісної конкуренції» як недобросовісна конкуренція, «юридичними особами, їх об'єднаннями та об'єднаннями громадян, що не є господарюючими суб'єктами», тягне за собою накладання на них Антимонопольним комітетом України, його територіальними відділеннями штрафів у розмірі до двох тисяч неоподатковуваних мінімумів доходів громадян (тобто до 34 тис. грн.).

2.6 ПРАВОВІ НОРМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ І ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Правові норми забезпечення безпеки і захисту інформації на конкретному підприємстві (фірмі, організації) формулюються у сукупності установчих, організаційних і функціональних документів.

Вимоги забезпечення безпеки і захисту інформації формулюються в **Статуті** (установчому договорі) у вигляді таких положень:

- підприємство має право визначати склад, обсяг і порядок захисту відомостей конфіденційного характеру, вимагати від своїх співробітників забезпечення їх збереження і захисту від внутрішніх і зовнішніх загроз;

- підприємство зобов'язане забезпечити збереження конфіденційної інформації.

Такі вимоги надають право адміністрації підприємства:

- створювати організаційні структури із захисту конфіденційної інформації;
- видавати нормативні і розпорядчі документи, що визначають порядок виділення відомостей конфіденційного характеру і механізми їхнього захисту;
- включати вимоги щодо захисту інформації в договори з усіх видів господарської діяльності;
- вимагати захисту інтересів підприємства з боку державних і судових інстанцій;
- розпоряджатися інформацією, що є власністю підприємства, з метою отримання вигоди і недопущення економічного збитку колективу підприємства і власнику засобів виробництва;
- розробити "Перелік відомостей, які становлять конфіденційну таємницю".

Вимоги правової забезпеченості захисту інформації передбачаються в колективному договорі. **Колективний договір** повинний містити такі вимоги.

Розділ "Предмет договору"

Адміністрація підприємства (у тому числі й адміністрація самостійних підрозділів) ЗОБОВ'ЯЗУЄТЬСЯ забезпечити розробку і здійснення заходів щодо визначення і захисту конфіденційної інформації.

Трудовий колектив бере на себе зобов'язання дотримуватися встановлених на підприємстві вимог щодо захисту конфіденційної інформації.

Адміністрація зобов'язана врахувати вимоги щодо захисту конфіденційної інформації в правилах внутрішнього розпорядку.

Розділ "Кадри. Забезпечення дисципліни праці"

Адміністрація зобов'язується притягувати до адміністративної і кримінальної відповідальності, згідно з чинним законодавством, порушників вимог щодо захисту комерційної таємниці.

Правила внутрішнього трудового розпорядку для робітників та службовців підприємства доцільно доповнити такими вимогами.

Розділ "Порядок прийому і звільнення робітників та службовців"

При вступі робітника чи службовця на роботу чи переведенні його у встановленому порядку на іншу роботу, зв'язану з конфіденційною інформацією підприємства, а також при звільненні адміністрація зобов'язана проінструктувати працівника чи службовця з правилами збереження комерційної таємниці з оформленням письмового зобов'язання про її нерозголошення.

Адміністрація підприємства має право приймати рішення про усунення від робіт осіб, що порушують установлені вимоги щодо захисту конфіденційної інформації.

Розділ "Основні обов'язки робітників та службовців"

Робітники та службовці зобов'язані дотримуватися вимог нормативних документів щодо захисту конфіденційної інформації підприємства.

Розділ "Основні обов'язки адміністрації"

Адміністрація підприємства, керівники підрозділів зобов'язані:

- забезпечити строге збереження конфіденційної інформації, постійно здійснювати організаційну і виховну профілактичну роботу, спрямовану на захист секретів підприємства;
- включити в посадові інструкції і положення обов'язки щодо збереження конфіденційної інформації;
- неухильно виконувати вимоги Статуту, колективного договору, трудових договорів, правил внутрішнього трудового розпорядку й інших організаційних і господарських документів у частині забезпечення економічної й інформаційної безпеки.

Зобов'язання конкретного співробітника, робітника чи службовця в частині захисту інформації обов'язково повинні бути застережені в трудовому договорі (контракті). Незалежно від форми (усної чи письмової) укладання договору підпис робітника на наказі про прийом на роботу підтверджує його згоду з умовами договору. Вимоги щодо захисту конфіденційної інформації можуть бути застережені в тексті договору, якщо договір укладається в письмовій формі. Якщо ж договір укладається в усній формі, то діють вимоги щодо захисту інформації, які випливають з нормативно-правових документів підприємства. При укладанні трудового договору й

оформленні наказу про прийом на роботу нового співробітника визначається поінформованість його про порядок захисту інформації підприємства. Це створює необхідний елемент включення даної Особи в механізм забезпечення інформаційної безпеки.

Використання договорів про нерозголошення таємниці – зовсім не самостійний захід для її захисту. Не слід думати, що після підписання такої угоди з новим співробітником таємниця буде збережена. Це тільки попередження співробітнику, що в справу вступає система заходів щодо захисту інформації і правова основа. Далі задача – не допустити втрати комерційних секретів.

2.7 УКРАЇНСЬКЕ ЗАКОНОДАВСТВО В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Відповідно до ст. 41 "Конституції" інформація є предметом державної охорони, яка забезпечується Законом України "Про інформацію", Законом України "Про захист інформації в автоматизованих системах" та ст. 361-363 Кримінального Кодексу України. Крім цих документів до нормативно-правової бази, яка регулює інформаційні правовідносини, належать наведені нижче положення та інструкції.

"*Положення про технічний захист в Україні*", затверджено постановою Кабінету Міністрів України від 09.09.94 р. № 632.

Положення визначає об'єкт захисту та мету технічного захисту інформації (ТЗІ), структуру та основні завдання складових частин системи ТЗІ, порядок та організацію комплексного технічного захисту інформації з обмеженим доступом на об'єктах різного призначення і організацію контролю за ефективністю ТЗІ.

Постанова Кабінету Міністрів України від 13.01.95 р. № 24 "*Про заходи щодо виконання постанови Верховної Ради України від* 05.07.94 р. № 80", "*Про введення в дію Закону України "Про захист інформації в автоматизованих системах" та статті* 34 *Закону України "Про Державну таємницю*".

"*Положення про порядок видачі суб'єктам підприємницької діяльності спеціальних дозволів (ліцензій) на здійснення окремих видів діяльності*", затверджено постановою Кабінету Міністрів України від 17.05.94 р. № 316.

Положення визначає види діяльності, на які передбачено законодавчими актами України видачу спеціальних дозволів (ліцензій), в тому числі виробництво та сервісне обслуговування систем і засобів виконання робіт, надання послуг, що забезпечують технічний захист інформації. Положення також визначає умови і правила одержання ліцензій.

"*Інструкція щодо умов і правил здійснення діяльності у галузі технічного захисту інформації та контролю за її дотриманням*", затверджена наказом ДСТСЗІ від 26.05.94 р. № 46, зареєстровано в Мінюсті України 01.06.94 р. № 120\329.

Інструкція визначає умови і правила здійснення діяльності у галузі ТЗІ з виробництва та сервісного обслуговування систем і засобів, виконання робіт, надання послуг, що забезпечують технічний захист інформації.

"*Положення про порядок опрацювання, прийняття, перегляду та скасування міжвідомчих нормативних документів системи технічного перегляду та скасування міжвідомчих нормативних документів системи технічного захисту інформації*", затверджено наказом ДСТСЗІ від 01.07.96 р. № 44, зареєстровано в Мінюсті України 18.07.96 р. № 366\1391.

Положення визначає порядок розроблення, погодження, затвердження, реєстрації та виконання нових, перегляду та скасування чинних міжвідомчих нормативних документів технічного характеру (норми, методики, положення, інструкції тощо) системи технічного захисту інформації, що не належать до нормативних документів із стандартизації, але є обов'язковими для виконання всіма центральними місцевими органами виконавчої влади, Урядом Автономної Республіки Крим, органами місцевого самоврядування, військовими частинами всіх військових формувань, створених відповідно до законодавства; підприємствами, установами й організаціями незалежно від

форм власності, діяльність яких пов'язана з технічним захистом інформації.

До загальнодержавних нормативних актів з питань захисту інформації відносять такі стандарти.

Державний стандарт України. ДСТУ 3396.0-96. *Захист інформації. Технічний захист інформації. Основні поняття.* Затверджено наказом Держстандарту України від 11.10.96 р. № 423, введено в дію 01.01.97 р.

Стандарт установлює об'єкт захисту, мету, основні організаційно-технічні поняття технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також етапи побудови системи захисту інформації та категорії нормативних документів з ТЗІ.

Вимоги стандарту обов'язкові для підприємств та установ усіх форм власності та підпорядкування, громадян – суб'єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин всіх формувань, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

Державний стандарт України. ДСТУ 3396.1-96. *Захист інформації. Технічний захист інформації. Порядок проведення робіт.* Затверджено наказом Держстандарту України від 19.12.96 р. № 51, введено в дію 01.01.97 р.

Цей стандарт установлює вимоги до порядку проведення робіт з технічного захисту інформації, який за наказом керівника підприємства передбачає:

- організацію проведення обстеження;
- організацію розроблення системи захисту інформації;
- реалізацію організаційних заходів захисту;
- реалізацію первинних технічних заходів захисту;
- реалізацію основних технічних заходів захисту;
- прийняття, визначення повноти та якості робіт.

Для участі в роботах, надання методичної допомоги, оцінювання

повноти та якості реалізації заходів захисту можуть залучатися спеціалісти з ТЗІ сторонніх організацій, які мають ліцензію органу, уповноваженого Кабінетом Міністрів України.

Державний стандарт України. ДСТУ 3396.2-97. *Захист інформації. Технічний захист інформації. Терміни та визначення.* Затверджено наказом Держстандарту України від 11.04.97 р. № 200, введено в дію 01.01.98 р.

Цей стандарт установлює терміни та визначення понять у сфері технічного захисту інформації.

Терміни, регламентовані у цьому стандарті, обов'язкові для використання в усіх видах організаційної та нормативної документації, а також для робіт зі стандартизації і рекомендовані для використання у довідковій та навчально-методичній літературі, що належить до сфери технічного захисту інформації.

Терміни стандарту є обов'язковими для використання підприємствами та установами усіх форм власності і підпорядкування, громадянами – суб'єктами підприємницької діяльності, міністерствами (відомствами), центральними і місцевими органами державної виконавчої влади, військовими частинами всіх військових формувань, представництвами України за кордоном, які володіють, використовують та розпоряджаються інформацією, що становить державну чи іншу передбачену законом таємницю або є конфіденційною інформацією, яка належить державі.

Державний стандарт України. ДСТУ 1.3-93. *Порядок розроблення, побудови, оформлення, узгодження, затвердження, позначення та реєстрації технічних умов.* Затверджено та введено в дію наказом Держстандарту України від 29.07.93 р. № 116.

Стандарт установлює порядок розроблення, побудови, викладу, оформлення, узгодження, затвердження, позначання та державної реєстрації технічних умов на продукцію (послуги), що виготовляється в усіх галузях народного господарства України, крім розроблюваної та виготовленої на замовлення Міністерства оборони, а також змін до них.

Вимоги цього стандарту є обов'язковими для підприємств, установ і

організацій, що діють на території України, а також для громадян – суб'єктів підприємницької діяльності незалежно від форм власності і видів діяльності.

Державні будівельні норми України. ДБН А.2.2-2-96. *Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та документації для будівництва.* Затверджено наказом Держкоммістобудування України від 02.09.96 р. № 156 і введено в дію 01.01.97 р.

Стандарт установлює норми та вимоги до організації проектування, проектної документації для нового будівництва, розширення, реконструкції підприємств та капітального ремонту будівель і споруд об'єктів, де є необхідність проведення робіт з ТЗІ. Заходи з ТЗІ можуть виконуватися організаціями, які мають відповідні ліцензії Держкоммістобудування України, або іншими організаціями, які мають ліцензії Держкомсекретів України, відповідно до завдання замовника. Положення норм обов'язкові для застосування суб'єктами інвестиційної діяльності України та представництвами України за кордоном при виконанні проектних і будівельних робіт з урахуванням вимог технічного захисту інформації, які містять відомості, що становлять державну або іншу передбачену законодавством України таємницю, а також конфіденційну інформацію, що є державною власністю.

Норми можуть бути використані суб'єктами, професійна діяльність яких пов'язана з захистом конфіденційної інформації, що не є власністю держави.

Цілу низку нормативних документів підготовлено Департаментом спеціальних телекомунікаційних систем і захисту інформації (ДСТСЗІ) Служби безпеки України, який у 2007 році перетворено у Державну службу спеціального зв'язку і захисту інформації.

Нормативний документ системи ТЗІ. ТРЕОТ-95. "*Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок*", затверджено наказом ДСТСЗІ від 09.06.96 р. № 25.

Нормативний документ системи ТЗІ. ТРАС-96. "*Тимчасові рекомендації щодо розроблення розділу із захисту інформації в технічному завданні на створення автоматизованої системи*", затверджено наказом ДСТСЗІ від 03.07.96 р. № 47.

Нормативний документ системи ТЗІ. НД ТЗІ 1.6-001-96. "*Правила побудови, викладення, оформлення та позначення нормативних документів системи ТЗІ*", затверджено наказом ДСТСЗІ від 26.07.96 р. № 51.

Нормативний документ системи ТЗІ. "*Інструкція про порядок надання дозволу на використання імпортних засобів ТЗІ а також продукції, яка містить їх у своєму складі*", затверджено наказом ДСТСЗІ від 31.05.95 р. № 13 і зареєстровано в Мінюсті України 12.07.95 р. № 215\751.

2.8 ЗАРУБІЖНЕ ЗАКОНОДАВСТВО В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Законодавчий рівень інформаційної безпеки найбільше забезпечений у США, де нараховується близько 500 законодавчих актів.

Ключову роль грає "*Закон про інформаційну безпеку*" (*Computer Security Act of 1987, Public Law 100-235 (H.R. 145), January 8, 1988*). Його мета – реалізація мінімально достатніх дій щодо забезпечення безпеки інформації у федеральних комп'ютерних системах, без обмежень всього спектра можливих дій.

На початку *Закону* називається конкретний виконавець – Національний інститут стандартів і технологій (*NIST*), що відповідає за випуск стандартів і положень, спрямованих на захист від знищення і несанкціонованого доступу до інформації, а також від крадіжок і фальсифікацій, що здійснюються за допомогою комп'ютерів. Таким чином, увага приділяється як регламентації дій фахівців, так і підвищенню інформованості всього суспільства.

Згідно із Законом, всі оператори федеральних ІС, що містять конфіденційну інформацію, повинні сформувати плани забезпечення ІБ. Обов'язковим є *періодичне навчання* всього персоналу таких ІС. NIST, у свою чергу, зобов'язаний проводити дослідження природи і масштабу вразливих місць, виробляти економічно виправдані заходи захисту. Результати досліджень розраховані на застосування не тільки в державних системах, але й в приватному секторі.

Для захисту федеральних ІС рекомендується ширше застосовувати технологічні рішення, засновані на розробках приватного сектора. Крім того, пропонується оцінити можливості загальнодоступних зарубіжних розробок.

Вітається розробка правил безпеки, нейтральних стосовно конкретних технічних рішень, використання у федеральних ІС комерційних продуктів, які реалізують шифрувальні технології, що дозволяє зрештою сформувати інфраструктуру, яку можна розглядати як резервну для федеральних ІС.

У 2001 році був схвалений законопроект – *Computer Security Enhancement Act of 2001 (H.R. 1259 RFS)*, який дозволив не загострювати більше увагу на криптографії в цілому, а зосередитися на одному з її найважливіших додатків – автентифікації, розглядаючи її за відпрацьованою на криптозасобах методикою.

Програма безпеки, що передбачає економічно виправдані захисні заходи і синхронізована з життєвим циклом ІС, згадується в законодавстві США неодноразово.

Звичайно, в законодавстві США є в достатній кількості і положення обмежувальної спрямованості, і директиви, що захищають інтереси таких відомств, як Міністерство оборони, ФБР і ЦРУ.

У законодавстві **ФРН** основним є *"Закон про захист даних" (Federal Data Protection Act of December 20, 1990 (BGBl.I 1990 S.2954), amended by law of September 14, 1994 (BGBl. I S. 2325)*. Він цілком присвячений захисту персональних даних. Як і у всіх інших законах аналогічної спрямованості, в даному випадку встановлюється пріоритет інтересів національної безпеки над збереженням таємниці приватного життя. В іншому права особи захищені вельми ретельно. Наприклад, якщо співробітник фірми обробляє персональні дані на користь приватних компаній, він дає підписку про нерозголошення, яка діє і після переходу на іншу роботу.

Державні установи, що зберігають і обробляють персональні дані, несуть відповідальність за порушення таємниці приватного життя "суб'єкта даних", як мовиться в Законі. У матеріальному виразі відповідальність обмежена верхньою межею в 250 тисяч німецьких марок.

У законодавстві **Великобританії** є сімейство так званих добровільних стандартів *BS 7799*, що допомагають організаціям на практиці сформувати програми безпеки.

У сучасному світі глобальних мереж законодавча база повинна бути узгоджена з міжнародною практикою. В цьому плані повчальний приклад Аргентини.

В 1996 році в Аргентині був заарештований системний оператор електронної дошки оголошень. Йому ставилися в провину систематичні вторгнення в комп'ютерні системи ВМС США, НАСА, а також у комп'ютерні системи Бразилії, Чилі, Кореї, Мексики і Тайваню. Проте, його відпустили без офіційного висування звинувачень, оскільки за аргентинським законодавством вторгнення в комп'ютерні системи не вважається злочином.

2.9 СТАНДАРТИ І СПЕЦИФІКАЦІЇ В ГАЛУЗІ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

Особливе місце на законодавчому рівні займають стандарти і специфікації, до яких належать:

- оцінні стандарти, спрямовані на класифікацію інформаційних систем і засобів захисту за вимогами безпеки;
- технічні специфікації, що регламентують різні аспекти реалізації засобів захисту.

Оцінні стандарти виділяють найважливіші, з погляду інформаційної безпеки, аспекти ІС, які виконують роль архітектурних специфікацій. Інші технічні специфікації визначають, як будувати ІС указаної архітектури.

"Помаранчева книга" як оцінний стандарт

Історично першим оцінним стандартом, що набув значного поширення і зробив величезний вплив на базу стандартизації інформаційної безпеки

у багатьох країнах, став стандарт Міністерства оборони США "*Критерії оцінювання довірених комп'ютерних систем*".

Дана праця, звана найчастіше за кольором обкладинки "*Помаранчевою книгою*", була вперше опублікована в серпні 1983 року. В ній мова йде не про безпечні, а про довірені системи, тобто системи, яким можна надати певний ступінь довіри. У "Помаранчевій книзі" наведено таке поняття безпечної системи:

Безпечна система – це така система, в якій за допомогою відповідних засобів здійснюється керування доступом до інформації в такий спосіб, що тільки належним чином авторизовані особи або процеси, що діють від їх імені, отримують право читати, записувати, створювати і видаляти інформацію.

Очевидно, що абсолютно безпечних систем не існує, це абстракція. Є сенс оцінювати лише ступінь довіри, яку можна надати тій чи іншій системі.

Довірена система – це система, що використовує достатні апаратні і програмні засоби для забезпечення одночасного оброблення інформації різного ступеня секретності групою користувачів без порушення права доступу.

Звернемо увагу, що у "Помаранчевій книзі" і безпека, і довіра оцінюються виключно з погляду управління доступом до даних, що є одним із засобів забезпечення конфіденційності і цілісності. Питання доступності не піднімається.

Ступінь довіри оцінюється за двома критеріями: політика безпеки і рівень гарантованості.

Політика безпеки – це набір законів, правил і норм поведінки, що визначають, як організація обробляє, захищає і поширює інформацію.

Зокрема, правила визначають, в яких випадках користувач може оперувати конкретними наборами даних. Чим вищий ступінь довіри системі,

тим суворішою та гнучкішою повинна бути політика безпеки. Політика безпеки – це аспект захисту, що містить аналіз можливих загроз і вибір заходів протидії.

Рівень гарантованості – це міра довіри, яка може бути надана архітектурі і реалізації ІС.

Важливим засобом забезпечення безпеки є механізм підзвітності (*протоколювання*). Довірена система повинна фіксувати всі події, що стосуються безпеки. Ведення протоколів повинно доповнюватися *аудитом* (аналізом реєстраційної інформації).

Мета **підзвітності** – в кожен момент часу знати, хто працює в системі і що робить. Засоби підзвітності діляться на три категорії:

- ідентифікація і автентифікація;
- надання довіреного шляху;
- аналіз реєстраційної інформації.

Звичайний спосіб ідентифікації – введення імені користувача при вході в систему. Стандартний засіб перевірки достовірності (автентифікації) користувача – пароль.

Аналіз реєстраційної інформації (аудит) має справу з подіями, які так або інакше стосуються безпеки системи.

Технічна специфікація X.800

Основний зміст цього стандарту трактує питання інформаційної безпеки розподілених систем, зокрема, специфічні мережеві функції (сервіси) безпеки, а також необхідні для їх реалізації захисні механізми.

Виділяються такі сервіси безпеки і виконувані ними ролі.

Автентифікація. Даний сервіс забезпечує перевірку достовірності партнерів по спілкуванню і перевірку достовірності джерела даних. Автентифікація партнерів використовується при встановленні з'єднання і періодично під час сеансу. Вона служить для запобігання таким загрозам, як маскарад і повторення попереднього сеансу зв'язку.

Управління доступом. Забезпечує захист від несанкціонованого використання ресурсів, доступних у мережі.

Конфіденційність даних. Забезпечує захист від несанкціонованого отримання інформації. Окремо виділяється конфіденційність трафіку (це захист інформації, яку можна одержати, аналізуючи мережеві потоки даних).

Цілісність даних поділяється на підвиди залежно від того, який тип спілкування використовують партнери – з встановленням з'єднання чи без нього, захищаються всі дані чи тільки окремі поля, чи забезпечується відновлення у разі порушення цілісності.

Безвідмовність (неможливість відмовитися від виконаних дій) забезпечує два види послуг: безвідмовність з підтвердженням достовірності джерела даних і безвідмовність з підтвердженням доставки.

Адміністрування засобів безпеки включає розповсюдження інформації, необхідної для роботи сервісів і механізмів безпеки, а також збирання і аналіз інформації про їх функціонування. Прикладами можуть служити розповсюдження криптографічних ключів, установлення значень параметрів захисту, ведення реєстраційного журналу і т.п.

Стандарт ISO/IEC 15408

Цей стандарт є найповнішим і найсучаснішим серед стандартів – "Критерії оцінювання безпеки інформаційних технологій" (виданий 1 грудня 1999 року), який часто називають "Загальними критеріями".

"Загальні критерії" визначають інструменти оцінювання безпеки ІС і порядок їх використання.

КОНТРОЛЬНІ ПИТАННЯ

1. Охарактеризуйте необхідність і важливість законодавчого рівня ІБ.
2. Наведіть основні елементи системи забезпечення ІБ України.
3. Наведіть структуру правових актів із захисту інформації.
4. Дайте характеристику основних нормативно-правових документів із захисту інформації.
5. Охарактеризуйте особливості страхового забезпечення захисту інформації.
6. Охарактеризуйте форми правового захисту інформації.
7. Назвіть способи захисту комерційної таємниці від розголошення.
8. Охарактеризуйте правові норми забезпечення безпеки і захисту інформації на підприємстві.
9. Назвіть основні законодавчі акти України, що стосуються ІБ.
10. Охарактеризуйте основні законодавчі акти щодо ІБ в різних країнах світу.
11. Охарактеризуйте основні положення "Помаранчевої книги".
12. Охарактеризуйте основні положення специфікації X.800.
13. Проаналізуйте основні положення "Загальних критеріїв".

Людині потрібно два роки, щоб навчитися говорити, і шістдесят років, щоб навчитися тримати язик за зубами.

Л. Фейхтвангер

3.1 ОСНОВНІ КЛАСИ ОРГАНІЗАЦІЙНИХ ЗАХОДІВ

Організаційний захист забезпечує:

- організацію охорони та режиму;
- роботу з персоналом;
- роботу з документацією та іншими носіями інформації;
- використання технічних засобів безпеки;
- інформаційно-аналітичну діяльність щодо виявлення внутрішніх та зовнішніх загроз підприємницькій діяльності.

Організаційний захист – це регламентація виробничої діяльності і взаємин виконавців на нормативно-правовій основі, що виключає чи істотно утрудняє неправомірне оволодіння конфіденційною інформацією та прояв внутрішніх і зовнішніх загроз.

В українських компаніях накопичено багатий досвід регламентації і реалізації організаційних (процедурних) заходів, але вони прийшли з "до-комп'ютерного" минулого і тому потребують переоцінювання.

Важливим є усвідомлення ступеня залежності сучасного суспільства від комп'ютерної обробки даних. Суспільству потрібно роз'яснювати не тільки переваги, але і небезпеки, пов'язані з використанням інформаційних технологій. Акцент у забезпеченні ІБ слід робити не на військовій або кримінальній стороні справи, а на цивільних аспектах, пов'язаних з підтримкою нормального функціонування апаратного і програмного забезпечення, тобто концентруватися на питаннях доступності і цілісності даних.

Організаційні заходи поділяються на:

- управління персоналом;
- фізичний захист;
- підтримка працездатності;
- реагування на порушення режиму безпеки;
- планування відновлювальних робіт.

3.1.1 Управління персоналом

Управління персоналом починається зі складання опису посади, а потім з прийому нового співробітника на роботу. Вже на даному етапі бажано підключити до роботи фахівця з інформаційної безпеки для визначення комп'ютерних привілеїв, що асоціюються з посадою. Існує два загальні принципи, які варто мати на увазі: розділення обов'язків та мінімізація привілеїв.

Принцип розділення обов'язків зобов'язує так розподіляти ролі і відповідальність, щоб одна людина не могла порушити критично важливий для організації процес. Наприклад, процедурні обмеження дій суперкористувача. Можна штучно "розділити" пароль суперкористувача, повідомивши першу його частину одному співробітнику, а другу – іншому. Тоді критично важливі дії з адміністрування ІС вони зможуть виконати тільки удвох, що знижує вірогідність помилок і зловживань.

Принцип мінімізації привілеїв полягає у виділенні користувачам тільки тих прав доступу, які необхідні їм для виконання службових обов'язків. Призначення цього принципу очевидне – зменшити збиток від випадкових або навмисних некоректних дій.

Попереднє складання опису посади дозволяє оцінити її критичність і спланувати процедуру перевірки і відбору кандидатів. Чим відповідальніша посада, тим ретельніше потрібно перевіряти кандидатів: навести довідки про них, можливо, поговорити з колишніми товаришами по службі тощо. Подібна процедура може бути тривалою і дорогою, тому немає сенсу додатково ускладнювати її. В той же час, не можна зовсім відмовлятися від попередньої перевірки, щоб випадково не взяти на роботу людину з кримінальним минулим або психічним захворюванням.

Коли кандидат визначений, він повинен пройти навчання або, принаймні, його слід детально ознайомити із службовими обов'язками, а також з нормами і процедурами інформаційної безпеки. Бажано, щоб заходи безпеки були їм засвоєні до вступу на посаду і до введення його системного рахунка з вхідним ім'ям, паролем і привілеями.

З моменту введення системного рахунка починається його адміністрування, а також протоколювання й аналіз дій користувача. Поступово змі-

нюється оточення, в якому працює користувач, його службові обов'язки і т.п. Все це вимагає відповідної зміни привілеїв. Технічну складність представляють тимчасові переміщення користувача, виконання ним обов'язків замість співробітника, що пішов у відпустку, та інші обставини, коли повноваження потрібно спочатку надати, а через деякий час скасувати. В такі періоди профіль активності користувача різко змінюється, що створює труднощі при виявленні підозрілих ситуацій. Певної обережності треба дотримуватися і при видачі нових постійних повноважень, не забуваючи ліквідовувати старі права доступу.

Ліквідація системного рахунка користувача, особливо у разі конфлікту між співробітником і організацією, повинна проводитися максимально оперативно. Можливо і фізичне обмеження доступу до робочого місця. Зрозуміло, якщо співробітник звільняється, у нього потрібно прийняти все його комп'ютерне господарство і, зокрема, криптографічні ключі, якщо використовувалися засоби шифрування.

В зв'язку з кризовою ситуацією в економіці компанія Microsoft наполегливо рекомендує компаніям та організаціям використовувати шифрування важливих даних та закривати доступ до внутрішньої мережі для звільнених або таких, що будуть звільнені, співробітників.
http://news.bbc.co.uk/

Управління співробітниками розповсюджується також на осіб, що працюють за контрактом (наприклад, фахівців фірми-постачальника, що допомагають запустити нову систему). Відповідно до принципу мінімізації привілеїв, їм потрібно виділити рівно стільки прав, скільки необхідно, і скасувати ці права відразу після закінчення контракту. Проблема, проте, полягає в тому, що на початковому етапі впровадження "зовнішні" співробітники адмініструватимуть "місцевих", а не навпаки. Тут на перший план виходить кваліфікація персоналу організації та його здатність швидко навчатися. Важливі і принципи вибору ділових партнерів.

Іноді зовнішні організації беруть на обслуговування і адміністрування відповідальні компоненти комп'ютерної системи, наприклад, мережеве устаткування. Нерідко адміністрування виконується у віддаленому режимі.

Взагалі кажучи, це створює в системі додаткові вразливі місця, які необхідно компенсувати посиленим контролем засобів віддаленого доступу або навчанням власних співробітників.

Отже, проблема навчання – одна з основних з погляду інформаційної безпеки. Якщо співробітник не знайомий з політикою безпеки своєї організації, він не може прагнути до досягнення сформульованої в ній мети. Не знаючи заходів безпеки, він не зможе їх дотримувати. Навпаки, якщо співробітник знає, що його дії протоколюються, він, можливо, утримається від порушень.

3.1.2 Фізичний захист

Безпека ІС залежить від оточення, в якому ця ІС функціонує. Необхідно вжити заходів для захисту будівель і прилеглої території, інфраструктури, обчислювальної техніки, носіїв даних.

Основний принцип фізичного захисту, дотримання якого слід постійно контролювати, формулюється як "безперервність захисту у просторі та часі".

Фізичний захист здійснюється за такими напрямками:

- фізичне управління доступом;
- протипожежні заходи;
- захист інфраструктури;
- захист від перехоплення даних;
- захист мобільних систем.

Заходи фізичного управління доступом дозволяють:

- контролювати і, в разі необхідності, обмежувати вхід і вихід співробітників і відвідувачів;
- виключити можливості таємного проникнення на територію та у приміщення сторонніх осіб;
- забезпечити зручність контролю проходу і переміщення співробітників і відвідувачів;

Прибиральниця просить у директора банку:
- Чи не могли б Ви дати мені ключі від сховища? А то мені доводиться кожен день по 20 хвилин морочитися зі шпилькою, щоб його відкрити та прибратися.

- створити окремі виробничі зони за типом конфіденційних робіт із самостійними системами доступу;
- контролювати дотримання часового режиму праці і перебування на території персоналу фірми;
- організувати і підтримувати надійний пропускний режим.

Важливо зробити так, щоб відвідувачі, по можливості, не мали безпосереднього доступу до комп'ютерів або, в крайньому випадку, потурбуватися про те, щоб від вікон і дверей не були видимими екрани моніторів і принтери. Необхідно, щоб відвідувачів на вигляд можна було відрізнити від співробітників.

Протипожежні заходи мають розробляти і реалізовувати професіонали пожежники. Однак, у будь-якому разі, основним заходом є встановлення протипожежної сигналізації і автоматичних засобів пожежогасіння.

До підтримуючої інфраструктури відносять системи електро-, водо- і теплопостачання, кондиціонери і засоби комунікацій. До них застосовні ті ж вимоги цілісності і доступності, що і до інформаційних систем. Для забезпечення цілісності потрібно захищати устаткування від крадіжок і пошкоджень. Для підтримки доступності слід вибирати устаткування з максимальним часом напрацювання на відмову, дублювати важливі вузли і завжди мати під рукою запчастини.

Перехоплення даних може здійснюватися найрізноманітнішими способами. Зловмисник може підглядати за екраном монітора, читати пакети, передані по мережі, здійснювати аналіз побічних електромагнітних випромінювань і наведень тощо. Захист від перехоплення даних можна забезпечити використанням криптографії, максимальним розширенням контрольованої території, контролем лінії зв'язку (наприклад, укладати їх в надувну оболонку з виявленням проколювання). Однак найрозумніше – усвідомити, що для комерційних систем забезпечення конфіденційності є все-таки не головним завданням.

Основна загроза **мобільним і портативним комп'ютерам** – це їхнє викрадення. Тому важливо не залишати їх без нагляду в автомобілі або на роботі.

Сумна статистика останніх інцидентів показую всю ненадійність захисту мобільних систем:

- В 2008 р. мобільний комп'ютер з секретними даними було вкрадено з автомобіля однієї з перших осіб Пентагону.
- З липня по жовтень 2007 р. Bank of Ireland, другий за величиною банк в Ірландії, втратив чотири ноутбуки з іменами громадян країни, їх адресами, відомостями про банківські рахунки та медичною інформацією.
- У вересні 2008 р. з Національного банку Канади серед робочого дня грабіжник виніс ноутбук з даними тисяч клієнтів іпотечної програми.
- За статистикою в аеропортах США губиться близько 20 тис. ноутбуків та мобільних телефонів, причому лише за половиною з них повертаються.

Взагалі кажучи, при виборі засобів фізичного захисту слід проводити аналіз ризиків. Так, ухвалюючи рішення про закупівлю джерела безперебійного живлення, необхідно врахувати якість електроживлення в будівлі, займаній організацією, характер і тривалість збоїв електроживлення, вартість доступних джерел і можливі втрати від аварій (поломка техніки, припинення роботи організації тощо). В той же час, у багатьох випадках рішення очевидні. Заходи протипожежної безпеки обов'язкові для всіх організацій. Вартість реалізації багатьох заходів (наприклад, установлення звичайного замка на двері серверної кімнати) мала або явно менша, ніж можливий збиток.

3.1.3 Підтримка працездатності

Відсутність заходів, спрямованих на підтримку працездатності ІС, призводить до найбільшої небезпеки. Ненавмисні помилки системних адміністраторів і користувачів загрожують пошкодженням апаратури, руйнуванням програм і даних, а, у кращому разі, вони створюють проломи в захисті, які роблять можливою реалізацію загроз.

Недооцінювання чинників безпеки в повсякденній роботі – проблема багатьох організацій. Дорогі засоби безпеки втрачають сенс, якщо вони погано документовані, конфліктують з іншим програмним забезпеченням, а пароль системного адміністратора не змінювався тривалий час.

Напрямками повсякденної діяльності є:

- **підтримка користувачів** – це перш за все, консультування і надання допомоги при вирішенні різного роду проблем. Іноді в орга-

нізаціях створюють для цієї мети спеціальний "довідковий стіл", але частіше цим займається системний адміністратор. Доцільно фіксувати питання користувачів, щоб виявляти їх типові помилки і розробляти пам'ятки з рекомендаціями;

З документації до бухгалтерської програми:
«Програма NN має складну структуру, тому для спрощення роботи з NN надається спеціальна навчальна програма BRNN, на даний момент не розроблена»

- **підтримка програмного забезпечення** – один з найважливіших засобів забезпечення цілісності інформації. Перш за все, необхідно стежити за тим, яке програмне забезпечення встановлено на комп'ютерах. Якщо користувачі встановлюватимуть програми на свій розсуд, це може призвести до зараження шкідливим ПЗ. Другий аспект підтримки ПЗ – контроль за відсутністю неавторизованої зміни програм і права доступу до них. Сюди ж можна віднести підтримку еталонних копій програмних систем;
- **конфігураційне управління** дозволяє контролювати і фіксувати зміни, що вносяться до програмної конфігурації. Перш за все, необхідно застрахуватися від випадкових або непродуманих модифікацій, вміти, як мінімум, повертатися до попередньої робочої версії;
- **резервне копіювання** необхідне для відновлення програм і даних після аварій. Потрібно налагодити розміщення копій в безпечному місці, захищеному від несанкціонованого доступу, пожеж, витоків, тобто від усього, що може призвести до крадіжки або пошкодження носіїв. Доцільно мати декілька екземплярів резервних копій і частину з них зберігати поза територією організації, захищаючись таким чином від крупних аварій і подібних інцидентів;
- **управління носіями** необхідно для забезпечення фізичного захисту і обліку носіїв електронної інформації та друкарських копій. Управління носіями повинно забезпечувати конфіденційність, цілісність і доступність інформації, що зберігається поза комп'ютерною системою;

- **документування** – невід'ємна частина інформаційної безпеки. Важливо, щоб документація була актуальною, відображала саме поточний стан подій, причому в несуперечливому вигляді. До зберігання одних документів (що містять, наприклад, аналіз вразливих місць системи і загроз) можна застосовувати вимоги забезпечення конфіденційності, до інших, таких як план відновлення після аварій, – вимоги цілісності і доступності (у критичній ситуації план необхідно знайти і прочитати);
- **регламентні роботи** – дуже серйозна загроза безпеці. Співробітник, що здійснює регламентні роботи, дістає винятковий доступ до системи, і на практиці дуже важко проконтролювати, які саме дії він здійснює. Тут на перший план виходить ступінь довіри до тих, хто виконує ці роботи.

3.1.4 Реагування на порушення режиму безпеки

Програма безпеки, прийнята організацією, повинна передбачати набір оперативних заходів, спрямованих на виявлення і нейтралізацію порушень режиму інформаційної безпеки. Важливо, щоб послідовність дій була спланована наперед, оскільки заходи потрібно вживати терміново та скоординовано.

Реагування на порушення режиму безпеки має забезпечити:

- локалізацію інциденту і зменшення шкоди, що завдається;
- виявлення порушника;
- попередження повторних порушень.

В організації повинна бути людина, доступна 24 години на добу (особисто, по телефону або електронній пошті), яка відповідає за реагування на порушення. Всі повинні знати координати цієї людини і звертатися до неї при перших ознаках небезпеки. Загалом, як при пожежі, потрібно знати, куди дзвонити, і що робити до приїзду пожежної команди.

Співробітники відділу захисту інформації приходять і уходять, а хакери залишаються (наслідок девізу Джоунза)
"Закони Мерфі для інформаційної безпеки" А.В. Лукацький

Часто вимога локалізації інциденту і зменшення шкоди, що завдається, вступає в конфлікт з бажанням виявити порушника. В політиці безпеки організації пріоритети повинні бути розставлені наперед.

Щоб запобігти повторним порушенням, необхідно аналізувати кожен інцидент, виявляти причини, накопичувати статистику. Які джерела шкідливого ПЗ? Які користувачі мають звичай вибирати слабкі паролі? На подібні питання і повинні дати відповідь результати аналізу.

Необхідно відстежувати появу нових вразливих місць і якнайшвидше ліквідовувати асоційовані з ними вікна небезпеки. Хтось в організації повинен займатися цим процесом, вживати короткострокових заходів і коректувати програму безпеки для вживання довгострокових заходів.

3.1.5 Планування відновлювальних робіт

Жодна організація не застрахована від серйозних аварій, викликаних природними причинами, діями зловмисника, халатністю або некомпетентністю. В той же час у кожній організації є функції, які керівництво вважає критично важливими і які повинні виконуватися, не дивлячись ні на що. Планування відновлювальних робіт дозволяє підготуватися до аварій, зменшити збиток від них і зберегти здатність до функціонування хоч би в мінімальному обсязі.

Заходи інформаційної безпеки розділяються на групи, залежно від того, спрямовані вони на попередження, виявлення чи ліквідацію наслідків атак. Більшість заходів носить попереджувальний характер. Оперативний аналіз реєстраційної інформації і деякі аспекти реагування на порушення (так званий активний аудит) служать для виявлення і відбиття атак.

Планування відновлювальних робіт відносять до останньої з трьох перерахованих груп. Процес планування відновлювальних робіт складається з таких етапів:

- виявлення критично важливих функцій організації, встановлення пріоритетів;

- ідентифікація ресурсів, необхідних для виконання критично важливих функцій;
- визначення переліку можливих аварій;
- розробка стратегії відновлювальних робіт;
- підготовка до реалізації вибраної стратегії;
- перевірка стратегії.

Плануючи відновлювальні роботи, слід усвідомлювати те, що повністю зберегти функціонування організації не завжди можливо. Необхідно виявити критично важливі функції, без яких організація втрачає свою особливість, і, навіть, серед критичних функцій розставити пріоритети, щоб найшвидше і з мінімальними витратами відновити роботу після аварії.

Ідентифікуючи ресурси, необхідні для виконання критично важливих функцій, слід пам'ятати, що багато з них має некомп'ютерний характер. На даному етапі бажано підключати до роботи фахівців різного профілю, здатних у сукупності охопити всі аспекти проблеми. Критичні ресурси, зазвичай, відносять до однієї з категорій:

- персонал;
- інформаційна інфраструктура;
- фізична інфраструктура.

Складаючи списки відповідальних фахівців, слід враховувати, що деякі з них можуть безпосередньо постраждати від аварії (наприклад, від пожежі), хтось може знаходитися в стані стресу, частина співробітників, можливо, буде позбавлена можливості потрапити на роботу (наприклад, у разі масових безладів). Бажано мати деякий резерв фахівців або наперед визначити канали, якими можна на певний час залучити додатковий персонал.

Інформаційна інфраструктура складається з таких елементів:

- комп'ютери;
- програми і дані;
- інформаційні сервіси зовнішніх організацій;
- документація.

Потрібно підготуватися до того, що на запасному місці, куди органі-

зація буде евакуйована після аварії, апаратна платформа може відрізнятися від базової. Відповідно, слід продумати заходи підтримки сумісності з програмою і даними.

До фізичної інфраструктури належать будівлі, інженерні комунікації, засоби зв'язку, оргтехніка і багато іншого. Комп'ютерна техніка не може працювати в поганих умовах, без стабільного електроживлення тощо.

Аналізуючи критичні ресурси, доцільно врахувати часовий профіль їх використання. Більшість ресурсів потрібні постійно, але в деяких потреба може виникати тільки в певні періоди (наприклад, в кінці місяця або року при складанні звіту).

При **визначенні переліку можливих аварій** потрібно спробувати розробити їх сценарії.

Стратегія відновлювальних робіт повинна базуватися на наявних ресурсах і не бути дуже накладною для організації. При розробці стратегії доцільно провести аналіз ризиків, яким піддаються критичні функції, і спробувати вибрати найбільш економічне рішення. Стратегія повинна передбачати не тільки роботу за тимчасовою схемою, але і повернення до нормального функціонування.

Підготовка до реалізації вибраної стратегії полягає у розробці плану дій в екстрених ситуаціях і після їх закінчення, а також у забезпеченні деякої надмірності критичних ресурсів. Останнє можливо і без великих витрат засобів, якщо укласти з однією або декількома організаціями угоди про взаємну підтримку у разі аварій. Ті, хто не постраждав, надають частину своїх ресурсів у тимчасове користування постраждалим.

Надмірність забезпечується також заходами резервного копіювання, зберіганням копій в декількох місцях, представленням інформації в різних видах (на папері та у файлах) тощо.

Має сенс укласти угоду з постачальниками інформаційних послуг про першочергове обслуговування в критичних ситуаціях або укладати угоди з декількома постачальниками. Однак такі заходи вимагають певних витрат.

Перевірка стратегії проводиться шляхом аналізу підготовленого плану, вжитих і намічених заходів.

3.2 СУБ'ЄКТИ КЕРУВАННЯ СИСТЕМОЮ КОРПОРАТИВНОЇ БЕЗПЕКИ

Під суб'єктами керування корпоративною безпекою розуміють ті підрозділи й окремих співробітників, хто цілеспрямовано впливає на систему з метою протидії факторам зовнішніх й внутрішніх загроз. До суб'єктів керування процесом забезпечення корпоративної безпеки компанії належать:

- вище керівництво;
- менеджер з безпеки;
- керівники основних підрозділів;
- служба персоналу;
- служба безпеки.

Керівництву фірми, компанії, організації належить ключова роль у розробці концепції корпоративної безпеки, визначенні необхідного рівня захисту, видачі санкцій на проведення оперативних заходів, у фінансуванні діяльності, що підтримує працездатність системи корпоративної безпеки.

Для рішення всіх цих завдань кожний керівник повинен бути ознайомлений хоча б з азами керування безпекою. Крім того, керівництво безпосередньо управляє інформаційно-аналітичним підрозділом і підрозділом маркетингової розвідки.

Людина, що знає як і куди правильно витратити гроші на інформаційну безпеку, і людина, яка їх виділяє - це завжди різні люди.
"Закони Мерфі для інформаційної безпеки" А.В. Лукацький

Менеджер з безпеки – це новий тип менеджера, основним завданням якого є координація дій всіх учасників процесу забезпечення корпоративної безпеки. Далеко не всі керівники фірм усвідомили необхідність введення в штат цієї посади, вважаючи, що наявність служби безпеки вирішує всі проблеми. Подібна думка помилкова, тому що в забезпеченні корпоративної безпеки, особливо у великих фірмах, бере участь велика кількість незалежних один від одного підрозділів, і координувати їхні дії повинен спеціально підготовлений менеджер, знайомий зі специфікою діяльності кожного з них.

Виходячи із цього, система психологічної безпеки має складатися з

підсистем заходів психологічної протидії факторам зовнішніх і внутрішніх загроз. Виявленням факторів загроз постійно займаються два підрозділи: служба безпеки і служба персоналу. При цьому служба безпеки більшою мірою орієнтована на вивчення факторів зовнішньої загрози. Служба персоналу – переважно на внутрішні.

Служба персоналу безпосередньо займається вирішенням таких завдань, як підбор і розстановка кадрів, моніторинг психологічного клімату, виявлення негативних тенденцій у колективі, атестація персоналу, звільнення співробітників.

Служба безпеки є самостійною організаційною одиницею підприємства, що підпорядковується безпосередньо керівникові підприємства. Очолює службу безпеки начальник служби в посаді заступника керівника підприємства з безпеки.

Діяльність служби безпеки спрямована на виконання таких загальних функцій:

- розвідувальних;
- контррозвідувальних;
- охоронних;
- фіскальних;
- каральних.

3.2.1 Служба персоналу

На всіх стадіях інформаційного процесу провідна роль належить людині. Від того, як будуть враховані в інформаційних процесах інтереси, психологічні установки, властивості особистості, залежить ефективність використання інформації.

Незважаючи на розмаїття і специфіку напрямків діяльності комерційних структур, можна виділити загальне для всіх фірм коло завдань забезпечення власної безпеки, що мають психологічну складову:

- професійний і психологічний відбір персоналу;

- профілактика, виявлення та розв'язання конфліктів різного походження;
- атестація персоналу;
- психологічне вивчення партнерів, конкурентів, представників кримінальних структур;
- розслідування надзвичайних подій;
- підготовка та проведення відповідальних переговорів різного рівня;
- психологічний захист інформації;
- навчання персоналу навичкам ефективної комунікації;
- психотерапія та психокорекція співробітників, що пережили складні або стресові ситуації.

З урахуванням цього діяльність служби персоналу здійснюється за такими напрямками:

- оцінювання й прогнозування надійності персоналу на стадії відбору;
- атестація персоналу;
- моніторинг психологічного клімату в підрозділах;
- виявлення груп корпоративного ризику.

Важливим індикатором явних і прихованих негативних процесів у колективі фірми або окремих її підрозділах є стан психологічного клімату. Найнебезпечнішими тенденціями є:

- поява неформальних лідерів;
- формування мікрогруп негативної спрямованості;
- поява знедолених, ізгоїв;
- виникнення конфліктів між окремими співробітниками й мікрогрупами.

Поява неформальних лідерів свідчить про зниження авторитету менеджерів, про порушення в управлінській вертикалі, про появу співробітників, що переросли свою роль у рамках команди.

Мікрогрупи з фатальною неминучістю утворюються в групах чисельністю більше 7 осіб. Найнебезпечнішими є мікрогрупи, які, переслідуючи свої групові цілі, вступають у конфлікт із іншими мікрогрупами, порушуючи тим самим ритм продуктивної діяльності всієї команди.

Поява в групі знедолених й великої кількості конфліктів є тривожним

симптомом, що свідчить про порушення внутрішньогрупових контактів. Знедолені через образу на всіх можуть стати каналом витоку інформації, що становить комерційну таємницю.

Створюючи умови для задоволення співробітником його потреб у самореалізації, у суспільному визнанні його значимості, можна в рамках фірми встановити сприятливий соціально-психологічний клімат, максимально знизити плинність кадрів, сформувати так званий "фірмовий патріотизм". У такій обстановці малоймовірна поява працівника, що буде намагатися самоствердитися шляхом передачі конкурентам секретів, тобто шляхом зрадництва.

Виходячи зі сказаного, необхідно в роботі з персоналом керуватися такими правилами:

- створити дієву систему матеріальних стимулів;
- забезпечити кожного співробітника довгостроковою роботою;
- ставитися до кожного співробітника як до самостійного індивіда;
- забезпечити участь у прибутках;
- створити можливості для просування по службі;
- забезпечити участь усього персоналу у формуванні рішень;
- створити гнучку систему звільнень, що не травмує.

Крім того, американські фахівці в галузі протидії промисловому шпигунству рекомендують:

- використовувати будь-яку можливість для пропаганди програм забезпечення економічної безпеки фірми;
- не забувати періодично винагороджувати співробітників фірми за успіхи в цій роботі;
- усіляко стимулювати участь співробітників фірми в реалізації програм забезпечення таємності.

На думку дослідників, для створення атмосфери інформаційної безпеки найбільш ефективні заходи пов'язані з підвищенням інформаційної культури на підприємстві.

Необхідно формувати чітку цільову настанову на підвищення надійності й відповідальності в питаннях захисту інформації. Так, у багатьох американських фірмах діє дворівнева система захисту інформації. Перший рівень – забезпечення інформаційної безпеки силами спецслужб, другий –

культивування атмосфери пильності та відповідальності за допомогою так званих координаторів, що призначаються із службовців середньої ланки.

Доцільно розбивати технологічний процес на ряд самостійних етапів, щоб службовці знали тільки частину секретів, а повне знання мало лише керівництво або вузьке коло осіб.

Необхідний постійний моніторинг стосунків між людьми, що працюють з інформацією, врахування їх морального та психологічного стану. Підставами для занепокоєння є: прояви емоційної неврівноваженості, невдоволення, хитрості, розчарування службовців, ідеї яких відкинуті.

Пропонується створювати систему внутріфірмової комунікації, що не допускає повної автономності окремих працівників.

У цілому, психологічне забезпечення комерційної таємниці в процесі відбору, підготовки, висування й звільнення кадрів ефективніше й дешевше, ніж при звичайному засекречуванні інформації.

Супровід персоналу є одним з невід'ємних елементів процесу забезпечення корпоративної безпеки кожної фірми й організації.

Супровід персоналу містить у собі:

- моніторинг співробітників;
- оцінювання динаміки й ступеня адаптації нового співробітника до робочого місця та колективу;
- визначення проблем, що виникають;
- навчання елементам самоменеджменту та ефективної комунікації;
- регулярна атестація співробітників;
- моніторинг психологічного клімату в колективі та у його окремих підрозділах;
- навчання персоналу (зокрема питанням забезпечення й підтримки корпоративної безпеки);
- звільнення.

Моніторинг співробітників необхідний для відстеження змін, що відбуваються зі співробітником у процесі роботи на фірмі, у компанії, організації й появи в нього якостей, що породжують загрозу корпоративній безпеці.

У багатьох компаніях серйозна увага приділяється питанням корпоративного навчання. Таке навчання сприяє виробленню згуртованості, пі-

двищенню працездатності команди, допомагає сформувати резерв на висування.

Поряд з обговоренням професійних питань, у ході навчання повинні розглядатися різні аспекти особистої й корпоративної безпеки.

Основними напрямками навчання можуть стати:

- правила роботи з документами, що містять комерційну таємницю;
- прийоми й методи, використовувані в промисловому шпигунстві;
- ефективна ділова комунікація;
- дії в екстремальних ситуаціях;
- тактика ведення переговорів і протидія маніпулятивному впливу;
- питання особистої безпеки при знаходженні за межами фірми.

Рекомендуються такі заходи щодо забезпечення інформаційної безпеки при звільненні співробітника. Про наміри співробітника звільнитися побічно свідчить відвідування відповідних сайтів в Інтернеті, розсилання резюме. З цього моменту все листування з робочої адреси та деякі операції на комп'ютері повинні бути взяті під негласний контроль. Якомога швидше під час відсутності даного користувача необхідно зробити резервну копію всіх його файлів. Беручи до уваги, що співробітник може змінити свої наміри та залишитися, а також припускаючи, що перегляд вакансій міг здійснюватися на прохання його знайомих, що шукають роботу, немає необхідності вживати відразу явних заходів безпеки.

Якщо співробітник оголосив про своє звільнення, можна вжити таких заходів:

- проінформувати всіх співробітників про майбутнє звільнення та заборонити передавати йому будь-яку або якусь конкретну інформацію, що стосується роботи;
- зробити резервну копію файлів користувача;
- організувати передачу справ;
- поступово, у міру передачі справ, скорочувати права доступу до інформації;
- при необхідності організувати супровід звільнення фахівцем з інформаційної безпеки.

Якщо співробітника викрито в промисловому шпигунстві, то необхідно:

- негайно позбавити його всіх прав доступу до інформаційної техніки;
- негайно скорегувати права доступу до загальних інформаційних ресурсів (баз даних, принтерів, факсів), перекрити входи в зовнішні мережі або змінити правила доступу до них;
- всі співробітники повинні змінити особисті паролі, при цьому до їхнього відома доводиться така інформація: "Співробітник N з (дата) не працює. У разі будь-яких спроб контакту з його боку негайно повідомляти службу безпеки";
- якийсь час контроль інформаційної системи здійснювати в посиленому режимі.

Якщо співробітник звільняється не через викриття в промисловому шпигунстві, то перераховані заходи не повинні бути надмірно наполегливими, щоб негативно не впливати на психологічний стан людини. Необхідно пояснити співробітникові, що таким є загальний порядок, і він особисто ні в чому не підозрюється.

Якщо співробітники побачать, що звільнення кожного працівника нерозривно пов'язане з моральним збитком, то постраждає загальний соціально-психологічний клімат: організація буде асоціюватися з в'язницею або сектою. Крім того, недоцільно псувати стосунки з усіма співробітниками, що звільняються: хтось може повернутися, а хтось – надати допомогу.

Якщо співробітника звільняють, викривши в промисловому шпигунстві, то процедура супроводу залишається на розсуд служби безпеки. Завдання служби персоналу полягає в тому, що події, які відбуваються, не повинні завдати шкоди соціально-психологічному клімату в колективі, а, по можливості, навпаки, консолідувати інших співробітників.

3.2.2 Служба безпеки

На **службу безпеки підприємства (СБ)** (фірми, організації) покладаються такі функції:

- організація і забезпечення охорони персоналу, матеріальних і фінансових цінностей і захисту конфіденційної інформації;
- забезпечення пропускного і внутріоб'єктового режиму на території, у будинках і приміщеннях, контроль за дотриманням вимог режиму

співробітниками, суміжниками, партнерами і відвідувачами;

- керівництво роботами з правового й організаційного регулювання заходів із захисту інформації;
- участь у розробці основних документів з метою закріплення в них вимог забезпечення безпеки і захисту інформації, а також положень про підрозділи, трудових договорів, угод, підрядів, посадових інструкцій і обов'язків керівництва, фахівців, робітників та службовців;
- розробка і здійснення разом з іншими підрозділами заходів щодо забезпечення роботи з документами, що містять конфіденційні відомості, під час виконання всіх видів робіт;
- вивчення всіх сторін виробничої, комерційної, фінансової й іншої діяльності для виявлення і наступної протидії будь-яким спробам нанесення збитку, ведення обліку й аналізу порушень режиму безпеки, нагромадження й аналіз даних про злочинні спроби конкурентних та інших організацій, про діяльність підприємства і його клієнтів, партнерів, суміжників;
- організація і проведення службових розслідувань за фактами розголошення відомостей, втрат документів, витоку конфіденційної інформації й інших порушень безпеки підприємства;
- розробка, ведення, відновлення і поповнення "Переліку відомостей конфіденційного характеру" та інших нормативних актів, що регламентують порядок забезпечення безпеки і захисту інформації;
- забезпечення строгого виконання вимог нормативних документів із захисту виробничих секретів підприємства;
- здійснення керівництва службами і підрозділами безпеки підвідомчих підприємств, організацій, установ і інших структур у частині умов, застережених у договорах;
- організація і регулярне проведення обліку співробітників підприємства і служби безпеки в усіх напрямках захисту інформації і забезпечення безпеки виробничої діяльності;
- ведення обліку і строгого контролю виділених для конфіденційної роботи приміщень, технічних засобів у них, що мають потенційні

канали витоку інформації і канали проникнення до джерел охоронюваних секретів;

- забезпечення проведення всіх необхідних заходів щодо припинення спроб нанесення морального і матеріального збитку з боку внутрішніх і зовнішніх загроз;
- підтримання контактів із правоохоронними органами і службами безпеки сусідніх підприємств в інтересах вивчення криміногенної обстановки в районі (зоні) і надання взаємної допомоги в кризових ситуаціях.

Керівником відділу захисту інформації призначають або відставного військового, або колишнього міліціонера, або колишнього співробітника 1-го відділу.

"Закони Мерфі для інформаційної безпеки" А.В. Лукацький

Така багатоплановість діяльності визначає складність структури служби.

Залежно від прийнятої концепції безпеки особовий склад служби безпеки може бути як постійною, так і змінною частиною персоналу компанії. Постійною частиною вона вважається в тому випадку, якщо співробітники служби безпеки є одночасно співробітниками компанії. Змінною - якщо співробітники служби безпеки є відрядженими до фірми співробітниками якого-небудь приватного охоронного підприємства.

Політика фірми стосовно служби безпеки може реалізовуватися в одній з таких форм:

- для виконання охоронних функцій запрошується охоронна фірма;
- охоронні функції покладають на охоронну фірму, а питання внутрішньої безпеки та захисту інформації забезпечуються силами власної служби безпеки;
- всі питання корпоративної безпеки вирішуються силами власної служби безпеки.

Передати свою безпеку на аутсорсінг - значить втратити контроль над мережею. Не передати - втратити контроль ще швидше.

"Закони Мерфі для інформаційної безпеки" А.В. Лукацький

Кожний із запропонованих варіантів має свої сильні й слабкі сторони.

У **першому варіанті**, віддавши функції охорони професіоналам, керівництво фірми позбувається необхідності вирішувати питання забезпечення цілісності й недоторканності власних об'єктів. Але, купуючи послуги охоронних фірм, варто враховувати, що при цьому втрачаються функції контролю за якістю підбору виконавців, їхньою кваліфікацією й професійною надійністю. Поза зоною уваги залишається велике коло питань, що мають істотне значення для створення комплексної системи безпеки, тому що ці питання носять глибоко інтимний характер для фірми і їх не можна довіряти стороннім.

Другий варіант кращий, тому що він припускає поділ функцій. Рутинна робота з фізичної охорони об'єктів покладається на охоронну фірму, а питання забезпечення внутрішньої безпеки, захисту інформаційних потоків, маркетингової розвідки є компетенцією власної служби безпеки.

Одним з недоліків цього варіанта є необхідність координації дій між двома фактично самостійними й незалежними структурами, що працюють на одну мету.

Третій варіант фактично позбавлений недоліків двох інших, але, вибираючи його, керівництво фірми змушене брати на себе вирішення питань щодо розробки власної концепції та власної політики корпоративної безпеки.

Структура, чисельність і завдання служби корпоративної безпеки розробляються на підставі результатів експертизи, поданої у формі розгорнутого висновку.

У відділі захисту інформації завжди не вистачає людей.
"Закони Мерфі для інформаційної безпеки" А.В. Лукацький

Повнокровна служба безпеки складається з таких підрозділів:

- підрозділ режиму й охорони;
- спеціальний підрозділ обробки документів конфіденційного характеру;
- інженерно-технічний підрозділ;
- інформаційно-аналітичний підрозділ.

Таку службу безпеки може собі дозволити тільки досить багата

фірма, що має численний персонал.

Більшість середніх і малих комерційних фірм обмежуються службою безпеки, орієнтованою, насамперед, на виконання охоронних функцій.

Займаючись виконанням своїх функціональних завдань, співробітники служби безпеки також повинні вирішувати специфічні проблеми, до яких належать:

- профілактика спроб здійснення протиправних дій відносно керівництва й співробітників фірми;
- попереднє розслідування надзвичайних подій, фактів використання наркотиків, шахрайства, злодійства серед співробітників компанії;
- розробка й підтримка системи охоронних заходів щодо захисту службовців, власності, клієнтів і гостей фірми;
- створення й підтримка системи інформаційної безпеки;
- взаємодія з місцевою владою та правоохоронними органами у випадку проведення різних розслідувань та ін.;
- проведення й координація розслідувань негативних явищ, особливо випадків присвоєння грошей службовцями, конфліктів інтересів і інших серйозних випадків, що загрожують корпоративній безпеці;
- забезпечення технічної та професійної підтримки всім членам правління у випадку висування обвинувачень проти них або проведення дізнання за підозрою в здійсненні протиправних діянь;
- періодична перевірка всіх приміщень компанії на відповідність вимогам безпеки;
- здійснення спецперевірки кандидатів на роботу.

3.3 ПОЛІТИКА БЕЗПЕКИ ОРГАНІЗАЦІЇ

3.3.1 Поняття політики безпеки

Головна задача керівництва організації щодо інформаційної безпеки – сформувати програму робіт у галузі інформаційної безпеки і забезпечити її виконання, виділяючи необхідні ресурси і контролюючи стан подій.

Основою програми є **політика безпеки**, що відображає підхід організації до захисту своїх інформаційних активів. Керівництво кожної організації повинне усвідомлювати необхідність підтримки режиму безпеки і виділення на ці цілі значних ресурсів.

Політика безпеки будується на основі аналізу ризиків, які визнаються реальними для ІС організації. Коли ризики проаналізовано і стратегію захисту визначено, тільки тоді складається програма забезпечення інформаційної безпеки. Під цю програму виділяються ресурси, призначаються відповідальні, визначається порядок контролю виконання програми тощо.

Термін "політика безпеки" є не зовсім точним перекладом англійського словосполучення "Security policy", проте в даному випадку калька краще відображає сенс цього поняття, ніж лінгвістично правильний переклад "правила безпеки". Тут мова йде не про окремі правила або їх набори, а про стратегію організації у галузі інформаційної безпеки. Для вироблення стратегії і втілення її в життя потрібні політичні рішення, що приймаються на найвищому рівні керівництва організації, установи чи підприємства.

Політика безпеки – це сукупність документованих рішень, що приймаються керівництвом організації і спрямовані на захист інформації та асоційованих з нею ресурсів.

Аналітична фірма Gartner Group виділяє 4 рівні зрілості компанії з точки зору забезпечення інформаційної безпеки:

0-й рівень:

- інформаційною безпекою в компанії ніхто не займається, керівництво компанії не усвідомлює важливості проблем інформаційної безпеки;
- фінансування відсутнє;
- інформаційна безпека реалізується штатними засобами операційних систем, СКБД і додатків (парольний захист, розмежування доступу до ресурсів і сервісів).

1-й рівень:

- інформаційна безпека розглядається керівництвом як чисто «технічна» проблема, відсутня єдина програма (концепція, політика)

розвитку системи забезпечення інформаційної безпеки компанії;

- фінансування здійснюється в рамках загального IT-бюджету;
- інформаційна безпека реалізується засобами нульового рівня плюс засоби резервного копіювання, «антивірусні» засоби, міжмережеві екрани, засоби організації VPN (віртуальних приватних мереж), тобто традиційні засоби захисту.

2-й рівень:

- інформаційна безпека розглядається керівництвом як комплекс організаційних і технічних заходів, існує розуміння важливості інформаційної безпеки для виробничих процесів, є затверджена керівництвом програма розвитку системи забезпечення інформаційної безпеки компанії;
- фінансування ведеться в рамках окремого бюджету;
- інформаційна безпека реалізується засобами першого рівня плюс засоби посиленої автентифікації, засоби аналізу поштових повідомлень і web-контенту, системи виявлення вторгнень, засоби аналізу захищеності та організаційні заходи (внутрішній і зовнішній аудит, аналіз ризиків, політика інформаційної безпеки, положення, процедури та регламенти).

3-й рівень:

- інформаційна безпека є частиною корпоративної культури, призначено менеджера з питань забезпечення інформаційної безпеки;
- фінансування здійснюється в рамках окремого бюджету;
- інформаційна безпека реалізується засобами другого рівня плюс системи управління інформаційною безпекою.

3.3.2 Розробка політики безпеки

З практичної точки зору політику безпеки доцільно розглядати на трьох рівнях деталізації.

До верхнього рівня належать рішення, що стосуються організації в цілому. Вони мають загальний характер і, як правило, виходять від керівницт-

ва організації. Список подібних рішень може складатися з таких елементів:

- рішення про формування або перегляд комплексної програми забезпечення інформаційної безпеки, призначення відповідальних за реалізацію програми;
- формулювання цілей, до яких прагне організація у галузі інформаційної безпеки, визначення загальних напрямків досягнення цих цілей;
- забезпечення бази для дотримання законів і правил;
- формулювання адміністративних рішень з тих питань реалізації програми безпеки, які повинні розглядатися на рівні організації в цілому.

Для політики верхнього рівня цілі організації в галузі інформаційної безпеки формулюються у термінах цілісності, доступності і конфіденційності. Якщо організація відповідає за підтримку критично важливих баз даних, на першому плані може стояти зменшення кількості втрат, пошкоджень або спотворень даних. Для організації, що займається продажем комп'ютерної техніки, ймовірно, важлива актуальність інформації про послуги і ціни та її доступність максимальній кількості потенційних покупців. Керівництво режимного підприємства в першу чергу піклується про захист від несанкціонованого доступу, тобто про конфіденційність.

На верхній рівень виносять управління захисними ресурсами і координація використання цих ресурсів, виділення спеціального персоналу для захисту критично важливих систем і взаємодія з іншими організаціями, що забезпечують або контролюють режим безпеки.

Політика верхнього рівня повинна чітко окреслювати сферу свого впливу. Можливо, це будуть всі комп'ютерні системи організації (або навіть більше, якщо політика регламентує деякі аспекти використання співробітниками своїх домашніх комп'ютерів). Можлива, проте, і така ситуація, коли до сфери впливу включаються лише найважливіші системи.

У політиці ІБ повинні бути визначені обов'язки посадовців щодо створення програми безпеки і впровадження її в життя.

Політика верхнього рівня має справу з трьома аспектами законопокірності і виконавської дисципліни:

- організація повинна дотримуватися існуючих законів;
- слід контролювати дії осіб, відповідальних за створення програми безпеки;
- необхідно забезпечити певний ступінь старанності персоналу, а для цього потрібно створити систему заохочень і покарань.

На верхній рівень слід виносити тільки ті питання, які забезпечують значну економію засобів, або без яких неможливо обійтися.

Британський стандарт BS 7799:1995 рекомендує включати до документа, що характеризує політику безпеки організації, такі розділи:

- вступний, який підтверджує заклопотаність вищого керівництва проблемами інформаційної безпеки;
- організаційний, що містить опис підрозділів, комісій, груп і т.д., які відповідають за роботи у галузі інформаційної безпеки;
- класифікаційний, що описує наявні в організації матеріальні і інформаційні ресурси і необхідний рівень їх захисту;
- штатний, що характеризує заходи безпеки, вживані до персоналу (опис посад з погляду інформаційної безпеки, організація навчання і перепідготовки персоналу, порядок реагування на порушення режиму безпеки і т.п.);
- розділ, який висвітлює питання фізичного захисту;
- розділ, який описує підхід до управління комп'ютерами і комп'ютерними мережами;
- розділ, що описує правила розмежування доступу до виробничої інформації;
- розділ, що характеризує порядок розробки і супроводу систем;
- розділ, що описує заходи, спрямовані на забезпечення безперервної роботи організації;
- юридичний розділ, який підтверджує відповідність політики безпеки чинному законодавству.

До середнього рівня відносять питання, що стосуються окремих аспектів інформаційної безпеки, але важливі для різних експлуатованих організацією систем. Приклади таких питань – ставлення до передових (але, можливо, недостатньо перевірених) технологій, доступ до Internet (як сумістити

свободу доступу до інформації із захистом від зовнішніх загроз?), використання домашніх комп`ютерів, застосування користувачами неліцензійного програмного забезпечення і т.д.

Політика середнього рівня повинна для кожного аспекту висвітлювати такі теми.

Опис аспекту. Наприклад, якщо розглянути застосування користувачами неофіційного програмного забезпечення, останнє можна визначити як таке, що не було схвалене та/або куплене на рівні організації.

Область застосування. Слід визначити, де, коли, як, стосовно кого і чому застосовується дана політика безпеки. Наприклад, чи торкається політика, пов'язана з використанням неліцензійного програмного забезпечення, організацій-субпідрядників? Чи стосується вона співробітників, що користуються портативними і домашніми комп'ютерами і змушених переносити інформацію на виробничі машини?

Як би добре не була написана політика безпеки, завжди знайдеться використовувана у вас технологія, що не врахована в ній.
"Закони Мерфі для інформаційної безпеки" А.В. Лукацький

Позиція організації за даним аспектом. Продовжуючи приклад з неофіційним програмним забезпеченням, можна уявити собі позиції повної заборони або розробки процедури приймання подібного програмного забезпечення. Позиція може бути сформульована і в набагато більш загальному вигляді, як набір цілей, до яких прагне організація в даному аспекті. Взагалі стиль документів, що визначають політику безпеки (як і їх перелік), в різних організаціях можуть значно відрізнятися.

Ролі і обов'язки. В "політичний" документ необхідно включити інформацію про посадовців, відповідальних за реалізацію політики безпеки. Наприклад, якщо для використання неофіційного програмного забезпечення співробітникам потрібен дозвіл керівництва, повинно бути відомо, у кого і як його можна одержати. Якщо неофіційне програмне забезпечення використовувати не можна, слід знати, хто стежить за виконанням даного правила.

Законослухняність. Політика повинна містити загальний опис заборонених дій і покарань за них.

Точки контакту. Повинно бути відомо, куди слід звертатися за роз'ясненнями, допомогою і додатковою інформацією. Звичайно "точкою контакту" служить певний посадовець, а не конкретна людина.

Політика безпеки *нижнього рівня* стосується конкретних інформаційних сервісів. Вона включає два аспекти – цілі і правила їх досягнення, тому її інколи важко відокремити від питань реалізації. На відміну від двох верхніх рівнів, дана політика повинна бути визначена детальніше. Є багато речей, специфічних для окремих видів послуг, які не можна однаково регламентувати в рамках усієї організації. В той же час, ці речі настільки важливі для забезпечення режиму безпеки, що рішення, які їх стосуються, повинні ухвалюватися на управлінському, а не технічному рівні. Наведемо декілька прикладів питань, на які слід дати відповідь у політиці безпеки нижнього рівня.

- Хто має право доступу до об'єктів, підтримуваних сервісом?
- За яких умов можна читати і модифікувати дані?
- Яким чином організовано віддалений доступ до сервісу?

При формулюванні цілей політики нижнього рівня можна виходити з міркування цілісності, доступності і конфіденційності, але не можна на цьому зупинятися. Її цілі повинні бути конкретнішими. Наприклад, якщо мова йде про систему розрахунку заробітної плати, можна поставити мету, щоб тільки співробітникам відділу кадрів і бухгалтерії дозволялося вводити і модифікувати інформацію. В більш загальному випадку цілі повинні зв'язувати між собою об'єкти сервісу і дії з ними.

З цілей виводяться правила безпеки, які описують, хто, що і за яких умов може робити. Чим докладніше правила, чим формальніше вони викладені, тим простіше підтримувати їх виконання програмно-технічними засобами. З іншого боку, дуже жорсткі правила можуть заважати роботі користувачів, тоді їх доведеться часто переглядати. Керівництво повинно знайти розумний компроміс, коли за прийнятну ціну буде забезпечений прийнятний рівень безпеки, а співробітники не будуть надмірно зв'язані. Зазвичай найформальніше задаються права доступу до об'єктів, зважаючи на особливу важливість даного питання.

Як тільки політику безпеки остаточно затверджено, вона вже остаточно застаріла.

"Закони Мерфі для інформаційної безпеки" А.В. Лукацький

3.3.3 Програма реалізації політики безпеки

Після того, як сформульована політика безпеки, можна приступати до складання програми її реалізації і власне до реалізації.

Щоб зрозуміти і реалізувати будь-яку програму, її потрібно структурувати за рівнями відповідно до структури організації. В простому і найпоширенішому випадку достатньо двох рівнів – верхнього, або центрального, який охоплює всю організацію, і нижнього, або службового, який стосується окремих послуг або груп однорідних сервісів.

Програму верхнього рівня очолює особа, яка відповідає за інформаційну безпеку організації. Головні цілі цієї програми такі:

- управління ризиками (оцінювання ризиків, вибір ефективних засобів захисту);
- координація діяльності у галузі інформаційної безпеки, поповнення і розподіл ресурсів;
- стратегічне планування;
- контроль діяльності в галузі інформаційної безпеки.

В рамках програми верхнього рівня ухвалюються стратегічні рішення із забезпечення безпеки, оцінюються технологічні новинки. Інформаційні технології розвиваються дуже швидко, і необхідно мати чітку політику відстеження і впровадження нових засобів.

Контроль діяльності в галузі безпеки має двосторонню спрямованість. По-перше, необхідно гарантувати, що дії організації не суперечать законам. При цьому слід підтримувати контакти із зовнішніми контролюючими організаціями. По-друге, потрібно постійно відстежувати стан безпеки всередині організації, реагувати на випадки порушень і доопрацьовувати захисні заходи з урахуванням зміни обстановки.

Слід підкреслити, *що програма верхнього рівня повинна займати*

строго певне місце в діяльності організації, вона повинна офіційно прийматися і підтримуватися керівництвом, а також мати певний штат і бюджет.

% Організації ICSA і SAIC організували опитування 745 респондентів у США, задавши їм питання: "Яка найбільша перешкода виникає перед вами при забезпеченні інформаційної безпеки?" Результати відповідей наведено у табл. 3.1.

Таблиця 3.1 – Результати опитування організацій США

Перешкода	Кількість респондентів, %
Обмеження бюджету	29
Недостатня підтримка з боку керівництва	14
Недостатній рівень кваліфікації співробітників і поінформованості кінцевого користувача	10
Некомпетентність персоналу, відповідального за інформаційну безпеку	9
Невідповідність внутрішній політиці безпеки	8
Недостатньо повноважень	8
Технічна складність	6
Незрозумілі обов'язки	4
Відсутність гарних засобів захисту	3
Інше	9

Аналіз цих результатів показує, що перешкодами на шляху забезпечення інформаційної безпеки є нестача фінансування та недостатня підтримка з боку керівництва.

Мета програми нижнього рівня – забезпечити надійний і економічний захист конкретного сервісу або групи однорідних сервісів. На цьому рівні вирішується, які слід використовувати механізми захисту, які купувати і встановлювати технічні засоби; виконується повсякденне адміністрування; відстежується стан слабких місць і т.п. Звичайно за програму нижнього рівня відповідають адміністратори сервісів.

3.3.4 Синхронізація програми безпеки з життєвим циклом систем

Якщо синхронізувати програму безпеки нижнього рівня з життєвим циклом сервісу, що захищається, можна досягти більшого ефекту з меншими витратами. Додати нову можливість вже готовій системі на порядок складніше, ніж спочатку спроектувати і реалізувати її. Те ж саме справедливо і для інформаційної безпеки.

У життєвому циклі інформаційного сервісу виділяються такі етапи та дії, що виконуються з позиції програми безпеки.

Ініціація. На даному етапі виявляється необхідність у придбанні нового сервісу, документується його передбачуване призначення.

З погляду інформаційної безпеки найважливішою дією тут є оцінювання критичності як самого сервісу, так і інформації, яка з його допомогою оброблятиметься.

Результати оцінювання критичності є відправним моментом у складанні специфікацій. Крім того, вони визначають ту міру уваги, яку служба безпеки організації повинна приділяти новому сервісу на подальших етапах його життєвого циклу.

Закупівля. На даному етапі складаються специфікації, опрацьовуються варіанти придбання, виконується власне закупівля.

Тут необхідно остаточно сформулювати вимоги до захисних засобів нового сервісу, до компанії, яка може претендувати на роль постачальника, і до кваліфікації, якою повинен володіти персонал, що використовує або обслуговує продукт, що купується. Всі ці відомості оформляються у вигляді специфікації, куди входять не тільки апаратура і програми, але і документація, обслуговування, навчання персоналу. Підкреслимо також, що нерідко засоби безпеки є необов'язковими компонентами комерційних продуктів, і потрібно прослідкувати, щоб відповідні пункти не випали із специфікації.

Встановлення. Сервіс встановлюється, конфігурується, тестується і вводиться в експлуатацію.

Коли продукт куплений, його необхідно встановити. По-перше, новий продукт слід конфігурувати. Як правило, комерційні продукти постав-

ляються з відключеними засобами безпеки; їх необхідно включити і належним чином налаштувати. Для великої організації, де багато користувачів і даних, початкове налаштування може стати вельми трудомісткою і відповідальною справою.

По-друге, новий сервіс потребує процедурних регуляторів. Слід потурбуватися про чистоту і охорону приміщення, про документи, що регламентують використання сервісу, про підготовку планів на випадок екстрених ситуацій, про організацію навчання користувачів тощо.

Після здійснення перерахованих заходів необхідно провести тестування. Його повнота і комплексність можуть служити гарантією безпеки експлуатації в штатному режимі.

Експлуатація. На даному етапі сервіс не тільки працює та адмініструється, але і піддається модифікаціям.

Період експлуатації – найтриваліший та складний. З психологічної точки зору найбільшою небезпекою в цей час є незначні зміни в конфігурації сервісу, в поведінці користувачів і адміністраторів. Якщо безпеку не підтримувати, вона слабшає. Користувачі не так відповідально виконують посадові інструкції, адміністратори менш ретельно аналізують реєстраційну інформацію. То один, то інший користувач одержує додаткові привілеї. Здається, що по суті нічого не змінилося, але, насправді, від минулої безпеки не залишилося й сліду. Для боротьби з ефектом повільних змін доводиться вдаватися до періодичних перевірок безпеки сервісу. Зрозуміло, що після значних модифікацій подібні перевірки є обов'язковими.

Виведення з експлуатації. Відбувається перехід на новий сервіс.

При виведенні з експлуатації зачіпаються апаратно-програмні компоненти сервісу та оброблювані ними дані. Апаратура продається, утилізується або викидається. Тільки в окремих випадках необхідно піклуватися про фізичне руйнування апаратних компонентів, що зберігають конфіденційну інформацію. При виведенні даних з експлуатації їх звичайно переносять на іншу систему, архівують, викидають або знищують. Якщо архівація проводиться з наміром згодом прочитати дані у іншому місці, слід поклопотатися про апаратно-програмну сумісність засобів читання і запису. Інформаційні технології розвиваються дуже швидко, і через декілька років пристроїв, здатних прочитати старий носій, можна просто не знайти.

IT-спеціаліст з Оксфорда Ендрю Чепмен (Andrew Chapman) купив на аукціоні eBay старенький комп'ютер. Проте він і припустити не міг, що всього за 35 фунтів стерлінгів можна придбати актив вартістю в мільйони доларів. Вивчивши вміст комп'ютеру, він побачив базу даних з як мінімум мільйоном записів про банківські карти American Express, NatWest і Royal Bank of Scotland і повідомив про свою знахідку в поліцію. Як з'ясувалося, проданий комп'ютер належав компанії Mail Source, яка пропонує фінансовим структурам послуги з обробки інформації.

cnews.ru

Якщо дані архівуються в зашифрованому вигляді, необхідно зберегти ключ і засоби розшифрування. При архівації і зберіганні архівної інформації не можна забувати про підтримку конфіденційності даних.

3.4 ІНФОРМАЦІЙНО-АНАЛІТИЧНА ДІЯЛЬНІСТЬ ПІДПРИЄМСТВА

3.4.1 Функції та задачі інформаційно-аналітичного підрозділу служби безпеки підприємства

Сучасний досвід показує, що жодне з підприємств не може ефективно проводити захист власних інформаційних ресурсів і працювати в умовах постійної і жорсткої конкуренції, якщо воно не має якісної і достовірної інформації про діяльність потенційних конкурентів і стан відповідного сегмента ринку. Отримання такої інформації забезпечується комплексом людських, матеріальних і інформаційних ресурсів, технічних засобів і технологій, спеціальних методів і організаційно-правових заходів. Ефективне практичне використання такого комплексу дозволяє виконувати одну з функцій служби безпеки – *корпоративну* або *конкурентну* розвідку.

Відомо, що прогноз, який заснований на достовірній і, що важливо, своєчасній інформації, дозволяє приймати ефективні рішення, які в більшості випадків є безпомилковими і дозволяють мінімізувати ризики. Основною функцією інформаційно-аналітичного підрозділу є підготовка перевірених даних, які отримані у результаті відповідної роботи і призначені для робіт, пов'язаних з плануванням, контролем і координацією інформаційної роботи, а також з редагуванням інформаційних ресурсів. Головним засобом, що

використовується для формування стратегії поведінки і реалізації політики безпеки, є *інформація*, яка може бути подана у будь-якій формі. Наявність фактів, навіть у достатньо великій кількості, не є великою цінністю, якщо ці факти не систематизовані певним чином і, найголовніше, не подані у потрібному вигляді. Тому важливими є так звані аналітичні методи обробки інформації, які успішно використовуються всіма сучасними підприємствами, установами та фірмами, що дбають про свою безпеку.

Інформаційно-аналітична діяльність підприємства – це системне отримання, накопичення інформації з елементами аналізу і прогнозування питань, які стосуються безпеки діяльності фірми.

Фірма здійснює аналітичну діяльність не тільки з метою захисту власної інформації, але й з метою отримання інформації щодо конкурентів. Аналітична робота є ядром такого поняття, як "*розвідка у бізнесі*" і дозволяє отримати 80-90% необхідної інформації, використовуючи при цьому тільки відкриті джерела інформації.

Так починає і проводить робочий день керівник служби безпеки одного з підприємств.

7 година 30 хвилин ранку. Жан Мартен прокидається під звук радіоприймача, який передає короткі новини: "Заворушення на Кавказі, 30 загиблих, біля берегів Каліфорнії зазнало катастрофи нафтоналивне судно – існує небезпека забруднення берегу" тощо .

8 година 00 хвилин. Сімейний сніданок. Жан Мартен розкриває місцеву газету і продивляється заголовки. Поки що немає нічого дійсно нового порівняно з вечірнім випуском новин.

8 година 30 хвилин. Жан Мартен відправляється на власному автомобілі до штаб-квартири фірми "Trident", де він працює на посаді начальника одного з департаментів. Фірма "Trident" займається виробництвом різноманітного спортивного одягу. По дорозі він прослуховує неперервні новини, різноманітні інтерв'ю і коментарі. В один момент він звернув увагу на таку фразу: " Снігова буря над ….". На жаль, кінець фрази він не почув, але різка зацікавленість цією фразою обумовлена тим, що збут гірського спортивного одягу залежить від наявності снігу. У фойє він зустрічає свого колегу Брюне і запитує чи не чув він що-небудь про снігову бурю. Той відповідає негативно. Робочий день продовжується у власному кабінеті, де він швидко проглядає періодичні видання. Його увагу привернуло лише одне повідомлення: "Як передає наш спеціальний кореспондент із Брюсселя, в результаті витоку інформації стало відомо, що великий хімічний концерн "Dubois" готується у найближчий тиждень викинути на ринок новий революційний текстильний матеріал". Невизначеність із прогнозом погоди повністю зникає після невимушеної бесіди з секретаркою, після якої він точно взнає, де випаде сніг.

Робочий день тільки почався, а у фахівця є величезна кількість інформації, яку необхідно сприйняти, обробити і відповідним чином подати. З цієї величезної кількості інформації необхідно виловити так звані "перлини", які у значній мірі і дозволяють формувати успіх фірми.

Специфічна діяльність створила певні передумови щодо формування структури і складу інформаційно-аналітичного підрозділу. В більшості випадків інформаційно-аналітичний підрозділ є ядром служби безпеки, оскільки саме служба безпеки є основним споживачем аналітично обробленої інформації і працює на випередження і прогнозування ймовірних подій.

Діяльність інформаційно-аналітичного підрозділу спрямована на виконання таких функцій:

- забезпечення захисту власних інформаційних ресурсів;
- забезпечення своєчасного отримання надійної інформації з певних питанньь;
- моделювання сценаріїв поведінки конкурентів, які можуть стосуватися інтересів фірми;
- здійснення постійного моніторингу конкурентного середовища;
- забезпечення ефективності та уникнення дублювання при збиранні, аналізі і розповсюдженні інформації.

Повний цикл інформаційно-аналітичної роботи наведено на рис. 3.1.

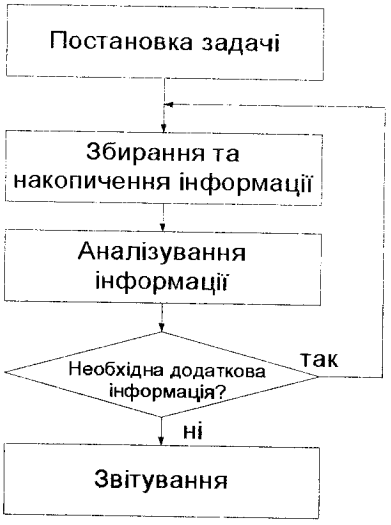


Рисунок 3.1 – Цикл інформаційно-аналітичної роботи

Цикл інформаційно-аналітичної роботи починається з постановки задачі на отримання інформації з певних питань, що стосуються дій конкурентів. Наступні дії передбачають збирання інформації, її аналіз, складання звіту у разі її достатності або планування певних дій для отримання додаткової інформації у разі її недостатності. Основними задачами інформаційно-аналітичного підрозділу є:

- виявлення фактичних можливостей розголошення, втрати і реалізації механізмів несанкціонованого доступу до конфіденційної інформації, зокрема, за опосередкованими ознаками, з урахуванням збору інформації конкурентами методами та шляхами як конкурентної розвідки, так і легально;
- прогнозування ймовірних дій конкурентів щодо конкретних інформаційних ресурсів підприємства;
- виявлення причин і обставин, які сприяють витоку конфіденційної інформації;
- оцінювання надійності і захищеності від внутрішніх і зовнішніх загроз.

Ці задачі спрямовані, в першу чергу, на аналіз дій конкурентів, а також на забезпечення власної інформаційної безпеки. Інформаційно-аналітичний підрозділ здійснює:

- зв'язок з громадськістю;
- довідково-інформаційну діяльність у регламентному режимі роботи, а також в інших випадках;
- розробку звітів, оперативних інформаційних довідок, тематичних підбірок тощо;
- проведення інформаційно-економічної розвідки та контррозвідки.

3.4.2 Напрямки інформаційно-аналітичної роботи

Основні напрямки інформаційної-аналітичної роботи визначаються окремо кожною фірмою і відображають сфери її інтересів, але існують основні напрямки цієї роботи, які є загальними для відповідного підрозділу. Напрямки інформаційно-аналітичної роботи в більшості випадків регламентуються

політикою інформаційної безпеки, яка розробляється конкретно під кожний об'єкт діяльності, і можуть бути постійними, періодичними і разовими.

Постійні напрямки аналітичної діяльності є найбільш важливими.

Періодичні і *разові* напрямки є залежними від постійних напрямків.

Проміжок часу, через який здійснюються роботи за періодичними напрямками, залежить від результатів роботи за постійним напрямками, а здійснення робіт за разовим напрямками залежить не тільки від результатів аналітичної роботи, але й, в більшості випадків, є наслідком результатів таких досліджень.

Напрямки аналітичної роботи для кожної фірми можуть бути різними, але в деяких аспектах діяльності можуть збігатися, проте логіка взаємодії і система зв'язків між різними напрямками досліджень повинна зберігатись. Як вже було наголошено, для конкретної фірми найважливішими є напрямки, за якими дослідження здійснюються постійно.

Практика діяльності багатьох фірм показує, що найскладнішою задачею є виявлення каналів несанкціонованого доступу до інформації, пов'язаних з так званими інсайдерами (внутрішніми співробітниками фірми). Важко виявити співробітництво ймовірних порушників з будь-яким працівником фірми, тому в основі знаходження таких каналів є постійна превентивна аналітична робота. Виявлення діючого або ймовірного несанкціонованого каналу доступу до конфіденційної інформації, а також попередження його появи можливе тільки за умови постійного контролю та аналізу загального рівня безпеки об'єкта захисту, а також захищеності інформаційних ресурсів як безпосередньо у джерелі, так і у каналах розповсюдження інформації.

Виявлення шляхів несанкціонованого доступу до конфіденційної інформації є однією із головних і постійних задач інформаційно-аналітичного підрозділу і у загальному випадку містить:

- аналіз джерел конфіденційної інформації;
- аналіз каналів розповсюдження інформації;
- аналітичну роботу з джерелами загроз інформації.

Виходячи з вищенаведеного можна зробити висновок, що всі напрямки інформаційно-аналітичної роботи, незалежно від їх типу мають бути

об'єднані в єдину систему, що дозволяє ефективно приймати рішення в площині прогнозування і попередження різних загроз.

3.4.3 Основні етапи інформаційно-аналітичної роботи

Інформаційно-аналітична робота передбачає виконання таких етапів:

1) *Загальне знайомство з проблемою.* Метою цього етапу є складання плану виконання робіт, визначення основних джерел інформації, що можуть бути використані, а також виконавців.

2) *Визначення термінів і основних понять, що використовуються.* Виконання цього етапу дозволить ліквідувати різні тлумачення основних термінів і понять, що використовуються у процесі роботи.

3) *Збирання фактів.* Цей етап може здійснюватися у таких режимах:

- неперервний режим або режим моніторингу, використовується тільки для збирання найважливіших факторів і характеризується найбільшими витратами;
- фокусний режим – відповідає збиранню інформації для кожної окремої задачі;
- пакетний режим відповідає паралельній роботі з декількома задачами і потребує звертання до одних джерел інформації.

4) *Вивчення та обробка фактів.* На цьому етапі виконується оцінювання, класифікація, аналіз та подання отриманої інформації.

5) *Побудова гіпотези.* Використовуючи результати виконання попереднього етапу, пропонується робоча гіпотеза. Побудова робочої гіпотези пов'язана з формулюванням конкретних питань, відповіді на які власне дозволяють перевірити і саму гіпотезу.

6) *Висновки.* На цьому етапі виконується робота, яка необхідна для доведення або спростування гіпотез, висунутих на попередньому етапі. Тут формулюються остаточні висновки, які є завершенням будь-якого аналітичного документа.

7) *Викладення.* Складання документа, який завершує роботу. Такий документ-звіт може бути 3-х видів:

- тактичний або оперативний звіт, необхідний для термінового прийняття рішення;
- стратегічний звіт, що містить більш повну інформацію з відповідного питання;
- періодичний звіт, що готується за певним графіком.

Всі звіти мають вміщувати якісну інформацію і мають бути подані у типовій формі.

Консультанти з безпеки – загадкові люди: спочатку вони випитують усе про вашу мережу та її безпеку, а потім наводять цю інформацію у своєму звіті, видаючи її за титанічний плід своїх зусиль (наслідок другого закону Макдональда).

"Закони Мерфі для інформаційної безпеки" А.В. Лукацький

3.4.4 Відомості, що становлять інтерес під час збирання та аналізу інформації

Відомості комерційного змісту:

- статутні документи фірми;
- зведені звіти про фінансову діяльність фірми (щомісячні, квартальні, річні, за кілька років);
- кредитні угоди з банками;
- угоди купівлі й продажу;
- відомості про перспективні ринки збуту, джерела засобів або сировини, товари, про вигідних партнерів;
- будь-яка інформація, надана партнерами, якщо за її розголошення передбачені штрафні санкції.
- дані про конкурентів, їх слабкі й сильні сторони;
- умови фінансової діяльності;
- технологічні секрети;
- заходи, що вживаються конкурентами щодо своїх супротивників;
- дані про потенційних партнерів, перевірка їх на несумлінність;
- інформація про місце зберігання вантажів, час й маршрути їхнього перевезення;

- виявлення уразливих ланок серед співробітників;
- виявлення осіб, перспективних для вербування шляхом підкупу, шантажу або іншого методу;
- зв'язки й можливості керівництва;
- виявлення кола постійних відвідувачів.

Відомості особистого характеру:

- джерела доходів;
- ставлення до тих або інших суспільних явищ, "сильних миру сього";
- побут особистого життя керівника та членів його родини;
- розклад і адреси зустрічей - ділових і особистих;
- дані про розміри фінансового благополуччя;
- інформація про людські слабкості;
- пагубні пристрасті;
- шкідливі звички;
- сексуальна орієнтація;
- дані про друзів, подруг, місця проведення дозвілля, способи і маршрути пересування;
- інформація про місця зберігання цінностей;
- місце проживання;
- подружня невірність;
- проблеми батьків і дітей.

3.4.5 Методи інформаційно-аналітичної роботи

Основним призначенням всіх інформаційно-аналітичних методів є збір, обробка отриманих даних, встановлення взаємозв'язку між ними, виявлення їх значущості і підготовка прийняття рішення. На практиці використовують такі методи аналізу:

- логічні методи (використовують для синтезу інформації на основі причинно-наслідкових зв'язків);
- структурні або системно-структурні методи (враховують зв'язки між елементами системи);

- статистичні методи (забезпечують ідентифікацію та інтерпретацію об'єктів, характеру їх діяльності за певними ознаками).

Наприклад, як ознаки можна розглядати періодичну появу біля фірми одних і тих самих автомобілів або людей, виявлення у приміщеннях спеціальних підслуховувальних пристроїв тощо. Наявність таких ознак говорить про безумовну зацікавленість діяльністю фірми або окремими співробітниками з боку потенційних конкурентів.

При використанні методів інформаційно-аналітичної роботи аналіз є основою роботи. Вся діяльність фірми загалом і окремого суб'єкта зокрема має свій технологічний цикл, який може характеризуватися різними виробничими ситуаціями, характеристиками продукції, наявними ресурсами тощо. У загальному випадку, кожний продукт діяльності фірми має свій, так званий конфіденційний термін, який закінчується після того, як цей продукт потрапляє у продаж. При цьому необхідно зауважити, що чим раніше будуть отримані дані про початок виробництва тієї чи іншої продукції, про ресурси, які є на початку виробництва, тим ефективнішими можуть бути випереджаючі дії виробника відносно конкурента.

У межах аналізу можна виділити деякі види і форми його реалізації.

Однією із форм є *хронологія подій*, яка дозволяє ідентифікувати події за важливою ознакою – яка подія вже відбулася, а яка ще ні. Спеціалісти вивчають хронологію подій, біографію певних осіб, часові етапи випуску продукції, її вдосконалення тощо.

Суть *якісного аналізу* полягає у поєднанні розрізнених фактів, які самі собою нічого не дають, але поєднання їх у єдину систему дозволяє отримати достатньо повний і ясний результат. Якісний аналіз дає суб'єктивний результат.

Кількісний аналіз дає більш об'єктивний результат і виконується з використанням класичних методів математичної статистики та економетрії, факторного, кореляційного, регресійного аналізу тощо.

Метод опитування є одним з найбільш розповсюджених. Мета полягає у отриманні об'єктивних і суб'єктивних фактів щодо об'єкта дослідження. Головною проблемою при опитуванні є коректне формулювання питання і власне сама техніка опитування. При опитуванні варто пам'ятати, що голо-

вною метою даної процедури є перевірка або підтвердження певної гіпотези, тому суть питань, що пропонуються, обов'язково має бути пов'язана зі змістом гіпотези.

Метод контрольної групи використовується при дослідженні конкретної проблеми. Суть методу полягає у тому, що проблема вивчається на двох групах (об'єктах дослідження), одна з яких є основною або експериментальною, а друга контрольною. Обов'язковою умовою є те, що обидві групи повинні мати однакові ознаки за винятком тієї, що досліджується. Контрольна група є відповідним фоном, на якому виявляються і аналізуються кількісні і якісні ознаки досліджуваного об'єкта. Порівняння результатів основної і контрольної груп показує, наскільки типовими є відповідні факти для певної групи.

Метод експертних оцінок широко використовується у випадку неповної або недостатньої інформації про певні факти. У цьому випадку оцінка об'єктивних і суб'єктивних фактів отримується завдяки думкам і пропозиціям фахівців, які мають відповідний професійний рівень. Необхідно відзначити, що оцінки, отримані експертним методом, мають суб'єктивний характер, а якість запропонованого рішення залежить від компетентності експерта, що, безумовно, є недоліком.

Документальний метод базується на вивченні документів на основі спеціально розроблених анкет. Анкета розробляється відповідно до мети, задач і предмета дослідження, що дозволяє формалізувати отримані дані і дає можливість у подальшому підготувати і прийняти відповідне рішення.

До окремої групи належать так звані *творчі методи.*

Метод сценаріїв, враховує невизначеність майбутнього стану в умовах постійних змін зовнішнього середовища. Метод сценаріїв передбачає розробку декількох варіантів розвитку подій, які містять песимістичний, оптимістичний і найімовірніший варіанти. Однією з головних задач методу є виявлення головних факторів, від яких буде залежати розвиток за тим чи іншим сценарієм.

Метод зворотного прогнозування є певною модифікацією попереднього методу. Цей метод на першому кроці передбачає формування варіантів розвитку, які є допустимими для даного підприємства, з урахуванням різних факторів зовнішнього середовища. На наступному кроці для кожного

допустимого варіанта розробляються можливі сценарії, які направлені від майбутнього до сьогодення. Іншими словами, спочатку визначається останній крок, який приводить до бажаного результату. У результаті залишаються лише такі сценарії, які не вміщують малоймовірних дій.

В останній час для виконання аналітичної роботи використовують елементи штучного інтелекту – *експертні системи*, які можуть видавати поради, проводити аналіз, виконувати класифікацію, ставити діагноз тощо.

3.5 УПРАВЛІННЯ РИЗИКАМИ

Управління ризиками, так само як і розробка власної політики безпеки, актуальне тільки для тих організацій, інформаційні системи яких та/або оброблювані дані можна вважати нестандартними. Звичайну організацію цілком влаштує типовий набір захисних заходів, вибраний на основі уявлення про типові ризики або взагалі без жодного аналізу ризиків. Можна провести аналогію між індивідуальним будівництвом і отриманням квартири в районі масової забудови. У першому випадку необхідно прийняти безліч рішень, оформити велику кількість паперів, а в другому випадку досить визначитися лише з декількома параметрами.

Ведення підприємницької діяльності пов'язано з певною сукупністю ризиків, зокрема в галузі інформаційної безпеки. Коли можливий збиток неприйнятно великий, необхідно вжити економічно виправданих заходів захисту. Періодичне переоцінювання ризиків необхідне для контролю ефективності діяльності у галузі інформаційної безпеки і для обліку змін обстановки.

З кількісної точки зору рівень ризику є функцією вірогідності реалізації певної загрози, що використовує деякі вразливі місця, а також величини можливого збитку.

Таким чином, суть заходів управління ризиками полягає в тому, щоб оцінити їх розмір, виробити ефективні і економічні заходи зниження ризиків, а потім переконатися, що ризики знаходяться в прийнятних межах і залиша-

ються такими. Отже, управління ризиками включає два види діяльності, які чергуються циклічно:

- переоцінювання ризиків;
- вибір ефективних і економічних захисних засобів (нейтралізація ризиків).
- Стосовно виявлених ризиків можливі такі дії:
- ліквідація ризику (наприклад, за рахунок усунення причини);
- зменшення ризику (наприклад, за рахунок використання додаткових захисних засобів);
- прийняття ризику (і вироблення плану дій у відповідних умовах);
- переадресація ризику (наприклад, шляхом укладення страхової угоди).

Процес управління ризиками складається з таких етапів.

1. Вибір об'єктів і рівня деталізації їх розгляду. Для невеликої організації допусується розглядати всю інформаційну інфраструктуру. Однак, якщо організація велика, то всеосяжне оцінювання може потребувати неприйнятних витрат часу і сил. У такому разі слід зосередитися на найважливіших сервісах, наперед погоджуючись з наближеністю підсумкової оцінки. Якщо важливих сервісів багато, вибираються ті з них, ризики для яких великі або невідомі. Для управління ризиками варто скласти карту ІС, оскільки вона наочно показує, які сервіси вибрані для аналізу, а якими довелося знехтувати. Якщо ІС змінюється, а карта підтримується в актуальному стані, то при переоцінюванні ризиків відразу стане ясно, які нові або істотно змінені сервіси потребують розгляду.

2. Вибір методології оцінювання ризиків. Метою оцінювання є отримання відповіді на два питання: чи прийнятні існуючі ризики, і якщо ні, то які захисні засоби варто використовувати. Тому оцінка повинна бути кількісною, що допускає зіставлення з наперед вибраними межами допустимості і витратами на реалізацію нових регуляторів безпеки. Управління ризиками – типове оптимізаційне завдання, і існує досить багато програмних продуктів, здатних допомогти в його вирішенні.

3. Ідентифікація активів. При ідентифікації активів, тобто тих ресурсів і цінностей, які організація намагається захистити, необхідно враховувати не тільки компоненти ІС, але й інфраструктуру, персонал, а також такі **нематеріальні цінності**, як репутація організації. Відправним моментом тут є уявлення про мі-

сію організації, тобто про основні напрями діяльності, які бажано (або необхідно) зберегти у будь-якому випадку. Одним з головних результатів процесу ідентифікації активів є отримання детальної інформаційної структури організації і способів її (структури) використання. Інформаційною основою крупної організації є мережа, тому до **апаратних активів** слід включити комп'ютери (сервери, робочі станції, ПК), периферійні пристрої, зовнішні інтерфейси, кабельне господарство, активне мережеве устаткування (мости, маршрутизатори і т.п.). До **програмних активів** відносять операційні системи (мережеві, серверні і клієнтські), прикладне програмне забезпечення, інструментальні засоби, засоби управління мережею і окремими системами. Важливо зафіксувати, в яких вузлах мережі зберігається програмне забезпечення і з яких вузлів воно використовується. Третім видом **інформаційних активів** є дані, які зберігаються, обробляються і передаються мережою. Слід класифікувати дані за типами і ступенем конфіденційності, виявити місця їх зберігання і обробки, способи доступу.

4. Аналіз загроз, їх наслідків, вразливих місць захисту. Ризик з'являється там, де є загрози. Короткий перелік найпоширеніших загроз був розглянутий раніше. На жаль, на практиці загроз значно більше, причому далеко не всі з них носять комп'ютерний характер. Так, цілком реальною загрозою є наявність мишей і тарганів у приміщеннях організації. Перші можуть пошкодити кабелі, другі – викликати коротке замикання. Як правило, наявність тієї або іншої загрози є наслідком пропусків у захисті інформаційної системи, які, у свою чергу, пояснюються відсутністю деяких сервісів безпеки або недоліками захисних механізмів. Види загроз слід вибирати, виходячи з міркувань здорового глузду (виключити, наприклад, цунамі, проте не забувати про можливості захоплення організації терористами), але в межах вибраних видів провести максимально докладний аналіз. Доцільно виявляти не тільки самі загрози, але й джерела їх виникнення – це допоможе у виборі додаткових засобів захисту. Наприклад, нелегальний вхід в систему може стати наслідком відтворення початкового діалогу, підбору пароля або підключення до мережі неавторизованого устаткування. Після ідентифікації загрози необхідно оцінити вірогідність її здійснення. Допустимо використовувати при цьому трибальну шкалу (низька (1), середня (2) і висока (3) вірогідності). Окрім вірогідності здійснення, важливо визначити розмір потенційного збитку. Наприклад, пожежі бувають нечасто, але втрати від кожної з них, як правило, великі. Величину втрат також можна оцінити за трибальною шкалою. Оцінюючи розмір втрат, необхідно мати на ува-

зі не тільки безпосередні витрати на заміну устаткування або відновлення інформації, але й втрати від підриву репутації, ослаблення позицій на ринку і т.п.

5. Оцінювання ризиків. Після того, як накопичені початкові дані і оцінений ступінь невизначеності, можна переходити до обробки інформації, тобто власне до оцінювання ризиків. Цілком допустимо застосувати такий простий метод, як множення вірогідності здійснення загрози на передбачувані втрати. Якщо для вірогідності та втрат використовувати трибальну шкалу, то можливих добутків буде шість: 1, 2, 3, 4, 6 і 9. Перші два результати можна віднести до низького ризику, третій і четвертий – до середнього, два останніх – до високого, після чого з'являється можливість знову привести їх до трибальної шкали. За цією шкалою і слід оцінювати прийнятність ризиків. Правда, граничні випадки, коли обчислена величина збіглася з прийнятною, доцільно розглядати ретельніше через наближений характер результату.

6. Вибір захисних заходів. Якщо які-небудь ризики є неприпустимо високими, необхідно їх нейтралізувати, реалізувавши додаткові заходи захисту. Як правило, для ліквідації або нейтралізації вразливого місця, яке зробило загрозу реальною, існує декілька механізмів безпеки, різних за ефективністю та вартістю. Наприклад, якщо велика вірогідність нелегального входу в систему, можна вимагати, щоб користувачі вибирали паролі за допомогою програми генерування паролів або щоб автентифікація виконувалася на основі інтелектуальних карт. Якщо є вірогідність навмисного пошкодження сервера баз даних, що може мати серйозні наслідки, можна врізати замки в двері серверної кімнати або поставити біля кожного сервера охорону.

Оцінюючи вартість заходів захисту, треба враховувати не тільки прямі витрати на закупівлю устаткування та/або програм, але і витрати на впровадження новинки і, зокрема, навчання і перепідготовку персоналу. Цю вартість також можна оцінити за трибальною шкалою і потім зіставити її з різницею між обчисленим і допустимим ризиками. Вибираючи відповідний спосіб захисту, доцільно враховувати можливість забезпечення одним механізмом безпеки відразу декількох прикладних сервісів. Важливою обставиною є сумісність нового засобу з організаційною і апаратно-програмною структурою, що склалася в організації.

Можна уявити собі ситуацію, коли для нейтралізації ризику не існує ефективних і прийнятних за ціною заходів. У такому разі доводиться піднімати планку прийнятного ризику і переносити центр тяжіння на пом'якшен-

ня наслідків і вироблення планів відновлення після аварій, стихійних лих та інших подій.

7. Реалізація і перевірка вибраних заходів. Як і будь-яку іншу діяльність, реалізацію і перевірку нових регуляторів безпеки слід заздалегідь планувати. У плані необхідно врахувати наявність фінансових коштів і терміни навчання персоналу. Якщо йдеться про програмно-технічний механізм захисту, потрібно скласти план тестування (автономного і комплексного).

8. Оцінювання залишкового ризику. Коли накреслені заходи прийняті, необхідно перевірити їх дієвість, тобто переконатися, що залишкові ризики стали прийнятними. Якщо це так, то можна призначити дату найближчого переоцінювання. Інакше доведеться проаналізувати допущені помилки і провести повторний сеанс управління ризиками.

Етапи 6 і 7 спрямовані на вибір захисних засобів (на нейтралізацію ризиків), інші – на оцінювання ризиків.

Перелік етапів показує, що управління ризиками – процес циклічний. Ризики потрібно контролювати постійно, періодично проводячи їх переоцінювання.

Управління ризиками, як і будь-яку іншу діяльність у галузі інформаційної безпеки, необхідно інтегрувати в життєвий цикл інформаційної системи. Тоді ефект виявляється найбільшим, а витрати – мінімальними. Розглянемо яким чином реалізується управління ризиками на кожному з етапів життєвого циклу.

На **етапі ініціації** відомі ризики слід врахувати для формування вимог до системи взагалі і засобів безпеки зокрема.

На **етапі закупівлі** (розробки) знання ризиків допоможе вибрати відповідні архітектурні рішення, які грають ключову роль у забезпеченні безпеки.

На **етапі встановлення** виявлені ризики слід враховувати при конфігурації, тестуванні і перевірці раніше сформульованих вимог, а повний цикл управління ризиками повинен передувати впровадженню системи в експлуатацію.

На **етапі експлуатації** управління ризиками повинно супроводжувати всі істотні зміни в системі.

При **виведенні системи з експлуатації** управління ризиками допомагає переконатися в тому, що міграція даних відбувається безпечним чином.

Організаційні заходи є вирішальною ланкою формування і реалізації комплексного захисту інформації і створення системи безпеки підприємства.

КОНТРОЛЬНІ ПИТАННЯ

1. Дайте означення поняття "організаційний захист".
2. Назвіть класи заходів організаційного захисту.
3. Наведіть основні принципи управління персоналом.
4. Назвіть основні напрями фізичного захисту інформації.
5. Дайте означення поняття "політика безпеки".
6. Дайте характеристику рівням розробки політики ІБ.
7. Які пункти виносяться на верхній рівень політики безпеки?
8. Що виноситься на середній рівень політики безпеки?
9. Які пункти виносяться на нижній рівень політики безпеки?
10. Чим відрізняється політика безпеки від програми безпеки?
11. Опишіть особливості складання програми реалізації політики безпеки.
12. Яким чином здійснюється синхронізація програми безпеки з життєвим циклом ІС.
13. Що таке управління ризиками?
14. Охарактеризуйте етапи управління ризиками.
15. Охарактеризуйте можливості заходів фізичного управління доступом.
16. Яким чином здійснюється реагування на порушення ІБ?
17. Обґрунтуйте необхідність планування відновних робіт.
18. Охарактеризуйте задачі та напрямки роботи служби безпеки підприємства.
19. Назвіть основні функції служби персоналу на підприємстві.
20. Перерахуйте функції та задачі інформаційно-аналітичного підрозділу служби безпеки підприємства.
21. Опишіть основні напрямки та етапи інформаційно-аналітичної роботи.
22. Охарактеризуйте методи інформаційно-аналітичної роботи

Якщо яка-небудь неприємність
може відбутися, вона трапляється
Закон Мерфи

4.1 ПОНЯТТЯ ІНЖЕНЕРНО-ТЕХНІЧНОГО ЗАХИСТУ

Інженерно-технічний захист – це сукупність спеціальних органів, технічних засобів і заходів щодо їхнього використання в інтересах захисту конфіденційної інформації.

Інженерно-технічні засоби класифікують за об'єктами впливу, функціональним призначенням, способами реалізації, масштабами охоплення, класами засобів зловмисників, яким протидіє служба безпеки.

За *об'єктами впливу* засоби інженерно-технічного захисту поділяються на засоби для захисту:

- людей;
- матеріальних засобів:
- фінансів;
- інформації;
- репутації тощо.

За *функціональним призначенням* розрізняють такі засоби інженерно-технічного захисту:

- фізичні;
- апаратні;
- програмні;
- криптографічні;
- стеганографічні.

До **фізичних засобів** належать різні засоби і споруди, що перешкоджають фізичному проникненню (чи доступу) зловмисників на об'єкти захисту і до матеріальних носіїв конфіденційної інформації, а також забезпечують захист персоналу, матеріальних засобів і фінансів та інформації від протиправних впливів.

До групи **апаратних засобів** входять прилади, пристрої, пристосування й інші технічні рішення, використовувані в інтересах захисту інфор-

мації. Основна задача апаратних засобів – забезпечення стійкого захисту інформації від розголошення, витоку і несанкціонованого доступу через технічні засоби забезпечення виробничої діяльності.

Групу **програмних засобів складають** спеціальні програми, програмні комплекси і системи захисту інформації в ІС різного призначення і засобах збирання, накопичення, зберігання, оброблення і передавання даних.

Криптографічні засоби – це спеціальні математичні й алгоритмічні засоби захисту інформації, що передається в системах і мережах зв'язку, зберігається й обробляється в комп'ютерах з використанням різноманітних методів шифрування;

Групу **стеганографічних засобів** утворюють спеціальні математичні й алгоритмічні засоби захисту інформації, спрямовані на приховання самої присутності конфіденційної інформації.

Очевидно, що такий розподіл засобів захисту інформації досить умовний, тому що на практиці дуже часто вони і взаємодіють і реалізуються в комплексі у вигляді програмно-апаратних модулів із широким використанням алгоритмів закриття інформації.

4.2 ФІЗИЧНІ ЗАСОБИ ЗАХИСТУ

4.2.1 Види фізичних засобів

Фізичні засоби захисту – це різноманітні пристрої, пристосування, конструкції, апарати, вироби, призначені для створення перешкод на шляху руху зловмисників.

До фізичних засобів належать механічні, електромеханічні, електронні, електронно-оптичні, радіо- і радіотехнічні й інші пристрої, що перешкоджають несанкціонованому доступу (входу, виходу), виносу (проносу) засобів і матеріалів і іншим можливим видам злочинних дій.

Ці засоби застосовуються для розв'язання таких задач:

- охорона території підприємства і спостереження за нею;
- охорона будинків, внутрішніх приміщень і контроль за ними;
- охорона устаткування, продукції, фінансів і інформації;

- забезпечення контрольованого доступу до будинків і приміщень.

До засобів фізичного захисту належать:

- **природні і штучні бар'єри,** які перешкоджають незаконному проникненню на територію об'єкта. Однак основне захисне навантаження лягає все-таки на штучні бар'єри – такі, як паркан та інші види огороджень. Практика показує, що огородження складної конфігурації здатні затримати зловмисника на досить великий час. На сьогодні нараховується значний арсенал таких засобів: від простих сітчастих до складних комбінованих огороджень, що в певній мірі відлякують порушника;
- **особливі конструкції** периметрів, проходів, віконних і дверних плетінь, приміщень, сейфів, сховищ тощо є обов'язковими з погляду безпеки для будь-яких організацій і підприємств. Ці конструкції повинні протистояти будь-яким способам фізичного впливу з боку кримінальних елементів: механічним деформаціям, руйнуванню свердлінням, термічному і механічному різанню, вибуху тощо; несанкціонованому доступу шляхом підробки ключів, угадування коду й ін. Одним з головних технічних засобів захисту проходів, приміщень, сейфів і сховищ є замки. Вони бувають простими (із ключами), кодовими (у тому числі і з часовою затримкою на відкривання) і з програмними пристроями, що відкривають двері і сейфи тільки у певні години;
- **зони безпеки,** які повинні розташовуватися на об'єкті послідовно, від паркана навколо території об'єкта до сховищ цінностей, створюючи ланцюг перешкод (рубежів), які буде потрібно подолати зловмиснику. Чим складніша і надійніша перешкода на його шляху, тим більше часу буде потрібно на подолання кожної зони і тем більше ймовірність того, що розташовані в кожній зоні засоби виявлення (охоронні пости, охоронна сигналізація й охоронне телебачення) виявлять наявність порушника і подадуть сигнал тривоги.

Усі фізичні засоби захисту об'єктів поділяються на три категорії:

- засоби попередження (грати, посилені двері);
- засоби виявлення (сигналізація, охоронне телебачення);

- системи ліквідації загроз (засоби пожежогасіння).

У загальному плані за фізичною природою і функціональним призначенням всі засоби попередження поділяються на такі групи:

- охоронні й охоронно-пожежні системи;
- охоронне телебачення;
- охоронне освітлення;
- захист елементів будинків і приміщень.

4.2.2 Охоронні системи

Охоронні системи призначені для:

- виявлення спроб проникнення на об'єкт захисту, в охоронювані зони і приміщення, спроб проносу (виносу) зброї, засобів промислового шпигунства, крадіжок матеріальних і фінансових цінностей тощо;
- оповіщення співробітників чи персоналу охорони об'єкта про появу загроз і про необхідність посилення контролю доступу на об'єкт, територію, у будинки і приміщення.

За тактичним призначенням **охоронні системи** поділяються на системи охорони:

- периметрів об'єктів;
- приміщень і проходів у службових і складських будинках;
- сейфів, устаткування, основних і допоміжних технічних засобів;
- автотранспорту;
- персоналу, у тому числі й особового складу охорони тощо.

Одним з найважливіших елементів охоронних систем є сенсори, що виявляють появу загрози. Розроблена і широко використовується значна кількість найрізноманітніших сенсорів як за принципами виявлення різних фізичних полів, так і за тактичним використанням. Ефективність роботи системи охорони й охоронної сигналізація в основному визначається параметрами і принципом роботи сенсорів.

Кожен тип сенсора реалізує певний вид захисту:

- точковий захист;
- захист лінії;
- захист площини;

- захист об'єму.

Механічні сенсори орієнтовані на захист лінії, килимки тиску – на точкове виявлення, а інфрачервоні сенсори знаходять широке застосування для захисту площини і об'єму.

Важливим об'єктом охоронної системи є засоби тривожного оповіщення: дзвоники, лампочки, сирени, що подають постійні чи перервні сигнали про появу загрози.

Основу планування й устаткування зон безпеки об'єкта складає принцип рівноміцності границь зон безпеки. Сумарна міцність зон безпеки оцінюється за найменшою з них.

4.2.3 Охоронне телебачення

Привабливою особливістю охоронного телебачення є можливість не тільки виявляти порушення режиму охорони об'єкта, але і контролювати обстановку навколо нього в динаміці її розвитку, визначати небезпеку дій, вести приховане спостереження і робити відеозапис як для наступного аналізу правопорушення, так і для притягнення порушника до відповідальності.

Джерелами зображення (сенсорами) у системах охоронного телебачення є відеокамери. Через об'єктив зображення зловмисника потрапляє на світлочутливий елемент камери, у якому воно перетворюється в електричний сигнал, що надходить потім по спеціальному коаксіальному кабелю на монітор і, при необхідності, зберігається в запам'ятовувальному пристрої.

З огляду на порівняно високу вартість відеокамер і їхньої експлуатації, у тому числі необхідність постійного спостереження за зображенням на екранах моніторів, камери встановлюють у місцях з максимальною потенційною загрозою.

Такими місцями є:

- входи до офісу, організації, на контрольно-пропускний пункт;
- територія організації зі слабким захистом (двір зі складованою продукцією, стоянка службового автотранспорту біля організації й ін.);
- операційні зали й бокси для стоянки інкасаторських машин;
- підступи до виділених приміщень (у коридорах);

- місця зберігання коштовних об'єктів захисту (у приміщеннях, сховищах, біля сейфів).

Відеокамера є найважливішим елементом системи охоронного телебачення, оскільки від її характеристик залежить ефективність і результативність усієї системи контролю і спостереження. В даний час розроблені та випускаються найрізноманітніші моделі, що різняться габаритами, можливостями і конструктивним виконанням.

Відеокамера вибирається з урахуванням:

- категорії значимості об'єкта;
- геометричних розмірів зони охорони;
- інформативних демаскувальних ознак об'єктів спостереження;
- освітленості зони охорони в різний час доби;
- розташування можливих місць проникнення зловмисника в охоронювану зону;
- умов експлуатації;
- виду спостереження – прихованого або відкритого.

Другим за значимістю елементом системи охоронного телебачення є монітор. Він повинен бути погоджений за параметрами з відеокамерою. Часто використовується один монітор з декількома камерами, що приєднуються до нього по черзі засобами автоматичного переключення за певним регламентом.

У деяких системах телевізійного спостереження передбачається можливість автоматичного підключення камери, в зоні огляду якої відбулося порушення. Використовується і більш складне устаткування, що містить засоби автоматизації, пристрій одночасного виведення декількох зображень, детектори руху для подачі сигналу тривоги при виявленні яких-небудь змін у зображенні.

4.2.4 Охоронне освітлення та засоби охоронної сигналізації

Розрізняють два види охоронного освітлення – чергове і тривожне.

Чергове освітлення призначається для постійного використання в не-

робочий, вечірній і нічний час як на території об'єкта, так і усередині будинку.

Тривожне освітлення включається при надходженні сигналу тривоги від засобу охоронної сигналізації. Крім того, за сигналом тривоги на додаток до освітлення можуть включатися і звукові прилади (дзвоники, сирени й ін.).

Сигналізація і чергове освітлення повинні мати резервне електроживлення на випадок аварії чи вимикання електромережі.

В останні роки велика увага приділяється створенню систем фізичного захисту, з'єднаних із системами сигналізації.

Відома електронна система сигналізації для використання з дротовим загородженням. Система складається з електронних сенсорів і мікропроцесора, що керує блоком обробки даних. Загородження довжиною до 100 м може встановлюватися на відкритій місцевості чи розміщатися на стінах, горищах і наявних огорожах. Стійкі до впливу навколишнього середовища сенсори монтуються на стійках, кронштейнах. Дротове загородження складається з 32 горизонтально натягнутих сталевих ниток, у середній частині кожної з який кріпиться електромеханічний сенсор, що перетворює зміну натягу ниток в електричний сигнал. Перевищення граничної величини напруги, що запрограмована для кожного сенсора окремо, викликає сигнал тривоги. Мікропроцесор автоматично через певні інтервали часу перевіряє роботу компонентів апаратури та програмних засобів і, у випадку встановлення відхилень, подає відповідний сигнал.

Подібні і ряд інших аналогічних систем фізичного захисту можуть використовуватися для захисту об'єктів по периметру з метою виявлення вторгнення на територію об'єкта.

Використовуються системи із сітки двох волоконно-оптичних кабелів, по яких передаються кодовані сигнали інфрачервоного діапазону. Якщо в сітці немає ушкоджень, то сигнали надходять на прийомний пристрій без спотворень. Спроби ушкодження сітки призведуть до обривів або деформації кабелів, що викличе сигнал тривоги. Оптичні системи відрізняються низьким рівнем помилкових тривог, викликаних впливом на неї дрібних тварин, птахів, зміною погодних умов і високою ймовірністю виявлення спроб вторгнення.

4.2.5 Захист елементів будинків і приміщень

Гарний фізичний захист віконних прорізів приміщень забезпечують традиційні металеві ґрати. Двері і вікна охоронюваного приміщення обладнуються сенсорами, що спрацьовують при руйнуванні скла, дверей, але не реагують на їхні коливання, викликані іншими причинами. Спрацьовування сенсорів викликає сигнал тривоги.

Рекомендуються такі типові заходи щодо захисту інформації від спостереження:

а) через вікна:

- зменшення освітленості об'єктів у приміщенні;
- зменшення прозорості вікон шляхом застосування:
  - фіранок;
  - штор;
  - жалюзі;
  - тонованих стекол і плівок на вікнах.

Слід зазначити, що застосування тонованого скла або плівок створює додаткові демаскувальні ознаки для визначення ззовні місця знаходження виділеного приміщення. Тому для приховування цієї ознаки доцільно застосувати таке скло або плівки на інших вікнах, хоча б відповідного поверху.

б) через відкриті двері:

- застосування засобу, що примусово зачиняє двері;
- встановлення на двері замка (краще кодового) із засувкою.

Захист інформації від прослуховування забезпечується такими типовими заходами:

а) для дверей:

- усунення щілин між дверним полотном і дверною рамою;
- підвищення поверхневої маси дверного полотна;
- покриття дверного полотна звуковбирними матеріалами;
- встановлення других дверей з тамбуром;

- встановлення на двері засобу, що примусово зачиняє;
- встановлення на двері замка із засувкою;

б) для вікон:

- закриття вікон;
- встановлення звукоізолювальних прокладок між віконними рамами;
- закриття вікна щільними шторами;
- віброакустичне зашумлення стекол вікон;
- встановлення трьох стекол;

в) для стін:

- збільшення товщини й поверхневої маси стіни шляхом додаткової цегельної кладки та встановлення екранів;
- покриття стіни звуковбирними матеріалами;
- віброакустичне зашумлення.

г) для вентиляції:

- встановлення перед вентиляційними отворами екранів;
- встановлення у вентиляційні отвори глушителів;

д) через водоопалювальні системи:

- встановлення перед батареями опалення і трубами акустичних екранів.

Серед засобів фізичного захисту особливо слід відзначити засоби захисту комп'ютерів від розкрадання і проникнення до їхніх внутрішніх компонентів. Для цього використовують металеві конструкції з клейкою підставкою, що забезпечує зчеплення з поверхнею столу із силою, яка унеможливлює вилучення чи переміщення комп'ютерів без порушення цілісності поверхні столу. Переміщення комп'ютера можливе тільки з використанням спеціальних ключів і інструментів.

Замикальні пристрої і спеціальні шафи займають особливе місце в системах обмеження доступу, оскільки мають ознаки як систем фізичного захисту, так і пристроїв контролю доступу. Вони відрізняються великою розмаїтістю і призначені для захисту документів, матеріалів, магнітних та фото носіїв, а також технічних засобів: комп'ютерів, калькуляторів, принтерів, ксероксів тощо.

Випускаються спеціальні металеві шафи для зберігання комп'ютерів та

іншої техніки. Такі шафи забезпечуються надійною подвійною системою запирання: замком ключового типу і три-п'ятизначним комбінованим замком. Такі шафи мають міцність і надійність, достатню для захисту від промислового шпигунства.

Виготовляються замки, в яких програмується час відкриття за допомогою механічного чи електронного годинника.

Регулювання доступу в приміщення чи будинки здійснюється за допомогою впізнання службою охорони чи технічними засобами.

Контрольований доступ забезпечує обмеження кола осіб, що допускаються у певні зони будинків і приміщень, а також контроль за пересуванням цих осіб усередині них.

Підставою для допуску служить результат впізнання чи порівняння з дозвільними параметрами системи. Існує дуже широкий спектр методів впізнання уповноважених осіб на право їхнього доступу в приміщення, будинки, зони.

На основі впізнання приймається рішення про допуск осіб, що мають на це право, чи про заборону допуску – для тих, хто не має його. Найбільше поширення одержали атрибутні і персональні способи ідентифікації та автентифікації.

В атрибутних способах для підтвердження повноважень вимагаються документи (паспорт, посвідчення й ін.), карти (фотокартки, карти з магнітними, електричними, механічними ідентифікаторами й ін.) та інші засоби (ключі, сигнальні елементи й ін.).

Персональні способи – це способи визначення особи за її персональними характеристиками.

Спосіб упізнання людиною (вахтер, вартовий) не завжди надійний через так званий "людський фактор", який полягає в тому, що людина піддається впливу багатьох зовнішніх умов (втома, погане самопочуття, емоційний стрес, підкуп і ін.). У противагу цьому знаходять широке застосування технічні засоби впізнання за допомогою біометричних даних.

Біометрія є сукупністю автоматизованих методів ідентифікації та/або автентифікації людей на основі їх фізіологічних і поведінкових характеристик. До фізіологічних характеристик належать особливості відбитків паль-

ців, сітківки і рогівки очей, геометрія руки і особи тощо. До поведінкових характеристик відносять динаміку підпису (ручний), стиль роботи з клавіатурою. На стику фізіології і поведінки знаходиться аналіз особливостей голосу і розпізнавання мови.

Біометрією у всьому світі займаються дуже давно, проте довгий час все, що було пов'язане з нею, відрізнялося складністю і дорожнечею. Останнім часом попит на біометричні продукти, в першу чергу у зв'язку з розвитком електронної комерції, постійно і вельми інтенсивно зростає. Це зрозуміло, оскільки з погляду користувача набагато зручніше пред'явити себе самого, ніж щось запам'ятовувати. Попит породжує пропозицію, і на ринку з'явилися відносно недорогі апаратно-програмні засоби, орієнтовані, в основному, на розпізнавання відбитків пальців.

У загальному вигляді робота з біометричними даними організована таким чином. Спочатку створюється і підтримується база даних характеристик потенційних користувачів. Для цього біометричні характеристики користувача знімаються, обробляються, і результат обробки (*біометричний шаблон*) заноситься в базу даних.

Надалі для ідентифікації (і одночасно автентифікації) користувача процес зняття і обробки повторюється, після чого проводиться пошук в базі даних шаблонів. У разі успішного пошуку особа користувача та її достовірність вважаються встановленими. Для автентифікації досить провести порівняння з одним біометричним шаблоном, вибраним на основі попередньо введених даних.

Активність у галузі біометрії дуже велика. Виконуються роботи зі стандартизації різних аспектів технології (формату обміну даними, прикладного програмного інтерфейсу і т.п.), публікується маса рекламних статей, в яких біометрія подається як засіб забезпечення надбезпеки, що став доступним широким масам.

Проте до біометрії слід ставитися вельми обережно. Необхідно враховувати, що вона має ті ж загрози, що й інші методи автентифікації.

По-перше, біометричний шаблон порівнюється не з результатом первинної обробки характеристик користувача, а з тим, що дійшло місця порівняння. Проте під час передавання даних багато чого може відбутися.

По-друге, біометричні методи не більш надійні, ніж база даних шаблонів.

По-третє, слід враховувати різницю між застосуванням біометрії на контрольованій території, під пильним оком охорони, і в "польових" умовах, коли, наприклад, до пристрою сканування рогівки можуть піднести муляж.

По-четверте, біометричні дані людини змінюються, і тому база шаблонів потребує супроводу, що створює проблеми і для користувачів, і для адміністраторів.

Але головна небезпека полягає в тому, що будь-яка "пробоїна" для біометрії виявляється фатальною. Паролі, при всій їх ненадійності, в крайньому випадку можна змінити. Загублену автентифікаційну карту можна анулювати і завести нову. Палець же, око або голос змінити не можна. Якщо біометричні дані будуть скомпрометовані, доведеться, як мінімум, проводити істотну модернізацію всієї системи.

Усі пристрої ідентифікації людини можуть працювати як окремо, так і в комплексі. Комплекс може бути вузькоспеціалізованим чи багатоцільовим, при якому система виконує функції охорони, контролю, реєстрації і сигналізації.

Комплексні системи забезпечують:

- допуск на територію підприємства при наявності картки (пропуску), що містить індивідуальний машинний код;
- блокування проходу у разі спроби несанкціонованого проходження;
- можливість блокування проходу для порушників графіка роботи (запізнення, передчасний вихід тощо);
- відкриття зони проходу для вільного виходу за командою вахтера;
- перевірку кодів пропусків на затримку їхніх пред'явників на контрольно-перепускному пункту за вказівкою оператора системи;
- реєстрацію часу проходу прохідної і збереження його в базі даних комп'ютера;
- обробку отриманих даних і формування різних документів (табель робочого часу, добовий рапорт, відомість порушників трудової дисципліни й ін.), що дозволяє мати оперативну інформацію про порушників трудової дисципліни, відпрацьований час тощо;
- оперативне корегування інформації бази даних;

- поточний і ретроспективний аналіз відвідування співробітниками підрозділів, пересування співробітників через контрольно-перепускний пункт, видачу облікового складу присутніх чи відсутніх в підрозділі чи на підприємстві для довільно обраного моменту часу (за умови збереження баз даних за минулі періоди);
- одержання оперативної інформації абонентами локальної мережі у випадку мережевої реалізації системи.

Такі ознаки можуть указувати на наявність уразливих місць у фізичному захисті:

- дозволено курити, їсти й пити поруч із комп'ютерами;
- комп'ютерне устаткування залишається в незамкнених кімнатах або є незахищеним з будь-якої іншої причини;
- не встановлена пожежна сигналізація;
- диски залишаються в шухлядах столів, не робиться архівних копій дисків та інших носіїв інформації;
- відвідувачам не задають питання про причину їхнього знаходження в приміщеннях, де встановлені комп'ютери;
- реєстр комп'ютерного устаткування та програм відсутній, неповний, не оновляється або не перевіряється після його заповнення;
- роздруківки, диски, що містять критичні дані, викидаються у звичайний кошик для сміття;
- замки на входах у приміщення, де розташоване комп'ютерне устаткування, ніколи не мінялися;
- не здійснювалося атестації автоматизованої системи організації, тобто аналізу, наскільки вона вразлива щодо доступу неавторизованих осіб, пожежі або повені.

4.3 АПАРАТНІ ЗАСОБИ ЗАХИСТУ

Апаратні засоби захисту інформації – це різноманітні за принципом дії, побудовою і можливостям технічні конструкції, що забезпечують припинення розголошення, захист від витоку і протидію несанкціонованому доступу до джерел конфіденційної інформації.

Апаратні засоби захисту інформації застосовуються для розв'язання таких задач:

- проведення спеціальних досліджень технічних засобів забезпечення виробничої діяльності на наявність можливих каналів витоку інформації;
- виявлення каналів витоку інформації на різних об'єктах і в приміщеннях;
- локалізація каналів витоку інформації;
- пошук і виявлення засобів промислового шпигунства;
- протидія несанкціонованому доступу до джерел конфіденційної інформації та іншим діям.

За функціональним призначенням апаратні засоби поділяються на:

- засоби виявлення;
- засоби пошуку і детальних вимірювань;
- засоби активної і пасивної протидії.

При цьому за своїми технічними можливостями засоби захисту інформації можуть бути загального призначення, розраховані на використання непрофесіоналами з метою одержання попередніх (загальних) оцінок, і професійні комплекси, що дозволяють проводити ретельний пошук, виявлення і точні вимірювання всіх характеристик засобів промислового шпигунства.

Прикладом перших є група індикаторів електромагнітних випромінювань типу "індикатор поля", з широким спектром прийнятих сигналів і досить низкою чутливістю.

До других належить, наприклад, комплекс "Дельта", який призначено для автоматичного виявлення і визначення місцезнаходження радіопередавачів, радіомікрофонів, телефонних закладок і мережевих радіопередавачів. Це вже складний сучасний пошуково-розвідувальний професійний комплекс.

Пошукова апаратура поділяється на апаратуру *пошуку засобів знімання інформації* та *дослідження каналів її витоку.*

Апаратура першого типу спрямована на пошук і локалізацію вже впроваджених зловмисниками засобів несанкціонованого доступу. Апаратура другого типу призначається для виявлення каналів витоку інформації.

Визначальними для такого типу систем є оперативність дослідження і

надійність отриманих результатів.

Використання професійної пошукової апаратури вимагає високої кваліфікації оператора.

Як у будь-якій галузі техніки, універсальність тієї чи іншої апаратури приводить до зниження її параметрів для кожної окремої характеристики. З іншого боку, існує величезна кількість різних за фізичною природою каналів витоку інформації, а також фізичних принципів, на основі яких працюють системи несанкціонованого доступу. Ці фактори обумовлюють різноманіття пошукової апаратури, а її складність визначає високу вартість кожного приладу. В зв'язку з цим достатній комплекс пошукового устаткування можуть дозволити собі мати структури, що постійно проводять відповідні обстеження. Це або великі служби безпеки, або спеціалізовані фірми, що надають послуги стороннім організаціям.

Для самостійного пошуку використовуються в більшості випадків досить прості засоби, які дозволяють проводити профілактичні заходи в проміжку між серйозними пошуковими обстеженнями.

В особливу групу виділяються апаратні засоби захисту комп'ютерів і комунікаційних систем на їхній базі.

Апаратні засоби захисту застосовуються як в окремих комп'ютерах, так і на різних рівнях і ділянках мережі.

Для захисту центральних процесорів застосовується кодове резервування – створення додаткових бітів у форматах машинних команд (розрядів таємності) і резервних регістрів. Одночасно передбачаються два можливих режими роботи процесора, що відокремлюють допоміжні операції від операцій безпосереднього вирішення задач користувача. Для цього служить спеціальна система переривання, реалізована апаратними засобами. Для позначення ступеня конфіденційності програм і даних, категорій користувачів використовуються біти, що називаються бітами конфіденційності (це два-три додаткових розряди, за допомогою яких кодуються категорії таємності користувачів, програм і даних).

Програми і дані, що завантажуються в оперативний запам'ятовувальний пристрій, мають потребу в захисті, що гарантує їх від несанкціонованого доступу. Часто використовуються біти парності, ключі,

постійна спеціальна пам'ять. При зчитуванні з оперативної пам'яті необхідно, щоб програми не могли бути знищені несанкціонованими діями користувачів чи унаслідок виходу апаратури з ладу. Для запобігання зчитування даних, що залишилися після обробки в оперативній пам'яті, застосовується спеціальна схема стирання.

Рекомендуються такі заходи щодо захисту носіїв інформації:

- ведення контролю та перевірка реєстрів носіїв інформації;
- навчання користувачів правильним методам очищення та знищення носіїв інформації;
- нанесення міток на носії інформації для відображення рівня критичності інформації, що міститься на них;
- знищення носіїв інформації відповідно до плану організації;
- надання тільки авторизованим особам доступу до носіїв інформації для їхнього зберігання, передачі, нанесення міток і знищення;
- зберігання носіїв інформації в недоступному місці;
- доведення всіх керівних документів до співробітників.

Апаратні засоби захисту застосовуються й у терміналах користувачів. Для запобігання витоку інформації при підключенні незареєстрованого термінала необхідно перед видачею запитуваних даних здійснити ідентифікацію (автоматичне визначення коду чи номера ідентифікації) термінала, з якого надійшов запит. У багатокористувацькому режимі цього термінала недостатньо. Необхідно здійснити автентифікацію користувача, тобто встановити його дійсність і повноваження. Це необхідно і тому, що різні користувачі, зареєстровані в системі, можуть мати доступ тільки до окремих файлів і строго обмежені повноваження їхнього використання.

Для ідентифікації термінала найчастіше застосовується генератор коду, включений в апаратуру термінала, а для автентифікації користувача – такі апаратні засоби:

- ключі,
- персональні кодові карти,
- персональний ідентифікатор,
- пристрої розпізнавання голосу користувача чи форми його пальців.

Але найбільш розповсюдженими засобами автентифікації є паролі, що перевіряються не апаратними, а програмними засобами розпізнавання.

4.4 ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ

Програмні засоби захисту даних – це складові програмного забезпечення, що реалізують функції захисту даних самостійно або в комплексі з іншими засобами захисту.

Класифікацію програмних засобів захисту за функціональним призначенням наведено на рис. 4.1.

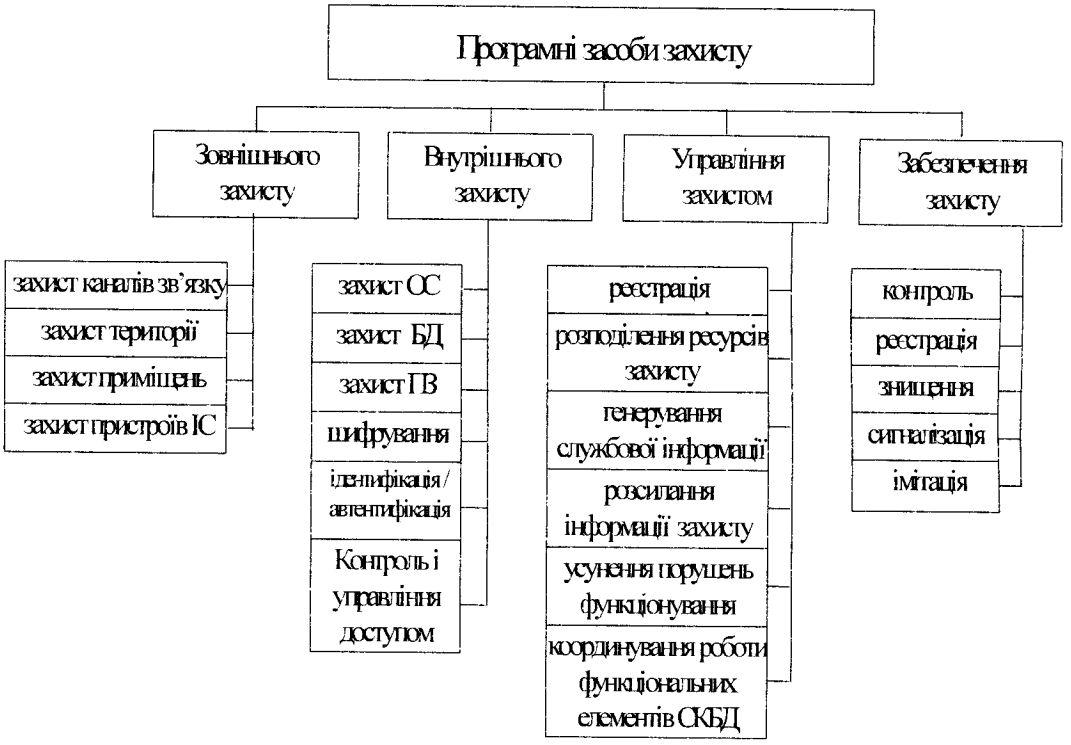


Рисунок 4.1 – Класифікація програмних засобів захисту

До **програмних засобів зовнішнього захисту** належать програмні засоби забезпечення функціонування фізичних засобів, захисту території, приміщень, окремих каналів зв'язку й пристроїв ІС. У цей час випускається безліч систем охоронної сигналізації, що містять мікропроцесори й комп'ютери. Програмні засоби використовуються також у пристроях біометричного розпізнавання особистості.

Основним методом захисту даних, що передаються по каналах зв'язку, є криптографічне закриття даних, яке реалізується програмними, апаратними і програмно-апаратними засобами.

Крім цього використовуються такі програмні засоби:

- розпізнавання користувачів;
- перевірка рівня таємності каналу;
- перевірка адрес користувачів;
- перевірка ідентифікаторів користувачів під час обміну великими обсягами даних і т.д.

Ідентифікація – це процедура однозначного розпізнавання унікального імені суб'єкта інформаційної системи.

Автентифікація – це процедура підтвердження того, що пред'явлене ім'я відповідає даному суб'єктові (підтвердження дійсності суб'єкта).

Пояснимо терміни на прикладі.
Суб'єкт приходить до дверей рідної домівки і стукає. Відбувається запит на ідентифікацію.
У відповідь він чує «Хто там?». Суб'єкт називає свій логін «Це ж я, що, не впізнаєш?». Ідентифікація пройдена.
Далі йде запит на автентифікацію «Діставай свій ключ і заходь». Суб'єкт бере свій ключ (апаратна автентифікація) і відкриває замок або називає ключове слово «Відкривай швидко, бо...» (парольна автентифікація). Автентифікація пройдена.
Авторизація означає, що суб'єкту нададуть права на отримання обіду і пульта від телевізора.

Програмні засоби внутрішнього захисту охоплюють сукупність засобів і механізмів захисту даних, що знаходяться в апаратурі ІС. Їхнім основним призначенням є регулювання і контроль використання даних та ресурсів системи відповідно до встановлених прав доступу.

- Тато, купи мені новий вінчестер, а то в мене для відео архіву місця мало!
- А що сказати треба?
- Ну ось, вже й тут паролів наставили...

Типова схема функціонування цих програмних засобів складається з таких основних етапів:

- установлення дійсності суб'єкта, що звертається до ресурсів системи;
- перевірка відповідності характеру запиту наданим повноваженням даного суб'єкта;
- ухвалення рішення відповідно до результату перевірки повноважень.

Регулювання використання технічних засобів звичайно здійснюється за такими параметрами, як час доступу і запитувана дія при доступі.

Захист програмного забезпечення здійснюється такими методами, як, наприклад, контрольне підсумовування і шифрування.

Програмні засоби керування захистом призначені для виконання таких завдань:

- керування користувачами мережі (реєстрація користувачів, генерування службової інформації для користувачів, розсилання службової інформації користувачам);
- керування базами даних (розподіл ресурсів захисту, координація роботи підсистем системи керування базами даних (СКБД);
- завдання прийняття рішень у позаштатних ситуаціях (система підтримки ухвалення рішення адміністратором СКБД, вироблення керувальних впливів для усунення порушення функціонування СКБД).

Програмні засоби забезпечення захисту функціонування СКБД виконують функції контролю, реєстрації, знищення, сигналізації та імітації.

Засоби контролю здійснюють тестування елементів СУБД, а також постійний збір інформації про функціонування елементів СКБД. Ця інформація служить вихідними даними для засобів підтримки ухвалення рішення і вироблення керувальних впливів.

Засоби реєстрації забезпечують збирання, зберігання, оброблення і видачу даних про стан СКБД.

Засоби знищення призначені для знищення залишкових даних і можуть передбачати аварійне знищення даних у випадку прямої загрози несанкціонованого доступу, яке не може бути блоковано системою.

Засоби сигналізації призначені для попередження користувачів при їхньому звертанні до захищених даних і для попередження адміністратора

СКБД при виявленні факту несанкціонованого доступу до даних, спотворення програмних засобів захисту, виході з ладу апаратних засобів захисту тощо.

Засоби імітації імітують роботу з порушниками при виявленні спроби несанкціонованого доступу до даних, що захищають. Імітація дозволяє збільшити час на визначення місця і характеру несанкціонованого доступу, що особливо важливо в територіально розподілених мережах, і "відвести" порушника вбік від даних, що захищаються.

Перевагами програмних засобів захисту інформації є:

- простота тиражування;
- гнучкість (можливість настроювання на різні умови застосування, що враховують специфіку загроз інформаційній безпеці конкретних ІС);
- простота застосування – одні програмні засоби, наприклад шифрування, працюють у "прозорому" (непомітному для користувача) режимі, а інші не вимагають від користувача ніяких нових (порівняно з іншими програмами) навичок;
- практично необмежені можливості їхнього розвитку шляхом внесення змін для врахування нових загроз безпеці інформації.

До недоліків програмних засобів захисту інформації належать:

- зниження ефективності ІС за рахунок споживання її ресурсів, необхідних для функціонування програм захисту;
- більш низька продуктивність виконання аналогічних функцій порівняно з апаратними засобами захисту;
- приєднання багатьох програмних засобів захисту, а не їхня вбудованість у програмне забезпечення, створює для порушника принципову можливість їхнього обходу;
- можливість злочинної зміни програмних засобів захисту в процесі експлуатації ІС.

4.5 КРИПТОГРАФІЧНІ ЗАСОБИ ЗАХИСТУ

4.5.1 Основні поняття криптографії

Для передавання потрібної інформації потрібному адресату таємно від інших є три можливості.

1. Створити абсолютно надійний, недоступний для інших канал зв'язку між абонентами.

2. Використовувати загальнодоступний канал зв'язку, але приховати сам факт передавання інформації.

3. Використовувати загальнодоступний канал зв'язку, але передавати по ньому потрібну інформацію в такому перетвореному вигляді, щоб відновити її міг тільки адресат.

Прокоментуємо ці три можливості.

1. При сучасному рівні розвитку науки і техніки створити такий канал зв'язку між віддаленими абонентами для кількаразової передачі великих обсягів інформації практично нереально.

2. Розробкою засобів і методів приховування факту передавання повідомлення займається *стеганографія.*

3. Розробкою методів перетворення (шифрування) інформації з метою її захисту від незаконних користувачів займається *криптографія.*

Криптографія – це прикладна наука, яка використовує найсучасніші досягнення фундаментальних наук і, в першу чергу, математики. З іншого боку, всі конкретні завдання криптографії істотно залежать від рівня розвитку техніки і технології, від застосовуваних засобів зв'язку і способів передавання інформації.

Криптографія займається методами перетворення інформації, які б не дозволили зловмиснику витягти її з повідомлень, що перехоплюються. При цьому по каналу зв'язку передається вже не сама інформація, що захищається, а результат її перетворення за допомогою шифру, і для зловмисника виникає складне завдання розкриття шифру.

Тобто, криптографія повинна забезпечити такий захист інформації, що навіть у випадку її перехоплення сторонніми особами й обробки будь-якими способами з використанням найшвидкодіючих комп'ютерів і останніх досягнень науки і техніки вона не повинна бути дешифрована протягом декількох десятків років.

Зашифрування – це процес перетворення інформації, при якому її зміст стає незрозумілим для суб'єктів, що не мають відповідних повноважень.

Результат зашифрування інформації називають *шифротекстом* або *криптограмою*.

Розшифрування – це процес відновлення інформації із шифротексту.

Сукупність процесів зашифрування і розшифрування називають *шифруванням*.

Алгоритми, використовувані при зашифруванні і розшифруванні інформації, звичайно не є конфіденційними, а конфіденційність шифротексту забезпечується використанням при зашифруванні додаткового параметра, називаного *ключем* шифрування. Знання ключа шифрування дозволяє виконати правильне розшифрування шифротексту.

Дешифрування (розкриття шифру) – процес одержання інформації із шифротексту без знання застосованого ключа.

Під *атакою на шифр* розуміють спробу розкриття цього шифру.

Здатність шифру протистояти будь-яким атакам на нього називають *стійкістю шифру*.

Стійкість конкретного шифру оцінюється тільки шляхом усіляких спроб його розкриття і залежить від кваліфікації криптоаналітиків, що атакують шифр.

Кожний програміст уважає себе фахівцем із криптографії, який вміє розробляти алгоритми шифрування, що не зламуються.
"Закони Мерфі для інформаційної безпеки" А.В. Лукацький

Протягом багатьох століть серед фахівців не вщухали суперечки про стійкість шифрів і про можливість побудови абсолютно стійкого шифру. Наведемо три характерних висловлення на цю тему.

"Будь-яка людина, навіть якщо вона не знайома з технікою розкриття шифрів, твердо вважає, що зможе винайти абсолютно стійкий шифр, і чим більш розумна і творча ця людина, тим більш твердо в цьому вона впевнена. Я сам розділяв цю впевненість протягом багатьох років. "

Чарльз Беббідж (19 ст.)

"Будь-який шифр може бути розкритий, якщо тільки в цьому є нагальна потреба й інформація, яку передбачається одержати, коштує витрачених засобів, зусиль і часу..."

Норберт Вінер

"Кожний, хто думає, що винайшов непробивну схему шифрування, – або неймовірний геній, або просто наївний і недосвідчений..."

"Кожний програміст уявляє себе криптографом, що веде до поширення винятково поганого криптозабезпечення..."

Ф. Зімерман (автор шифру PGP)

Останнім часом поряд зі словом "криптографія" часто зустрічається слово "криптологія", але співвідношення між ними не завжди розуміється правильно. Зараз відбувається остаточне формування цих наукових дисциплін, уточнюються їхній предмет і завдання.

Криптологія – наука, що складається із двох галузей: криптографії і криптоаналізу.

Криптографія – наука про способи перетворення (шифрування) інформації з метою її захисту від незаконних користувачів.

Криптоаналіз – наука (і практика її застосування) про методи і способи розкриття шифрів.

Співвідношення криптографії та криптоаналізу очевидне: криптографія – це захист, тобто розробка шифрів, а криптоаналіз – це напад, тобто атака на шифри. Однак ці дві дисципліни пов'язані між собою – не буває гарних криптографів, що не володіють методами криптоаналізу.

4.5.2 Методи шифрування

Криптографія необхідна для реалізації, принаймні, трьох сервісів безпеки:

- шифрування;
- контролю цілісності;
- автентифікації.

Шифрування – найбільш могутній засіб забезпечення конфіденційності. Воно займає центральне місце серед програмно-технічних регуляторів безпеки, бувши основою реалізації багатьох з них, і в той же час останнім (а часом і єдиним) захисним рубежем. Наприклад, для портативних комп'ютерів тільки шифрування дозволяє забезпечити конфіденційність даних навіть у разі крадіжки.

На практиці для шифрування інформації використовують *методи симетричного і асиметричного шифрування.*

Метод симетричного шифрування передбачає використання одного і того ж ключа, що зберігається у секреті, для за шифрування і для розшифрування даних.

Розроблено вельми ефективні (швидкі і надійні) методи симетричного шифрування. Існують і національні стандарти на алгоритми криптографічного перетворення.

На рис. 4.2 наведено схему, що ілюструє використання методу симетричного шифрування.

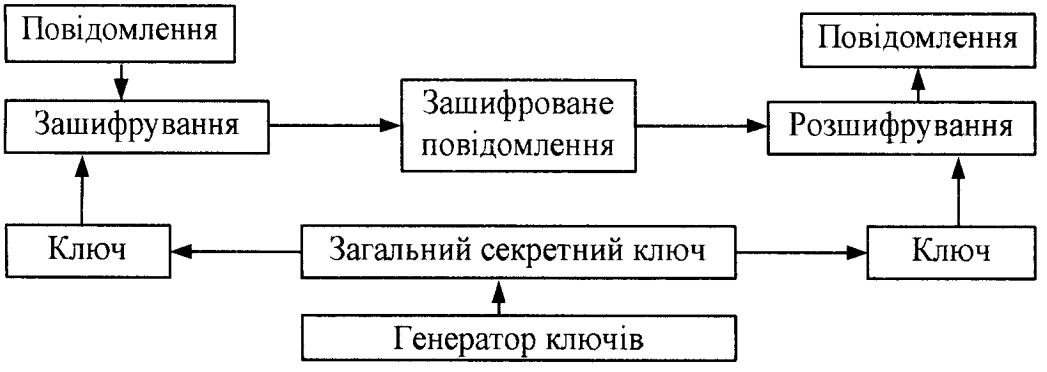


Рисунок 4.2 – Схема використання методу симетричного шифрування

Основним недоліком симетричного шифрування є те, що секретний ключ повинен бути відомий і відправнику, і одержувачу. З одного боку, це створює нову проблему розповсюдження ключів. З іншого боку, одержувач на підставі наявності зашифрованого і розшифрованого повідомлень не може довести, що він одержав це повідомлення від конкретного відправника, оскільки таке ж повідомлення він міг згенерувати самостійно.

В основі **методів асиметричного шифрування** лежить поняття односпрямованої функції, що має такі властивості:

- прості (не вимагають значних ресурсів) обчислення значення функції $y = f(x)$;
- існування оберненої функції $x = f^{-1}(y)$;
- складні (вимагають ресурсів за межами можливостей сучасних комп'ютерів) обчислення значення оберненої функції $x = f^{-1}(y)$.

Фактично в асиметричній криптографії використовується підклас односпрямованих функцій – односпрямовані функції з обхідними шляхами, для яких обернена функція може бути обчислена так само просто, як і пряма, тільки якщо відома спеціальна інформація про обхідні шляхи. Ця спеціальна інформація виконує роль секретного ключа.

Методи асиметричного шифрування передбачають використання двох ключів. Один з них, несекретний (він може публікуватися разом з іншими відкритими відомостями про користувача), застосовується для зашифрування, інший (секретний, відомий тільки одержувачу) – для розшифрування.

Схему методу асиметричного шифрування наведено на рис. 4.3.

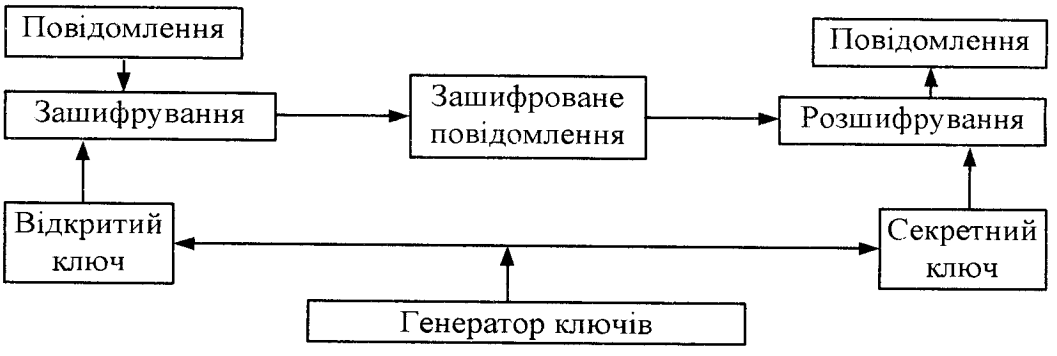


Рисунок 4.3 – Схема використання методу асиметричного шифрування

Найвідомішими асиметричними криптографічними системами є системи RSA (Rivest, Shamir, Adleman), Діффі-Хелмана, Эль-Гамаля і криптосистема на основі еліптичних кривих.

Основними застосуваннями асиметричних криптосистем є:

- передача секретного ключа симетричного шифрування по відкритій мережі (відправник зашифровує цей ключ за допомогою відкритого ключа одержувача, який тільки і зможе розшифрувати отримане повідомлення за допомогою свого секретного ключа);
- системи електронного цифрового підпису для захисту електронних документів (творець документа засвідчує його дійсність за допомогою свого секретного ключа, після чого будь-який власник відповідного відкритого ключа зможе перевірити автентичність даного документа).

Методи асиметричного шифрування також дозволили вирішити важливе завдання спільного формування секретних ключів (це істотно, якщо сторони не довіряють один одному), що обслуговують сеанс взаємодії при початковій відсутності загальних секретів.

Однак сучасні асиметричні криптосистеми не можуть повністю замінити симетричні криптосистеми з таких причин:

- велика тривалість процедур зашифрування і розшифрування (приблизно в 1000 разів більше ніж при симетричному шифруванні);
- необхідність використання істотно більш довгого ключа шифрування для забезпечення тої ж криптостійкості шифру (наприклад, симетричному ключу довжиною 56 бітів відповідає асиметричний ключ довжиною 384 біти, а симетричному ключу довжиною 112 бітів -- асиметричний ключ довжиною 1792 біти).

4.5.3 Криптографічні протоколи

Розв'язання основних задач інформаційної безпеки можна домогтися шляхом реалізації таких криптографічних методів захисту як користувальницької і службової інформації, так і інформаційних ресурсів у цілому:

- шифрування всього інформаційного трафіка, що передається через відкриті мережі передавання даних, і окремих повідомлень;
- криптографічна автентифікація об'єктів, що встановлюють зв'язок;
- захист трафіка, що несе дані, засобами захисту від нав'язування помилкових повідомлень і електронного цифрового підпису з метою забезпечення цілісності і вірогідності переданої інформації;
- шифрування даних, що представлені у вигляді файлів, або що зберігаються в базі даних;
- контроль цілісності програмного забезпечення шляхом застосування криптографічно стійких контрольних сум;
- застосування електронного цифрового підпису для забезпечення юридичної значимості платіжних документів;
- застосування затемненого цифрового підпису для забезпечення неможливості відстеження дій клієнта в платіжних системах, заснованих на понятті електронних грошей.

При реалізації більшості з наведених методів криптографічного захисту виникає необхідність обміну деякою інформацією.

У загальному випадку взаємодія об'єктів (суб'єктів) подібних систем завжди відбувається за певним протоколом.

Протокол – це послідовність дій об'єктів (суб'єктів) для досягнення певної мети.

Криптографічний протокол – це протокол, у якому учасники для досягнення певної мети використовують криптографічні перетворення інформації.

Основні задачі забезпечення інформаційної безпеки, що розв'язуються за допомогою криптографічних протоколів, такі:

- обмін ключовою інформацією з наступним встановленням захищеного обміну даними. При цьому не існує ніяких припущень, чи спілкувалися попередньо між собою сторони, що обмінюються

ключами (наприклад, системи розподілу ключової інформації в розподілених мережах передавання даних);

- автентифікація сторін, що встановлюють зв'язок;
- авторизація користувачів для забезпечення доступу до телекомунікаційних і інформаційних служб.

Завдяки широкому застосуванню таких відкритих мереж передавання даних, як Internet і побудованих на їхній основі мереж Intranet і Extranet криптографічні протоколи знаходять усе більш широке застосування для розв'язання різноманітного кола задач і забезпечення послуг, що надаються користувачам таких мереж.

4.5.4 Контроль цілісності

Криптографічні засоби дозволяють:

- надійно контролювати цілісність як окремих порцій даних, так і їх наборів (таких як потік повідомлень);
- визначати достовірність джерела даних;
- гарантувати неможливість відмовитися від виконаних дій ("безвідмовність").

В основі криптографічного контролю цілісності лежать два поняття: хеш-функція та електронний цифровий підпис.

Хеш-функція – це односпрямована функція. Нехай є початкові дані D, цілісність яких потрібно перевірити, хеш-функція h і раніше обчислений результат її застосування до початкових даних (так званий дайджест) $h(D)$, дані D^*, що перевіряються. Контроль цілісності даних зводиться до обчислення значення хеш-функції $h(D^*)$ і перевірки рівності $h(D^*)=h(D)$. Якщо ця рівність виконується, то вважається, що $D^* = D$.

Збіг дайджестів для різних даних називається колізією. У принципі, колізії можливі, оскільки множини дайджестів менші, ніж множини хешованих даних, проте, оскільки h є односпрямованою функцією, то за прийнятний час спеціально організувати колізію неможливо.

Для вироблення і перевірки **електронного цифрового підпису** (ЕЦП) застосовується асиметричне шифрування.

У найпростішому випадку ЕЦП є зашифрованим на секретному ключі значенням хеш-функції для даних, що підписуються, $E_K(h(D))$.

Електронний цифровий підпис захищає цілісність повідомлення і засвідчує особу відправника, тобто захищає цілісність джерела даних і служить основою безвідмовності.

Для контролю цілісності послідовності повідомлень (тобто для захисту від крадіжки, дублювання і переупорядкування повідомлень) застосовують часові штампи і нумерацію елементів послідовності, при цьому штампи і номери включають у текст, що підписується.

При використанні методів асиметричного шифрування (і, зокрема, для електронного цифрового підпису) необхідно мати гарантію достовірності пари (ім'я користувача, відкритий ключ користувача).

Для вирішення цього завдання в специфікаціях X.509 вводяться поняття *цифрового сертифіката* і *засвідчувального центру.*

Засвідчувальний центр – це компонент глобальної служби каталогів, що відповідає за управління криптографічними ключами користувачів.

Відкриті ключі й інша інформація про користувачів зберігається засвідчувальними центрами у вигляді цифрових сертифікатів, що мають таку структуру:

- порядковий номер сертифіката;
- ідентифікатор алгоритму електронного підпису;
- ім'я засвідчувального центру;
- термін придатності;
- ім'я власника сертифіката;
- відкриті ключі власника сертифіката (ключів може бути декілька);
- ідентифікатори алгоритмів, що асоціюються з відкритими ключами власника сертифіката;
- електронний підпис, що згенеруваний з використанням секретного ключа засвідчувального центру (підписується результат хешування всієї інформації, що зберігається в сертифікаті).

Цифрові сертифікати мають такі властивості:

- будь-який користувач, що знає відкритий ключ засвідчувального центру, може дізнатися відкриті ключі інших клієнтів центру і перевірити цілісність сертифіката;
- ніхто, окрім засвідчувального центру, не може модифікувати інформацію про користувача без порушення цілісності сертифіката.

У специфікаціях X.509 не описується конкретна процедура генерування криптографічних ключів і управління ними, проте даються деякі загальні рекомендації. Зокрема, обумовлюється, що пара ключів може породжуватися будь-яким з таких способів:

- **ключі може генерувати сам користувач**. У такому разі секретний ключ не потрапляє до рук третьої особи, проте потрібно розв'язувати задачу безпечного зв'язку із засвідчувальним центром;
- **ключі генерує довірена особа**. У такому разі доводиться розв'язувати задачі безпечної доставки секретного ключа власнику і надання довірених даних для створення сертифіката;
- **ключі генеруються засвідчувальним центром**. У такому разі залишається тільки завдання безпечного передавання ключів власнику.

4.5.5 Технологія шифрування мови

Розповсюдженим способом шифрування аналогового мовного сигналу є розбиття його на частини.

У цьому випадку вхідний мовний сигнал надходить у смугові фільтри для виділення смуг спектра, що шифрується. Вихідний сигнал кожного фільтра в процесі шифрування піддається або перестановці за частотою, або перевороту спектра (інверсія), або і тому й іншому одночасно. Потім синтезується повний шифрований вихідний сигнал.

За цим принципом працює, наприклад, AVP-система (Analog Voice Prived System) – мовний шифратор (скремблер), що здійснює перестановку окремих "вирізок" вхідного сигналу за допомогою смугового фільтра-

аналізатора. Система має 12 ключів шифрування, обумовлених можливими перестановками, що забезпечує надійність застосовуваного методу. Система використовується в реальному часі з будь-якими уніфікованими телефонами. Якість шифрування мови висока.

Значне поширення знаходять цифрові системи шифрування мовних сигналів. Ці системи забезпечують високу надійність шифрування.

У системах шифрування даних використовуються, в основному, два елементарних перетворення:

- **перестановка** (біти усередині блоку вхідних даних міняються місцями).
- **заміна** (біти усередині блоку вхідних даних заміняються).

Для захисту промислової і комерційної інформації на міжнародному і вітчизняному ринках пропонуються різні технічні пристрої і комплекти професійної апаратури шифрування і криптозахисту телефонних і радіопереговорів.

Поширення одержали так звані скемблери та маскувачі, що замінюють мовний сигнал цифровою передачею даних. Виробляються засоби захисту телетайпів, телексів і факсів. Для цих цілей використовуються шифратори, виконувані у вигляді окремих пристроїв чи у вигляді приставок до апаратів, що вбудовуються в конструкцію телефонів, радіостанцій, факсів-модемів і інших апаратів зв'язку.

4.6 СТЕГАНОГРАФІЧНІ ЗАСОБИ ЗАХИСТУ

Застосування методів криптографії дозволяє приховати від невтаємничених зміст конфіденційної інформації, але не здатне приховати самого факту її наявності або передачі. Методи стеганографії спрямовані на приховання самої присутності конфіденційної інформації.

Стеганографічні методи приховування інформації відомі ще з "докомп'ютерних" часів. Ось кілька прикладів.

Відомий такий спосіб приховання письмового повідомлення: голову раба голили, на шкірі голови писали повідомлення і після відростання волосся раба відправляли до адресата.
З детективних творів добре відомі різні способи тайнопису (від молока до складних хімічних реактивів з наступною обробкою) між рядків звичайного тексту, що не захищається.

XVII - XVIII століття відомі як ера "чорних кабінетів" - спеціальних державних органів перехоплення, перлюстрації та дешифрування переписки. У штат "чорних кабінетів", крім криптографів і дешифрувальників, входили й інші фахівці, зокрема, хіміки. Наявність фахівців-хіміків була необхідною через активне використання так званих “невидимих чорнил”.

Прикладом може служити цікавий історичний епізод: повсталими дворянами в Бордоілі був арештований францисканський чернець Берто, що був агентом кардинала Мазаріні. Повсталі дозволили Берто написати листа знайомому священикові в місто Блей. Однак наприкінці цього листа релігійного змісту чернець зробив приписку, на яку ніхто не звернув увагу: "Посилаю Вам мазь для очей. Натріть нею очі, і Ви будете краще бачити". Так він зумів переслати не тільки приховане повідомлення, але й вказав спосіб його виявлення. У результаті чернець Берто був урятований.

Узагальнену модель стегосистеми наведено на рис. 4.4.

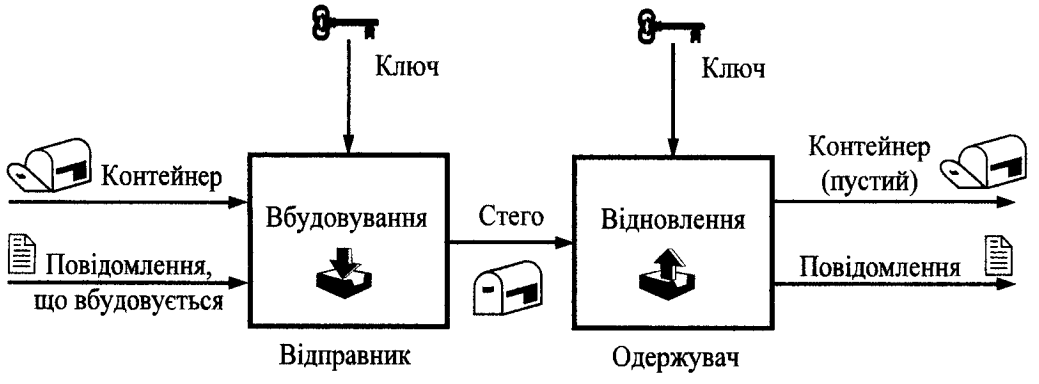


Рисунок 4.4 – Узагальнена модель стегосистеми

Як дані може використовуватися будь-яка інформація: текст, повідомлення, зображення й т.п.

У загальному ж випадку доцільно використовувати слово "повідомлення", тому що повідомленням може бути як текст або зображення, так і, наприклад, аудіодані.

Контейнер – це будь-яка інформація, призначена для приховання таємних повідомлень.

Порожній контейнер – контейнер без убудованого повідомлення; заповнений контейнер або стего-контейнер, що містить вбудовану інформацію.

Стегоключ або просто ключ - секретний ключ, необхідний для приховування інформації. Залежно від кількості рівнів захисту (наприклад, вбудовування попередньо зашифрованого повідомлення) у стегосистемі може бути один або кілька стегоключів.

При побудові стегосистеми повинні враховуватися такі положення:

- супротивник має повне уявлення про стеганографічну систему й деталі її реалізації. Єдиною інформацією, що залишається невідомою потенційному супротивникові, є ключ, за допомогою якого тільки його власник може встановити факт присутності та зміст прихованого повідомлення;
- якщо супротивник якимось чином довідається про факт існування прихованого повідомлення, то це не повинно допомогти йому витягти вбудоване повідомлення доти, поки ключ зберігається в таємниці;
- потенційний супротивник повинен бути позбавлений будь-яких технічних і інших переваг у розпізнаванні або розкритті змісту таємних повідомлень.

За аналогією із криптографією, за типом стегоключа стегосистеми поділяються на два типи:

- з секретним ключем;
- з відкритим ключем.

У стегосистемі із секретним ключем використовується один ключ, що повинен бути визначений або до початку обміну секретними повідомленнями, або переданий по захищеному каналу.

У стегосистемі з відкритим ключем для вбудовування та витягування повідомлення використовуються різні ключі, які розрізняються таким чи-

ном, що за допомогою обчислень неможливо розрахувати один ключ знаючи інший. Тому один ключ (відкритий) може передаватися вільно по незахищеному каналу зв'язку. Крім того, дана схема добре працює й при взаємній недовірі відправника й одержувача.

Будь-яка стегосистема повинна відповідати таким вимогам:

- Властивості контейнера повинні забезпечувати таку модифікацію, щоб зміни неможливо було виявити при візуальному контролі. Ця вимога визначає якість приховання впроваджуваного повідомлення: для забезпечення безперешкодного проходження стегоповідомлення по каналу зв'язку воно жодним чином не повинно привернути увагу того, хто атакує.
- Стегоповідомлення повинно бути стійким до спотворень, у тому числі й зловмисних. У процесі передачі зображення (звук або інший контейнер) може піддаватися різним трансформаціям: зменшуватися або збільшуватися, перетворюватися в інший формат і т.д. Крім того, воно може бути ущільнене, у тому числі й з використанням алгоритмів ущільнення із втратою даних.
- Для збереження цілісності повідомлення, що вбудовується, необхідно використання коду з виправленням помилки.
- Для підвищення надійності повідомлення, що вбудовується, необхідно продублювати.

У наш час існує три напрямки застосування стеганографії: приховування даних (повідомлень), цифрові водяні знаки й заголовки.

Приховування впроваджуваних даних, які в більшості випадків мають великий обсяг, висуває серйозні вимоги до контейнера: розмір контейнера в кілька разів повинен перевищувати розмір даних, що вбудовуються.

Цифрові водяні знаки використовуються для захисту авторських або майнових прав на цифрові зображення, фотографії або інші оцифровані твори мистецтва. Основними вимогами, які висуваються до таких вбудованих даних, є надійність і стійкість до спотворень.

Цифрові водяні знаки мають невеликий обсяг, однак, з урахуванням зазначених вище вимог, для їхнього вбудовування використовуються більш складні методи, ніж для вбудовування просто повідомлень або заголовків.

Заголовки використовуються для маркірування зображень у великих електронних сховищах (бібліотеках) цифрових зображень, аудіо- і відеофайлів.

У цьому випадку стеганографічні методи використовуються не тільки для впровадження ідентифікувального заголовка, але й інших індивідуальних ознак файлу.

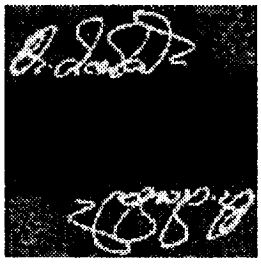
Впроваджувані заголовки повинні вносити незначні спотворення й бути стійкими до основних геометричних перетворень.

Можливі такі варіанти контейнерів:

- контейнер генерується самою стегосистемою. Прикладом може служити програма MandelSteg, у якій як контейнер для вбудовування повідомлення генерується фрактал Мандельброта;
- контейнер вибирається з деякої множини контейнерів. У цьому випадку генерується велика кількість альтернативних контейнерів, щоб потім вибрати такий, що найбільше задовольняє вимоги щодо приховання повідомлення, при цьому найважливішою вимогою є природність контейнера. Єдиною проблемою залишається те, що контейнер дозволяє приховати незначну кількість даних при дуже великому обсязі самого контейнера;
- контейнер надходить ззовні. У цьому випадку відсутня можливість вибору контейнера і тому він не завжди буде задовольняти в повній мірі вимоги повідомлення, що вбудовується.

На рисунках 4.5 та 4.6 представлені варіанти контейнера та вбудована інформація.

а)



б)

Рисунок 4.5 – Контейнер (а) з вбудованим факсимільним зразком підпису (б).

а) б)

Рисунок 4.6 – Контейнер (а) з вбудованим зразком відбитків пальців (б).

Методи стеганографії одержали значний розвиток в останні роки у зв'язку з бурхливим розвитком комп'ютерних технологій.

Комп'ютерна стеганографія базується на таких принципах:

- забезпечення автентичності і цілісності файлу-повідомлення;
- відкритість методів комп'ютерної стеганографії;
- збереження основних властивостей файлу-контейнера після вбудування в нього повідомлення (після цього файл-контейнер можна відкривати, ущільнювати, відновлювати без втрати якості і зміни змісту інформації в контейнері);
- складність витягування повідомлення з файлу контейнера, коли відомо про факт приховання повідомлення, але невідомий ключ.

Основні задачі захисту інформації, які можуть розв'язуватися за допомогою методів комп'ютерної стеганографії:

- захист від несанкціонованого доступу до конфіденційної інформації;
- подолання систем мережевого моніторингу і керування мережевими ресурсами (наприклад, систем промислового шпигунства, що реєструють частоту обміну конфіденційними повідомленнями навіть при відсутності можливості їх розшифрування);
- камуфлювання конфіденційного програмного забезпечення (захист його від використання незареєстрованними користувачами шляхом приховання в мультимедійних файлах);
- захист авторських прав творців (власників) електронних документів шляхом нанесення на файли із цими документами (фото-, аудіо- та відеоматеріалами) спеціальної мітки (водяного знака), розпізнаваного тільки спеціальним програмним забезпеченням.

Відомо дві основні групи методів комп'ютерної стеганографії.

До першої групи методів комп'ютерної стеганографії належать методи, що використовують спеціальні властивості форматів електронних документів:

- зарезервовані для подальшого застосування поля;
- спеціальне форматування текстових документів;
- невикористовувані місця дискової пам'яті (наприклад, останні байти і сектори останнього виділеного файлу кластера);
- імітувальні функції для генерування осмисленого тексту файлу-контейнера для приховуваного повідомлення й ін.

Недоліком методів комп'ютерної стеганографії даної групи є невеликий розмір повідомлення, що може бути приховано в контейнері.

До другої групи методів комп'ютерної стеганографії належать методи, що використовують природну надмірність оцифрованих графічних зображень, звуку і відеоінформації. Ці методи звичайно називають методами останнього значущого біта (Last Significant Bit, LSB). Наприклад, повнокольорові графічні файли у форматі RGB кодують кожну точку (піксел) зображення трьома байтами для подання, відповідно, червоної, зеленої і синьої складових. Зміна кожного із трьох молодших бітів (для зберігання бітів приховуваного повідомлення) приведе до зміни колірних характеристик даної точки зображення менш ніж на 1 %, що абсолютно непомітно для людського ока. Цей метод дозволяє приховати в графічному файлі розміром 800 кілобайтів повідомлення розміром до 100 кілобайтів.

Аналогічно одна секунда оцифрованого звуку із частотою дискретизації 44100 герців і рівнем відліку 8 бітів у стереорежимі дозволяє за методом LSB сховати повідомлення розміром до 10 кілобайтів.

Прикладами відомих програм комп'ютерної стеганографії є Steganos (приховування повідомлень у графічних, звукових, текстових файлах і файлах у форматі HTML) і Contraband (приховування повідомлень у bmp-файлах).

Можливе об'єднання методів криптографії і стеганографії, при якому повідомлення попередньо зашифровується перед вбудовуванням у контейнер.

КОНТРОЛЬНІ ПИТАННЯ

1. Наведіть класифікацію засобів інженерно-технічного захисту.
2. Охарактеризуйте види фізичних засобів захисту.
3. Наведіть класифікацію охоронних систем.
4. Опишіть особливості використання систем охоронного телебачення.
5. Дайте характеристику видам охоронного освітлення і засобам охоронної сигналізації.
6. Опишіть організацію захисту елементів будинків і приміщень.
7. Назвіть переваги та недоліки біометричної ідентифікації та автентифікації.
8. Які задачі захисту розв'язуються за допомогою апаратних засобів?
9. Наведіть класифікацію програмних засобів захисту.
10. Що таке криптографія та шифрування даних?
11. Охарактеризуйте метод симетричного шифрування.
12. Охарактеризуйте методи асиметричного шифрування.
13. Назвіть основні задачі забезпечення інформаційної безпеки, що розв'язуються за допомогою криптографічних протоколів.
14. З використанням чого здійснюється криптографічний контроль цілісності?
15. Опишіть технологію шифрування мови
16. Охарактеризуйте основні методи комп'ютерної стеганографії.
17. Які задачі захисту інформації можуть розв'язуватися за допомогою методів комп'ютерної стеганографії?

СПИСОК ЛІТЕРАТУРИ

1. Закон України "Про інформацію" від 02.10. 1992 р. №2657-XII.

2. Закон України "Про науково-технічну інформацію" від 25.06. 1993 р. №3322-XII.

3. Закон України "Про державну таємницю" від 21.01. 1994 р. №3855-XII.

4. Закон України "Про захист інформації в автоматизованих системах" від 05.07. 1994 р. №80/94-ВР.

5. Закон України "Про Концепцію Національної програми інформатизації" від 04.02. 1998 р. №75/98-ВР.

6. Закон України "Про ліцензування певних видів господарської діяльності" від 01.06. 2000 р. №1775-III.

7. Закон України "Про стандартизацію" від 17.05. 2001 р. №2408-III.

8. Закон України "Про авторське право і суміжні права" від 23.12. 1993 р. №3792-XII (в редакції закону України від 11.07. 2001 р. №2627-III, з подальшими змінами та доповненнями).

9. Закон України "Про електронні документи та електронний документообіг" від 22.05. 2003 р. №851-IV.

10. Закон України "Про електронний підпис" від 22.05. 2003 р. № 852-IV.

11. Закон України "Про охорону прав на промислові зразки" від 15.12. 1993 р. №3688-XII (із змінами і доповненнями станом на 01.01. 2004р.).

12. Закон України "Про охорону прав на знаки для товарів і послуг" від 15.12. 1993 р. №3689-XII (із змінами і доповненнями станом на 01.01. 2004 р.).

13. Постанова Кабінету Міністрів України "Про затвердження Концепції технічного захисту інформації в Україні" від 08.10. 1997 р. №1126.

14. Державний стандарт України ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні поняття, – К.: Держстандарт України, 1996. – 8 с.

15. Державний стандарт України ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. – К.: Держстандарт України, 1996. – 11 с.

16. Державний стандарт України ДСТУ 3396.0-96. Захист інформації. Терміни та визначення. – К.: Держстандарт України, 1996. – 16 с.

17. Правила обов'язкової сертифікації засобів обчислювальної техніки (Затв. наказом Держстандарту України від 25.06. 1997 р. №366).

18. Правила обов'язкової сертифікації технічних засобів охоронної та охоронно-пожежної сигналізації (Затв. наказом Держстандарту України від 10.04. 1997 р. №191).

19. Авраменко В.Ф., Брудний Г.О., Жлобін С.І., Лазарев Г.П., Дорошко В.О. Правові основи охорони інформації. – К.: ТОВ „Поліграф Консалтинг", 2003. – 173 с.

20. Аграновский А.В., Пузыренко А.Н. Компьютерная стеганография: Теория и практика. – МК-Пресс, 2006. – 283 с.

21. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. Учебное пособие. – М.: Гелиос АРВ, 2001. – 480 с.

22. Анин Б. Защита компьютерной информации. – СПб. БХВ-Санкт-Питербург, 2000. – 384 с.

23. Бабак В.П., Корченко О.Г. Інформаційна безпека та сучасні мережеві технології.. – К.: «МК-Пресс», 2003. – 248 с.

24. Бармен Скотт. Разработка правил информационной безопасности. Пер. с англ. – М.: «Вільямс», 2002. – 208 с.

25. Бородин И.А. Основы психологии корпоративной безопасности. - М.: Высшая школа психологии, 2004. — 160 с.

26. Вертузаєв М.С., Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу. Навч. посібник / За ред. С.Г. Лаптева. – К.: Вид-во Європ. ун-ту, 2001. – 321 с.

27. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. В 2-х кн. – М.: Энергоатомиздат, 1994. – 576 с.

28. Голубєв В.О., Гавловський В.Д., Цимбалюк В.С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій. Навч. посібник / За заг. ред. доктора юридичних наук, професора Р.А. Калюжного. – Запоріжжя: ГУ „ЗІДМУ", 2002. – 292 с.

29. Домарев В.В. Безопасность информационных технологий. Методология создания ситем защиты. – К.: ООО «ТИД «ДС», 2001. – 688 с.

30. Дронин А.И. Бизнес-разведка. – М.: Издательство «Ось-89», 2002 - 288 с.

31. Инженерно-техническая защита информации // Торокин А.А. - М.: Гелиос АРВ, 2005. – 960 с.

32. Зегжда Д. П. Как построить защищенную информационную систему // Под ред. Д. П. Зегжды и В. В. Платонова. – СПб: Мир и семья, 1995. – 234 с.

33. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях – М.: КУДИЦ-ОБРАЗ, 2001. – 346 с.

34. Игнатьев В.А. Информационная безопасность современного коммерческого предприятия: Монография. — Старый Оскол: ООО «ТНТ», 2005. — 448 с.

35. Касперски К. Техника сетевых атак. – М.: Солон-Р, 2001. – 524 с.

36. Конахович Г.Ф., Климчук В.П., Паук С.М., Потапов В.Г. Защита информации в телекомуникационных системах. – К.: «МК-Пресс», 2005. – 288 с.

37. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. – СПб: БХВ-Петербург, 2003. – 752 с.

38. Копейкин Г., Лапина Н. Психологические аспекты информационной безопасности организации // Защита информации. Кофидент № 3, 2003.

39. Лукацкий А.В. Обнаружение атак. – СПб: БХВ-Петербург, 2001. – 224 с.

40. Медведев Н.Г., Москалюк Д.В. Аспекты информационной безопасности виртуальных частных сетей. Учебное пособие. – К.: Изд-во Европ. ун-та, 2002. – 95 с.

41. Мельников В.П. Информационная безопасность и защита информации. Учебное пособие. – М.: Издательский центр «Академия», 2008. – 336 с.

42. Одинцов А.А, Защита предпринимательства (информационная и экономическая безопасность). Учебное пособие. –М.: Междунар. отношения, 2003. – 328 с.

43. Основы информационной безопасности. Учебное пособие для вузов / Е.Б. Белов, В.П.Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2006 – 544с.

44. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК, 2000. – 448 с.

45. Петров М.И. Безопасность и персонал. - ООО "Журнал "Управление персоналом", 2006 – 227 с.

46. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях // Под ред. В. Ф. Шаньгина. – М.: Радио и связь, 2001. – 376 с.

47. Сёмкин С.Н., Беляков Э.В., Гребенев С.В., Козачок В.И. Основы организационного обеспечения информационной безопасности объектов информатизации: Учебное пособие. — М.: Гелиос АРВ, 2005. —192 с.

48. Смит Р.Э. Аутентификация: от паролей до открытых ключей. – М.: «Вильямс», 2002. – 432 с.

49. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации: Учеб. пособие. — М.: ИНФРА-М, 2001. — 304 с.

50. Столингс В. Криптография и защита сетей: принципы и практика, 2-е изд. : Пер. с англ. – М.: «Вильямс», 2001. – 672 с.

51. Цирлов В.Л.Основы информационной безопасности автоматизированных систем. – М.: Феникс, 2008 – 87 с.

52. Чмора А.Л. Современная прикладная криптография. – М.: Гелиус АРВ, 2001. – 244 с.

53. Хант Ч., Зартаньян В. Разведка на службе вашего предпреятия. – К.: Укрзакордонвизасервис. 1992 – 196 с.

54. Хорев А.А. Способы и средства зашиты информации. - М.: МО РФ, 2000. - 316 с.

55. Хорошко В.О., Азаров О.Д., Шелест М.Є., Яремчук Ю.Є. Основи комп'ютерної стеганографії. Навчальний посібник. – Вінниця: ВДТУ, 2003. – 143 с.

56. Ярочкин В.И. Информационная безопасность. Учебное пособие. – М.: Междунар. отношения, 2000. – 400 с.

57. Ярочкин В.И., Бузанова Я.В. Корпоративная разведка. - М.: Издательство «Ось-89», 2004 - 288 с.

Навчальне видання

Володимир Андрійович Лужецький
Олеся Петрівна Войтович
Андрій Веніамінович Дудатьєв

Інформаційна безпека

Навчальний посібник

Оригінал-макет підготовлено авторами

Редактор В.О. Дружиніна

Видавництво ВНТУ «УНІВЕРСУМ-Вінниця»
Свідоцтво Держкомінформу України
серія ДК № 746 від 25.12.2001
21021, м. Вінниця, Хмельницьке шосе, 95, ВНТУ
Тел. (0432) 59-85-32

Підписано до друку 26.03.2009 р.
Формат 29,7×42 ¼ Папір офсетний.
Гарнітура Times New Roman.
Друк різографічний. Ум. друк. арк. 27,72.
Наклад 120 прим. Зам № 2009-075.

Віддруковано в комп'ютерному інформаційно-видавничому центрі
Вінницького національного технічного університету
Свідоцтво Держкомінформу України
серія ДК № 746 від 25.12.2001
21021, м. Вінниця, Хмельницьке шосе, 95, ВНТУ
Тел. (0432) 59-81-59


TECHNISCHE
UNIVERSITÄT
DRESDEN


UNIVERSITA'
DEGLI STUDI
DI SALERNO


Вінницький
національний
технічний
університет


Одеський
національний
політехнічний
університет


Інститут
підприємництва
та сучасних
технологій