Методичні вказівки
до виконання самостійної роботи з дисципліни
«Захист інформації в телекомунікаційних системах»
зі спеціальності «Електроніка, електронні комунікації,
приладобудування та радіотехніка»

(освітня програма «Програмне забезпечення

телекомунікаційних систем»)

Міністерство освіти і науки України
Вінницький національний технічний університет

Методичні вказівки до виконання самостійної роботи з дисципліни «Захист інформації в телекомунікаційних системах» зі спеціальності «Електроніка, електронні комунікації, приладобудування та радіотехніка»

(освітня програма «Програмне забезпечення телекомунікаційних систем»)

Вінниця
ВНТУ
2026

Рекомендовано до видання Радою з якості освіти Вінницького національного технічного університету Міністерства освіти і науки України (протокол № 13 від 18.06.2026 р.)

Рецензенти:
А. О. Семенов, доктор технічних наук, професор
О. П. Войтович, кандидат технічних наук, доцент

Методичні вказівки до виконання самостійної роботи з дисципліни «Захист інформації в телекомунікаційних системах» зі спеціальності «Електроніка, електронні комунікації, приладобудування та радіотехніка» (освітня програма «Програмне забезпечення телекомунікаційних систем») / уклад.: Д. В. Михалевський. Електрон. текст. дані. Вінниця : ВНТУ, 2026. 36 с.

Методичні вказівки містять матеріали для самостійного опрацювання навчальної програми із дисципліни «Захист інформації в телекомунікаційних системах» для освітньої програми «Програмне забезпечення телекомунікаційних систем». Наведено матеріали для самостійного опрацювання та закріплення теоретичних знань на базі тестів самоконтролю та індивідуальних завдань дослідницького характеру.

ЗМІСТ

1 ЗАГАЛЬНІ ПОЛОЖЕННЯ 4

ТЕМА 1. ОСНОВНІ ПОЛОЖЕННЯ ТЕОРІЇ 6

ТЕМА 2. КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ 9

ТЕМА 3. АНАЛІЗ ТА МОНІТОРИНГ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ 13

ТЕМА 4. СИСТЕМИ ВИЯВЛЕННЯ АТАК 16

ТЕМА 5. ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ 19

ТЕМА 6. ОСНОВНІ ШЛЯХИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ .. 22

ТЕМА 7. ЗАСОБИ, МЕТОДИ І СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ 25

ТЕМА 8. ОСНОВИ КРИПТОГРАФІЇ ТА ШИФРУВАННЯ 28

ЗАВДАННЯ ДЛЯ ПІДГОТОВКИ ДО ЗАЛІКУ 31

ПЕРЕЛІК ЛІТЕРАТУРНИХ ДЖЕРЕЛ 35

1 ЗАГАЛЬНІ ПОЛОЖЕННЯ

Методичні вказівки до самостійної роботи з дисципліни «Захист інформації в телекомунікаційних системах» мають на меті узагальнити набуті теоретичні знання сучасних методів та засобів захисту інформації у телекомунікаційних мережах, а також передбачає вивчення основних проблем захисту інформації у телекомунікаційних та радіотехнічних системах, а також аналіз та тестування комплексних систем інформаційної безпеки. Також передбачається надання допомоги в організації самостійної роботи студентів з вивчення навчального матеріалу та підготовки до складання заліку.

Метою дисципліни «Захист інформації в телекомунікаційних системах» є формування основних знань та положень у майбутнього фахівця системи знань і практичних навиків в галузі інформаційної безпеки телекомунікаційних систем.

Основними завданнями вивчення дисципліни є визначення стратегії розвитку сучасних методів та засобів захисту телекомунікаційних систем та їх застосування; формування теоретичної бази, практичних навиків і представлення про технічний і криптографічний захист інформації; канали витоку інформації; виявлення загроз інформації в інформаційно-телекомунікаційних системах і забезпечення їхньої інформаційної безпеки.

Навчальна дисципліна «Захист інформації в телекомунікаційних системах» базується на результатах навчання, здобутих під час вивчення таких компонент, як теорія передачі інформації, інтернет-технології та вебдизайн.

За результатами вивчення дисципліни студенти набувають компетентностей:

ІК. Здатність розв’язувати спеціалізовані задачі та практичні проблеми у галузі телекомунікацій та радіотехніки, що характеризується комплексністю та невизначеністю умов.

СК1. Здатність розуміти сутність і значення інформації в розвитку.

СК2. Здатність вирішувати стандартні завдання професійної діяльності на основі інформаційної та бібліографічної культури із застосуванням інформаційно-комунікаційних технологій і з урахуванням основних вимог інформаційної безпеки.

СК5. Здатність використовувати нормативну та правову документацію, що стосується інформаційно-телекомунікаційних мереж, телекомунікаційних та радіотехнічних систем (закони України, технічні регламенти, міжнародні та національні стандарти, рекомендації Міжнародного союзу електрозв’язку і т.п.) для вирішення професійних завдань.

СК18 Здатність до застосування існуючих та створення нових програмно-апаратних засобів тестування телекомунікаційного та радіотехнічного обладнання.

А також програмні результати навчання:

РН1. Аналізувати, аргументувати, приймати рішення при розв’язанні спеціалізованих задач та практичних проблем телекомунікацій та радіотехніки, які характеризуються комплексністю та неповною визначеністю умов.

РН2. Застосовувати результати особистого пошуку та аналізу інформації для розв’язання якісних і кількісних задач подібного характеру в інформаційно-комунікаційних мережах, телекомунікаційних і радіотехнічних системах.

РН6. Адаптуватись в умовах зміни технологій інформаційно-комунікаційних мереж, телекомунікаційних та радіотехнічних систем.

РН7. Грамотно застосовувати термінологію галузі телекомунікацій та радіотехніки.

РН21. Забезпечувати надійну та якісну роботу інформаційно-комунікаційних мереж, телекомунікаційних та радіотехнічних систем.

ТЕМА 1. ОСНОВНІ ПОЛОЖЕННЯ ТЕОРІЇ ЗАХИСТУ ІНФОРМАЦІЇ

1. Яке основне завдання теорії захисту інформації?
а) Оптимізація обробки даних
б) Забезпечення конфіденційності, цілісності та доступності інформації
в) Підвищення швидкості передачі даних
г) Збільшення обсягу збережуваної інформації

2. Що входить до складу базової тріади інформаційної безпеки (CIA)?
а) Конфіденційність, автентичність, аудит
б) Цілісність, доступність, контроль
в) Конфіденційність, цілісність, доступність
г) Автентифікація, авторизація, аудит

3. Що входить до складу базової концепції інформаційної безпеки?
а) Конфіденційність, автентичність, аудит
б) Цілісність, доступність, контроль
в) Конфіденційність, цілісність, доступність
г) Автентифікація, авторизація, аудит

4. Що таке автентифікація?
а) Процес визначення прав доступу до ресурсів
б) Процес перевірки автентичності особи або пристрою
в) Процес шифрування даних
г) Процес резервного копіювання інформації

5. Який із заходів представляє організаційний рівень захисту інформації?
а) Встановлення відеоспостереження
б) Фізичне обмеження доступу до серверних кімнат
в) Розробка політики безпеки інформації
г) Застосування криптографічного шифрування даних

6. Як слід розуміти поняття «ризик» у контексті захисту інформації?
а)Як ймовірність виникнення загрози у поєднанні з потенційними наслідками
б) Як абсолютна відсутність заходів безпеки
в) Як результат технічних збоїв устаткування
г) Як тільки математична оцінка вразливостей

7. Який із наведених методів є прикладом технічного захисту інформації?

а) Навчання персоналу

б) Застосування шифрування даних

в) Розробка політик управління доступом

г) Проведення аудиту безпеки

8. Що включає фізичний захист інформації?

а) Використання антивірусного програмного забезпечення

б) Створення та підтримка політик безпеки

в) Обмеження фізичного доступу до серверних приміщень та обладнання

г) Використання криптографічних алгоритмів

9. Які з наступних варіантів найкраще відображають основний набір завдань інформаційної безпеки?

а) Конфіденційність, цілісність, доступність

б) Швидкість, ефективність, масштабованість

в) Надійність, зручність використання, економічність

г) Ідентифікація, аналіз, контролювання

10. Що таке загроза інформаційній безпеці?

а)Плановий аудит систем безпеки

б) Потенціал або можливість виникнення події, що може вплинути на конфіденційність, цілісність або доступність даних

в) Техніка резервного копіювання

г) Метод шифрування інформації

11. Що таке вразливість інформаційної системи?

а) Надійна система захисту даних

б) Недолік або слабке місце в системі, яке може бути використане зловмисниками для отримання несанкціонованого доступу чи зміни даних

в) Стратегія моніторингу інформаційних потоків

г) Захищене з’єднання між пристроями

12. Ризик в контексті інформаційної безпеки

а) Неможливість зберегти дані після атаки

б) Застосування резервного копіювання даних

в) Поєднання ймовірності реалізації загрози через певну вразливість та величини можливих збитків

г) Процедура автентифікації користувача

13. Які з наведених методів є основними для забезпечення конфіденційності даних у телекомунікаційних системах?

а) Використання криптографічних алгоритмів, VPN,
систем контролю доступу та багатофакторної автентифікації

б) Монотонне оновлення програмного забезпечення

в) Виключно резервне копіювання інформації

г) Моніторинг мережевого трафіку без додаткових заходів захисту

14. У чому полягає різниця між автентифікацією та авторизацією?

а) Автентифікація шифрує дані, авторизація їх декодує

б) Автентифікація – це процес встановлення з’єднання, авторизація – забезпечення доступності

в) Немає різниці, це синоніми

г) Автентифікація – перевірка особистості користувача, а авторизація – це визначення прав доступу після успішної автентифікації

15. Які з наступних принципів є основними для створення ефективної системи захисту інформації?

а) Defense in Depth (багаторівневий захист), принцип найменших привілеїв, неперервний моніторинг і аудит, адаптивність та резервне копіювання з відновленням

б) Централізований контроль, використання одного рівня захисту, зниження витрат

в) Максимальна доступність, відкритий доступ до систем, мінімальні заходи безпеки

г) Фокус лише на фізичному захисті, відмова від криптографічних методів, ігнорування організаційних аспектів

Таблиця правильних відповідей

1	2	3	4	5	6	7	8
б	в	в	б	в	а	б	в

9	10	11	12	13	14	15
а	б	б	в	а	г	а

ТЕМА 2. КАНАЛИ ВИТОКУ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

1. Що означає термін «канал витоку інформації» в контексті телекомунікаційних систем?

а) Засіб для ефективної передачі зашифрованих даних між легітимними користувачами

б) Несанкціонований шлях передачі інформації, що виникає через побічні ефекти роботи обладнання

в) Протокол для забезпечення цілісності даних

г) Метод оптимізації передачі інформації у мережі

2. Яким із наступних варіантів є прикладом використання електромагнітного каналу витоку інформації?

а) Створення захищених тунелів VPN для передачі даних

б) Використання шифрування для кодування інформаційного потоку

в) Аудит мережевого трафіку за допомогою систем моніторингу

г) Збір електромагнітних випромінювань, що випадково генеруються

3. Який із наступних варіантів найкраще описує акустичний канал витоку інформації?

а) Передача даних через оптичні волокна

б) Використання радіочастотних сигналів для зв’язку

в) Несвідоме випромінювання звукових сигналів пристроями, яке може бути перехоплено для отримання інформації

г) Захищена передача голосових даних через VoIP

4. Що може стати основою оптичного каналу витоку інформації?

а) Неправильна конфігурація мережевого обладнання

б) Атаки за допомогою шкідливого програмного забезпечення

в) Несвідоме випромінювання світла з дисплеїв, індикаторів або оптичних кабелів, що може передавати інформацію

г) Фізичне ушкодження волоконно-оптичних ліній зв’язку

5. Який із наведених методів ефективно зменшує ризик витоку інформації через канали сторонніх ефектів?

а) Застосування потужних передавачів даних для збільшення сигналу

б) Екранізація обладнання, належне заземлення та зниження побічних випромінювань

в) Використання лише програмних засобів шифрування

г) Підвищення інтенсивності роботи обладнання для посилення сигналу

6. Який із наступних підходів є найбільш ефективним для виявлення витоків інформації через ненавмисні канали?

а) Використання стандартних мережевих моніторів з базовою антивірусною перевіркою

б) Використання спеціалізованих сенсорів та аналізу електромагнітних, акустичних або оптичних сигналів, що представляють побічні ефекти

в) Регулярне моделювання мережевого трафіку

г) Застосування програмних рішень для оптимізації пропускної здатності мережі

7. Які з наступних факторів можуть підвищувати ризик витоку інформації через електромагнітні канали?

а) Відсутність екранізації, неналежне заземлення та застосування старого або несправного обладнання

б) Використання сертифікованого захищеного обладнання з належною екранізацією

в) Підвищене використання алгоритмів цифрового шифрування

г) Використання оптичних волокон для організації з’єднань

8. Які з наведених заходів є найбільш ефективними для зниження ризику витоку інформації через канали, що виникають внаслідок побічних ефектів роботи обладнання?

а) Регулярне оновлення програмного забезпечення систем безпеки

б) Перехід на бездротові технології зв’язку

в) Застосування одноразових пристроїв для разових комунікацій

г) Використання спеціалізованої апаратури з високим рівнем екранізації, належним заземленням та впровадженням технологій відведення побічних сигналів

9. Який із наступних варіантів описує фактор, сприятливий для виникнення оптичного витоку інформації?

а) Надмірне зовнішнє освітлення, що приглушує сигнал дисплею

б) Використання сучасних оптичних волокон з високою пропускною здатністю

в) Несанкціоноване випромінювання світла з дисплеїв, індикаторів або оптичних кабелів, що може бути перехоплено

г) Обмежене використання візуальних індикаторів у пристроях

10. Який з наступних методів є найбільш ефективним для виявлення витоків інформації через електромагнітні, акустичні та оптичні побічні канали?

а) Застосування спеціалізованих сенсорів та обладнання для моніторингу електромагнітних, акустичних і оптичних сигналів

б) Аналіз логів доступу до мережевих серверів
в) Використання стандартних мережевих моніторів з базовою антивірусною перевіркою
г) Періодичне оновлення програмного забезпечення пристроїв

11. Який із наступних сценаріїв найкраще описує ризик витоку інформації через магнітний канал?
а) Пристосування високоякісних кабелів із вбудованим екрануванням
б) Відсутність належного магнітного екранірування, що дозволяє магнітним полям розповсюджуватись за межі пристроїв
в) Використання інфрачервоних сенсорів для моніторингу температури обладнання
г) Організація спеціалізованих кімнат для серверів із кондиціонуванням повітря

12. Яке з наведених рішень є ефективним для своєчасного виявлення витоків інформації через побічні канали?
а) Використання спеціалізованих програмних засобів для аналізу електромагнітних, акустичних та оптичних сигналів
б) Регулярне оновлення антивірусного програмного забезпечення
в) Інтеграція стандартних логів роботи мережевого обладнання
г) Застосування класичних систем моніторингу за доступом до файлів

13. Як фізичне розміщення обладнання впливає на потенціал витоку інформації через побічні канали?
а) Розташування обладнання не має значного впливу, якщо дані зашифровані
б) Некоректне розміщення обладнання поза спеціальними захисними зонами може сприяти появі побічних сигналів, що використовуються для витоку інформації
в) Правильне фізичне розміщення забезпечує лише оптимальну передачу даних, без впливу на безпеку
г) Розміщення обладнання у відкритому просторі знижує ризик витоку завдяки природній вентиляції

14. Який із наведених заходів не сприяє запобіганню витоку інформації через побічні канали?
а) Використання екранованих кабелів і належного заземлення пристроїв
б) Регулярне проведення технічних перевірок та моніторингу обладнання
в) Встановлення спеціалізованих сенсорів для оперативного виявлення витоків
г) Збільшення потужності передавача з метою посилення сигналу

15. Який із наступних чинників є менш сприятливим для виникнення витоку інформації через побічні канали?

а) Сильні електромагнітні перешкоди, що надходять від зовнішніх джерел

б) Інтенсивне шумове навантаження та вібрації в робочій зоні

в) Контрольований клімат та стабільні умови в спеціально обладнаних серверних кімнатах

г) Нерегульоване середовище з нестабільними електропостачанням і підвищеними механічними навантаженнями

Таблиця правильних відповідей

1	2	3	4	5	6	7
б	г	в	в	б	б	а

8	9	10	11	12	13	14	15
г	в	а	б	а	б	г	в

ТЕМА 3. АНАЛІЗ ТА МОНІТОРИНГ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

1. Що таке аналіз безпеки телекомунікаційних систем?

а) Процес оцінки фінансової ефективності IT-інфраструктури

б) Системний підхід до виявлення вразливостей, оцінки ризиків і загроз телекомунікаційних систем

в) Метод оптимізації швидкості передачі даних через мережу

г) Процедура резервного копіювання інформації

2. Який із наступних засобів найбільш підходить для забезпечення моніторингу безпеки телекомунікаційних систем у режимі реального часу?

а) Система інформаційної безпеки та управління подіями

б) Антивірусне програмне забезпечення

в) Статичне резервне копіювання логів

г) VPN-технології

3. Які етапи включає процес аналізу безпеки телекомунікаційних систем?

а) Розгортання нових мережевих рішень і оптимізація обладнання

б) Тестування швидкодії каналів та оптимізація трафіку

в) Розподіл прав доступу між користувачами

г) Збирання інформації, виявлення вразливостей, оцінка ризиків та розробка заходів для мінімізації загроз

4. Який із наступних методів найбільш ефективно використовується для виявлення аномалій у мережевому трафіку?

а) Ручний аналіз логів без застосування алгоритмів

б) Використання систем поведінкового аналізу та методів машинного навчання для аналізу логів і трафіку

в) Періодичне оновлення шкідливих програм

г) Застосування класичного алгоритму шифрування даних

5. Що таке SIEM і яка її основна функція в контексті моніторингу безпеки?

а) Платформа для збору, аналізу, кореляції подій безпеки і генерації сповіщень про інциденти

б) Система для оптимізації мережевого трафіку

в) Програмне забезпечення для архівації даних

г) Інструмент для шифрування комунікаційних потоків

6. Який із наведених засобів використовується для пасивного моніторингу мережевого трафіку?

а) IDS-системи

б) IPS-системи

в) VPN-клієнти

г) Засоби резервного копіювання даних

7. Які дані є ключовими для аналізу безпеки телекомунікаційних систем?

а) Фінансові звіти, маркетингові дослідження і дані продажів

б) Дані про виробничі процеси

в) Логи подій, мережевий трафік, дані автентифікації та інформація з систем моніторингу

г) Географічні дані про розташування офісів

8. Який із заходів дозволяє суттєво знизити час реагування на інциденти безпеки?

а) Регулярне оновлення операційних систем

б) Впровадження автоматизованої системи кореляції подій із функціями оповіщення

в) Розгортання додаткових VPN-з’єднань

г) Підвищення швидкості резервного копіювання даних

Тест 9. Який із наступних підходів є ключовим для кореляції подій у процесі моніторингу безпеки?

а) Ручне зведення даних із різних джерел

б) Моніторинг лише одного джерела даних (наприклад, тільки мережевого трафіку)

в) Автоматизований аналіз даних із різних логів і систем подій для виявлення закономірностей та аномалій

г) Ізолювання окремих IP-адрес без аналізу контексту

10. Який із наступних компонентів не входить до повного циклу аналізу та моніторингу безпеки телекомунікаційних систем?

а) Планування бюджетних витрат на маркетингові стратегії

б) Збирання даних з різних джерел (логи, трафік, дані аутентифікації)

в) Оцінка ризиків і виявлення вразливостей

г) Реагування на інциденти та впровадження заходів щодо усунення недоліків

11. Який із наступних методів дозволяє здійснювати детальний аналіз мережевого трафіку шляхом розбору пакетів на рівні протоколів?

а) Ручний аналіз логів за допомогою текстових редакторів

б) Загальний аналіз статистики використання пропускної здатності

в) Використання стандартних мережевих моніторів без додаткової обробки даних

г) Глибока перевірка пакетів

12. Яка з наступних переваг є основною при інтеграції систем штучного інтелекту в процес моніторингу мережі?

а) Збільшення обсягу зберігання логів

б) Можливість прогнозування загроз на основі аналізу великих даних та виявлення аномалій

в) Підвищення швидкості передачі даних у мережі

г) Спрощення протоколів шифрування інформації

13. Яка технологія дозволяє збирати статистичні дані про потоки мережевого трафіку для подальшого аналізу безпеки?

а) FTP (File Transfer Protocol)

б) SMTP

в) NetFlow

г) ICMP

14. Як хмарні технології сприяють ефективнішому моніторингу безпеки телекомунікаційних систем?

а) Забезпечують ізоляцію мережевих сегментів, але не об’єднують дані

б) Забезпечують централізований збір і аналіз даних із різних джерел для виявлення загроз у режимі реального часу

в) Автоматично усувають всі загрози без участі адміністратора

г) Виключають потребу в локальних системах збереження логів

15. Який метод дозволяє ефективно виявляти підозрілу активність користувачів у системі?

а) Періодичне оновлення паролів для всіх користувачів

б) Блокування облікових записів після одного невдалого входу

в) Поведінковий аналіз користувацької активності із застосуванням алгоритмів машинного навчання

г) Використання статики для порівняння показників роботи системи

Таблиця правильних відповідей

1	2	3	4	5	6	7
б	а	г	б	а	а	в

8	9	10	11	12	13	14	15
б	в	а	г	б	в	б	в

ТЕМА 4. СИСТЕМИ ВИЯВЛЕННЯ АТАК

1. Що таке система виявлення атак?
а) Програма для резервного копіювання інформації
б) Система, яка здійснює моніторинг мережевої або системної активності для виявлення ознак атак або аномальної поведінки
в) Засіб для оптимізації пропускної здатності мережі
г) Оперативна система для управління серверним обладнанням

2. Які з наступних варіантів є основними категоріями систем виявлення атак?
а) Апаратні та програмні засоби
б) Системи з відкритим та закритим кодом
в) Системи моніторингу трафіку та системи аналізу логів
г) Мережеві та хостові системи виявлення атак

3. Який із методів виявлення характерний для систем, що використовують базу підписів
а) Аналіз поведінки користувачів
б) Виявлення аномалій за допомогою машинного навчання
в) Порівняння вхідних даних з базою відомих шаблонів атак
г) Визначення збоїв у апаратному забезпеченні

4. Який з наступних описів найбільш відповідає аномальному методу виявлення атак?
а) Виявлення атак за допомогою порівняння з наперед заданими підписами
б) Використання статистичних моделей для прогнозування нормальної поведінки і виявлення відхилень
в) Аналіз потоку даних з використанням статистичних показників та алгоритмів машинного навчання, що дозволяють виявити нетипову активність
г) Автоматичне блокування мережевого трафіку без попереднього аналізу

5. Що таке хибно-позитивне спрацювання у контексті IDS?
а) Ситуація, коли система помилково класифікує легітимну активність як атаку
б) Ситуація, коли атака не була виявлена системою
в) Процес автоматичного відновлення після атаки
г) Функція системи, що збільшує точність виявлення атак

6. Яка основна відмінність між системами виявлення атак та системами запобігання атак?

а) IDS блокують атаку, а IPS лише реєструють подію

б) IDS здійснюють моніторинг та сигналізують про підозрілу активність, тоді як IPS можуть автоматично вживати заходів для блокування загрози

в) IDS застосовуються тільки для мережевого трафіку, а IPS – тільки для системних журналів

г) IDS і IPS виконують однакову функцію, відрізняються лише інтерфейсом

7. Який з наступних підходів найчастіше використовується для покращення виявлення аномалій за допомогою машинного навчання?

а) Встановлення жорстких правил на основі підписів атак

б) Виключно використання статистичних порогів для фільтрації даних

в) Ручне оглядання кожного окремого запису журналу подій

г) Побудова моделей поведінкового аналізу на основі історичних даних для ідентифікації відхилень від норми

8. Який підхід є найбільш ефективним для виявлення атаки нульового дня?

а) Специфічно налаштований аналіз заздалегідь підписів атак

б) Ручне моделювання атак на основі історичних даних

в) Використання аномального методу виявлення із застосуванням машинного навчання для аналізу поведінки

г) Виключно мережеве сегментування без аналізу трафіку

9. Яка з наступних характеристик є обмеженням сигнатурного виявлення атак?

а) Забезпечення високої швидкості обробки даних

б) Неможливість виявлення невідомих атак, оскільки не мають відповідних підписів

в) Простота інтеграції з іншими системами безпеки

г) Мінімальний рівень хибних спрацювань

10. Яка перевага гібридних систем, що комбінують сигнатурне та аномальне виявлення?

а) Виключно базуються на статичних правилах

б) Автоматично усувають виявлені загрози без участі адміністратора

в) Застосовуються тільки на хостових рівнях системи

г) Забезпечують ширший спектр виявлення завдяки комбінації фіксованих підписів та аналізу відхилень від нормальної поведінки

11. Що відрізняє розподілені системи виявлення атак від традиційних централізованих?

а) Розподіляють сенсори по мережевих сегментах для локального збору та попередньої обробки даних із подальшою централізованою кореляцією

б) Виключно обробляють дані з центрального сервера

в) Застосовуються лише для захисту окремих хостів

г) Повністю замінюють потребу в системах

12. Який метод є найбільш ефективним для виявлення складних, маргінальних аномалій у поведінці системи?

а) Виключно застосування статичних правил, заснованих на підписах

б) Використання простих порогів для сповіщень про відхилення

в) Застосування розширених алгоритмів машинного навчання для аналізу поведінкових особливостей і виявлення нетипової активності

г) Ручний аналіз кожної окремої події в реальному часі

13. Яка основна функція honeypot у контексті виявлення атак?

а) Забезпечення додаткових ресурсів для хостинга легітимних сервісів

б) Приманка для зловмисників з метою виявлення та аналізу атакуючих методів

в) Систематизація оновлень підписів

г) Шифрування даних перед передачею в мережі

14. Яка з наступних характеристик описує технологію sFlow у контексті виявлення атак?

а) Застосовується для збереження повних копій усього мережевого трафіку

б) Забезпечує шифрування мережевого трафіку для підвищення безпеки

в) Використовується для аналізу лише голосового трафіку

г) Використовує метод семплінгу для збору даних про мережеві потоки, що дозволяє оцінювати патерни трафіку

Таблиця правильних відповідей

1	2	3	4	5	6	7
б	г	в	в	а	б	г

8	9	10	11	12	13	14
в	б	г	а	в	б	г

ТЕМА 5. ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

1. Що таке технології захисту інформації?
а) Комплекс методів, засобів та процедур для забезпечення конфіденційності, цілісності та доступності інформації
б) Методики організації резервного копіювання даних
в) Виключно криптографічні алгоритми
г) Система управління IT-персоналом

2. Який із наступних алгоритмів є симетричним засобом шифрування?
а) RSA
б) AES
в) ECC
г) SHA-256

3. До якого типу криптографічних алгоритмів належить RSA?
а) Симетричні алгоритми
б) Гібридні алгоритми
в) Асиметричні алгоритми
г) Хеш-функції

4. Яка з наступних функцій використовується для забезпечення цілісності даних?
а) AES
б) RSA
в) SHA-256
г) ECC

5. Що лежить в основі цифрового підпису як технології забезпечення захисту інформації?
а) Шифрування даних за допомогою симетричного ключа
б) Використання пари ключів для створення унікального відбитку даних і подальшої перевірки їх цілісності
в) Виключно хешування даних без шифрування
г) Технологія резервного копіювання

6. Яка основна мета використання відкритих ключів у сфері захисту інформації?
а) Організація централізованого зберігання резервних копій даних
б) Захист від DDoS атак
в) Моніторинг мережевого трафіку
г) Забезпечення підписання, шифрування та автентифікації даних за допомогою сертифікатів і пар ключів

7. Що таке VPN у контексті технологій захисту інформації?
а) Засіб для створення захищеного тунелю і шифрування переданої інформації через незахищені мережі
б) Система виявлення аномалій у мережевому трафіку
в) Протокол цифрових підписів
г) Технологія резервного копіювання даних

8. Яка основна функція протоколів TLS/SSL у захисті інформації?
а) Формування цифрових підписів документів
б) Забезпечення захищеного з'єднання між клієнтом і сервером шляхом шифрування даних
в) Архівування та резервне копіювання файлів
г) Моніторинг мережевого трафіку

9. Яка з наступних переваг апаратного шифрування порівняно з програмним шифруванням?
а) Вища гнучкість налаштування
б) Вища продуктивність і зменшення навантаження на центральний процесор
в) Простота інтеграції з програмним забезпеченням
г) Можливість використання на будь-якому апаратному забезпеченні без спеціалізованих модулів

10. Яка основна функція цифрових сертифікатів у рамках інфраструктури відкритих ключів?
а) Забезпечення зашифрованого зберігання даних
б) Оптимізація передачі мережевого трафіку
в) Автентифікація суб'єктів обміну інформацією та зв'язок між публічним і приватним ключами
г) Моніторинг логів безпеки

11. Яка характеристика блокчейн-технології сприяє забезпеченню цілісності інформації?
а) Централізована архітектура з надійним сервером
б) Автоматичне резервне копіювання даних
в) Використання симетричного шифрування для всіх транзакцій
г) Децентралізована структура з використанням хеш-функцій, що зв'язують блоки даних і гарантують незмінність записів

12. Який із наступних протоколів використовується для забезпечення захищених вебз'єднань?
а) TLS/SSL
б) FTP

в) SMTP
г) IMAP

13. Яка з наступних технологій дозволяє забезпечити збереження інформації на випадок її втрати?
а) Шифрування даних за допомогою AES
б) Статичне шифрування файлів
в) Регулярне резервне копіювання із застосуванням автоматизованих систем зберігання
г) Використання систем моніторингу аномалій

14. Як віртуалізація сприяє підвищенню рівня захисту інформації?
а) Забезпечує підвищену швидкість передачі даних
б) Дозволяє ізолювати робочі середовища, що зменшує ризик поширення атак між підсистемами
в) Оптимізує конфігурацію апаратного забезпечення
г) Збільшує обсяг доступного сховища даних

15. Яка з наступних технологій дозволяє обмежити поширення кібератак в межах організації?
а) Використання одного типу шифрування для всієї мережі
б) Резервне копіювання даних
в) Мережева сегментація та мікросегментація для ізоляції критичних систем
г) Аналіз логів за допомогою SIEM без інтеграції з іншими захисними заходами

Таблиця правильних відповідей

1	2	3	4	5	6	7
г	б	в	в	б	г	а

8	9	10	11	12	13	14	15
б	б	в	г	а	в	б	в

ТЕМА 6. ОСНОВНІ ШЛЯХИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ

1. Що таке забезпечення безпеки інформації?

а) Комплекс організаційних, технічних, правових та фізичних заходів, спрямованих на підтримання конфіденційності, цілісності та доступності інформації

б) Сукупність заходів із резервного копіювання даних

в) Набір криптографічних алгоритмів для шифрування інформації

г) Метод оптимізації мережевої інфраструктури

2. Який із наступних підходів відноситься до організаційних заходів забезпечення безпеки інформації?

а) Розробка, впровадження та моніторинг політик безпеки, стандартів і процедур

б) Використання сучасних антивірусних програм

в) Застосування криптографічних методів шифрування

г) Встановлення систем фізичного контролю доступу

3. Який із наведених прикладів є технічним заходом забезпечення безпеки інформації?

а) Розробка нормативно-правових актів

б) Впровадження засобів шифрування, мережевих брандмауерів, IDS/IPS-систем і антивірусного захисту

в) Навчання співробітників основам безпеки

г) Створення корпоративних кодексів етики

4. Що означає принцип конфіденційності в системах безпеки інформації?

а) Захист інформації від несанкціонованого доступу та її розголошення

б) Забезпечення високої доступності інформації для всіх користувачів

в) Автоматичне резервне копіювання даних

г) Оптимізація потоків мережевого трафіку

5. Що входить до поняття цілісності інформації?

а) Забезпечення доступності інформації в режимі 24/7

б) Захист від мережевих атак за допомогою шифрування

в) Створення резервних копій даних

г) Гарантування того, що інформація не була змінена або спотворена несанкціонованим чином

6. Який із наступних заходів спрямований на забезпечення доступності інформації?

а) Використання систем резервного копіювання, відмовостійких архітектур і високодоступних серверів

б) Впровадження складних криптографічних алгоритмів

в)Розробка корпоративних політик безпеки

г) Обмеження доступу через фізичне сек'юритування

7.Який із наступних варіантів відноситься до правових заходів забезпечення безпеки інформації?

а) Використання систем шифрування та криптографії

б) Налаштування мережевих брандмауерів і систем IDS/IPS

в) Розробка та впровадження нормативно-правових актів, стандартів договорів щодо захисту даних

г) Організація фізичного контролю доступу до серверних кімнат

8. Який із наступних прикладів ілюструє фізичні заходи у забезпеченні безпеки інформації?

а) Розробка внутрішніх політик безпеки даних

б) Впровадження шифрування інформації за допомогою апаратних засобів

в) Встановлення систем контролю доступу (біометрія, карткові системи) та організація охоронних заходів у приміщеннях

г) Моніторинг мережевого трафіку за допомогою SIEM-систем

9. Який із наступних варіантів найкраще характеризує комплексний підхід до забезпечення безпеки інформації?

а) Використання виключно технічних засобів захисту

б) Застосування лише правових норм і стандартів

в) Інтеграція організаційних, технічних, правових та фізичних заходів для комплексного захисту інформації

г) Виключно впровадження резервного копіювання даних

10. Які з наступних заходів становлять основні шляхи забезпечення безпеки інформації у сучасних організаціях?

а) Лише використання криптографічних методів

б) Всі заходи, спрямовані виключно на забезпечення фізичного захисту

в) Виключно технічні заходи з моніторингу системи

г) Комплексний підхід, що включає організаційні, технічні, правові та фізичні заходи, спрямовані на забезпечення конфіденційності, цілісності та доступності інформації

11. Які з наведених цілей є базовими для забезпечення безпеки інформації?

а) Конфіденційність, цілісність, доступність

б) Ефективність, зручність, швидкодія

в) Надійність, масштабованість, інноваційність

г) Контроль, аудит, моніторинг

12. Що таке автентифікація в контексті безпеки інформації?

а) Процес розподілу повноважень

б) Процес підтвердження особистості користувача

в) Процес збереження резервної копії даних

г) Процес виявлення кібератак

13. Що таке контроль доступу у системах інформаційної безпеки?

а) Процес забезпечення доступності системи без обмежень для всіх

б) Процес обмеження доступу лише для авторизованих користувачів

в) Процес збереження резервних копій даних

г) Процес шифрування конфіденційної інформації

14. Який з наступних пристроїв або систем найбільше спрямований на виявлення несанкціонованого доступу у мережі?

а) Фаєрвол

б) Антивірусне ПЗ

в) Система виявлення вторгнень (IDS)

г) Резервне копіювання

15. Який із наступних заходів відноситься до технічних, а не організаційних методів забезпечення безпеки?

а) Розробка політик безпеки

б) Проведення аудиту безпеки

в) Встановлення міжмережевого екрана (фаєрвола)

г) Навчання персоналу

Таблиця правильних відповідей

1	2	3	4	5	6	7
а	а	б	а	г	а	в

8	9	10	11	12	13	14	15
в	в	г	а	б	б	в	в

ТЕМА 7. ЗАСОБИ, МЕТОДИ І СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

1. Яке з наведених визначень найкраще описує поняття «засоби захисту інформації»?

а) Комплекс апаратних, програмних і організаційних засобів для забезпечення безпеки інформації

б) Лише апаратні засоби, що використовуються для збереження даних

в) Тільки програмні рішення для моніторингу системи

г) Сукупність внутрішніх політик та інструкцій

2. Який із наступних елементів є прикладом технічного засобу захисту інформації?

а) Розробка корпоративних політик безпеки

б) Навчання персоналу з питань інформаційної безпеки

в) Міжмережевий екран

г) Проведення аудиту безпеки

3. Які засоби захисту інформації використовують криптографічні методи для забезпечення конфіденційності та цілісності даних?

а) Фізичний контроль доступу

б) Шифрування та хешування

в) Оргтехнологічні заходи

г) Системи резервного копіювання

4. Який із наступних методів використовується для перевірки цілісності даних?

а) Шифрування

б) Автентифікація

в) Резервне копіювання

г) Хешування

5. Яке з наступних визначень найкраще характеризує систему управління інформаційною безпекою?

а) Система виключно для забезпечення шифрування даних

б) Лише апаратні засоби моніторингу мережевого трафіку

в) Збірник внутрішніх правил без механізмів реагування на інциденти

г) Інтегрована платформа, що поєднує технічні, організаційні та фізичні заходи захисту

6. Що з наведеного є прикладом фізичного захисту інформації?

а) Відеоспостереження серверних приміщень

б) Встановлення вірулентного антивірусного програмного забезпечення

в) Створення резервних копій даних

г) Використання криптографічних протоколів

7. Який із наступних методів спрямований на запобігання несанкціонованому фізичному доступу до інформаційних ресурсів?

а) Біометрична автентифікація

б) Системи контролю доступу

в) Використання VPN-туннелів

г) Хешування паролів

8. Яке завдання є ключовим для організаційних заходів безпеки в інформаційних системах?

а) Забезпечення апаратного захисту серверних кімнат

б) Встановлення фаєрволів

в) Реалізація криптографічного захисту

г) Розробка та впровадження політик і стандартів безпеки

9. Який із наведених варіантів найкраще описує комплексний підхід до захисту інформації у телекомунікаційних системах?

а) Використання лише систем шифрування для захисту даних

б) Застосування тільки фізичного захисту для обмеження доступу

в) Інтеграція технічних засобів, організаційних заходів, фізичного захисту та навчання персоналу

г) Моніторинг мережевого трафіку без інших заходів

10. Який із наступних заходів забезпечує захист від атак типу «відмова у обслуговуванні» (DoS) на рівні мережевого трафіку?

а) Використання складних паролів

б) Фільтрація трафіку

в) Резервне копіювання

г) Аудит систем безпеки

11.Яка технологія є однією з найбільш надійних для реалізації автентифікації в умовах підвищених кіберзагроз?

а) Біометрична автентифікація

б) Простий пароль

в) Використання статичних логінів

г) Застосування шифрування дисків

12. Який із наступних елементів є ключовим для управління ризиками у системах захисту інформації?

а) Регулярне оновлення програмного забезпечення

б) Фізичний захист серверів

в) Аудит та моніторинг систем безпеки

г) Використання складних користувацьких паролів

13. Який із наступних елементів характерний для систем виявлення вторгнень?

а) Аналіз мережевого трафіку для виявлення підозрілої активності

б) Резервне копіювання критичних даних

в) Фізичний контроль доступу до серверних кімнат

г) Організація внутрішніх політик безпеки

14. Який із наведених методів дозволяє забезпечити контроль доступу до інформаційних ресурсів?

а) Резервне копіювання інформації

б) Моніторинг мережевого трафіку

в) Фізичний захист серверних приміщень

г) Використання комплексної системи автентифікації та авторизації

15. Який із наступних підходів є найбільш ефективним для захисту хмарних сервісів?

а) Використання шифрування даних як при зберіганні, так і при передачі

б) Фізичний захист локальних серверів

в) Застосування виключно організаційних заходів

г) Використання простих паролів для доступу

Таблиця правильних відповідей

1	2	3	4	5	6	7
а	в	б	г	г	а	б

8	9	10	11	12	13	14	15
г	в	б	а	в	а	г	а

ТЕМА 8. ОСНОВИ КРИПТОГРАФІЇ ТА ШИФРУВАННЯ

1. Що таке криптографія?
а) Технологія фізичного захисту серверів
б) Наука про захист інформації за допомогою шифрування
в) Метод моніторингу мережевого трафіку
г) Варіанти а-в вірні

2. Який із наведених алгоритмів є прикладом симетричного шифрування?
а) RSA
б) ECC
в) D. DSA
г) AES

3. Яким ключем користується алгоритм асиметричного шифрування для розшифрування даних?
а) Приватним ключем
б) Тільки симетричним ключем
в) Загальнодоступним ключем
г) Кодом авторизації

4. Що означає властивість "цілісність даних" у контексті криптографії?
а) Доступ до даних має лише авторизований користувач
б) Дані можуть бути відновлені після пошкодження
в) Дані є доступними для всіх користувачів
г) Дані залишаються незміненими під час передачі

5. Який алгоритм використовується для створення хеш-функцій?
а) SHA-256
б) AES
в) RSA
г) DES

6. Що з наведеного є перевагою асиметричного шифрування?
а) Використання одного і того ж ключа для шифрування та розшифрування
б) Висока швидкість обробки даних
в) Можливість передавати загальнодоступний ключ для шифрування повідомлень
г) Надмірне навантаження на процесор

7. Який із наведених алгоритмів шифрування відноситься до асиметричних?

а) A. AES

б) DES

в) RSA

г) Blowfish

9. Яка з наведених особливостей є характерною для хеш-функцій?

а) Вони є оборотними (можна розшифрувати дані).

б) Вони генерують унікальний вихідний код фіксованого розміру для будь-якого вхідного повідомлення.

в) Вони використовуються лише для забезпечення конфіденційності.

г) Вони є прикладом симетричного шифрування.

10. Який із наведених стандартів використовується для захисту веб-даних за допомогою шифрування?

а) HTTPS (SSL/TLS)

б) FTP

в) SMTP

г) POP3

11. У якому із випадків може бути ефективно застосовано стеганографію?

а) Захист системних даних від зовнішніх атак

б) Шифрування великого об’єму даних для резервного копіювання

в) Прихований обмін конфіденційною інформацією у публічних мережах

г) Генерація криптографічних ключів

12. Який із нижченаведених принципів є основою асиметричного шифрування?

а) Використання однакового ключа для шифрування та дешифрування

б) Розділення на публічний і приватний ключ

в) Використання криптографічних хеш-функцій для шифрування

г) Детерміноване перетворення даних

13. Чому електронний цифровий підпис є важливим для безпеки електронної комунікації?

а) Він виключно шифрує дані

б) Забезпечує анонімність відправника

в) Використовується для генерації криптографічних ключів

г) Гарантує цілісність, автентичність та невідмовність повідомлення

14. Що з наведеного найкраще визначає поняття «криптографічний протокол»?

а) Набір математичних алгоритмів для створення хешів

б) Стандартизований набір правил та процедур для безпечного обміну інформацією

в) Метод шифрування на основі простих чисел

г) Метод випадкового генерування ключів

15. Чому важлива генерація криптографічно сильних випадкових чисел?

а) Для забезпечення унікальності ключів

б) Для оптимізації швидкості шифрування

в) Для зменшення розміру шифротексту

г) Для покращення інтерфейсу програми

Таблиця правильних відповідей

1	2	3	4	5	6	7
г	г	а	г	а	в	в

8	9	10	11	12	13	14	15
б	а	в	б	г	а	б	а

ЗАВДАННЯ ДЛЯ ПІДГОТОВКИ ДО ЗАЛІКУ

1 модуль

1. Інформація як об’єкт захисту.
2. Характеристика загроз безпеці інформації.
3. Основні означення та поняття теорії захисту інформації.
4. Інформаційна безпека в телекомунікаційних та радіотехнічних системах.
5. Вразливість в телекомунікаційних та радіотехнічних системах.
6. Канали витоку інформації та їх класифікація.
7. Загрози безпеці інформації в телекомунікаційних та радіотехнічних системах.
8. Канали несанкціонованого отримання інформації.
9. Проблеми захисту інформації в комп’ютерних системах.
10. Види комп’ютерних злочинів. Причини поширення комп’ютерної злочинності.
11. Поняття і класифікація комп’ютерних вірусів.
12. Стратегія та архітектура захисту інформації.
13. Політика безпеки інформації.
14. Види забезпечення безпеки інформації.
15. Засоби захисту інформації в комп’ютерних системах.
16. Методи і системи захисту інформації.
17. Методи ідентифікації і встановлення достовірності об’єктів і суб’єктів.
18. Особливості захисту інформації в телекомунікаційних та радіотехнічних системах.
19. Загрози інформації в телекомунікаційних та радіотехнічних системах.
20. Захист в телекомунікаційних та радіотехнічних систем від несанкціонованого доступу.

2 модуль

1. Електромагнітні канали витоку інформації технічними засобами передачі інформації.
2. Електромагнітні канали витоку інформації ВЧ випромінювання технічних засобів передачі інформації.
3. Електромагнітні канали витоку інформації на частотах самозбудження підсилювачів низької частоти
4. Електричні канали витоку – наводки електромагнітних випромінювань.
5. Електричні канали витоку – проникнення інформаційних каналів у ланки живлення.

6. Електричні канали витоку – проникнення інформаційних каналів у ланки заземлення.

7. Електричні канали витоку – електричні закладки.

8. Повітряні акустичні канали витоку інформації.

9. Вібраційно-акустичні канали витоку інформації.

10. Електроакустичні канали витоку інформації.

11. Оптоелектронні канали витоку інформації.

12. Акустично-параметричні канали виток інформації.

13. Витік інформації через випромінювання від активного мережевого обладнання.

14. Витік інформації через електромагнітне випромінювання трафіку локальних мереж.

15. Витік інформації через прийом та перевипромінення інтерференційних мереж.

16. Витік інформації через віруси.

17. Візуальні канали витоку інформації.

18. Індукційні канали витоку інформації.

19. Параметричні канали витоку інформації.

20. Програмні та апаратні закладки.

Студенти денної та заочної форми навчання, за рішенням кафедри, можуть готувати окремі науково-дослідні роботи за індивідуальними темами у вигляді рефератів з окремих тем курсу або підготовка доповіді на щорічну науково-теоретичну конференцію викладачів, співробітників та студентів ВНТУ, в рамках СРС та практичних занять за наступними темами:

1. Аналіз сучасних загроз у телекомунікаційних системах.

Необхідно провести огляд останніх кіберзагроз, з якими стикаються телекомунікаційні мережі (DDoS, фішинг, атаки типу «людина посередині» тощо). Передбачає дослідження еволюції загроз за останні 5 років із формуванням аналітичного звіту, що містить опис загроз, їхніх характеристик та можливі наслідки.

2. Розробка політики безпеки для телекомунікаційної компанії

Необхідно сформулювати основні принципи та вимоги до політик інформаційної безпеки для організації. Оцінити практичні аспекти впровадження стандартних процедур (аудит, моніторинг, реагування на інциденти) та підготувати алгоритми дій реагування на загрози безпеки.

3. Дослідження криптографічних алгоритмів у захисті даних

Необхідно провести аналіз основних алгоритмів симетричного (AES) і асиметричного шифрування (RSA, ECC) та їх застосування в телекомунікаціях. Провести порівняльний аналіз за критеріями продуктивності, стійкості та застосованості в різних сценаріях. Підготувати рекомендації щодо вибору алгоритмів для конкретних прикладних завдань.

4. Оцінка ризиків та побудова моделі управління безпекою

Необхідно провести системний аналіз вразливостей типового телекомунікаційного середовища. Розробити модель оцінки ризиків із використанням сучасних методик (наприклад, аналіз SWOT або методика CVSS). Запропонувати комплекс заходів для зниження ризиків і продемонструвати їхню ефективність через аналіз сценаріїв.

5. Практичне впровадження засобів захисту мережі

Необхідно встановити та налаштувати засоби мережевого захисту (VPN, IDS/IPS, Firewall). Провести дослідження та тестування ефективності застосовуваних рішень у локальній мережі. Порівняти результати тестування з рекомендованими стандартами безпеки.

6. Розробка плану реагування на атаку мережі

Необхідно описати етапи виявлення, аналізу та реагування на порушення інформаційної безпеки. Розробіть план реагування із зазначенням ролей, обов'язків та процедур відновлення роботи мережі.

7. Вивчення стандартів та нормативних документів (ISO/IEC)

Необхідно дослідити вимоги стандартів ISO/IEC 27001, 27002 та інші, що стосуються захисту інформації. Проаналізувати, як ці стандарти можна адаптувати для телекомунікаційних систем. Підготувати рекомендації щодо впровадження та сертифікації відповідних систем безпеки.

8. Огляд безпеки мереж 5G

Необхідно дослідити специфіку захисту інформації в мережах 5G, враховуючи нові архітектурні рішення та протоколи. Проаналізувати типові вразливості 5G і запропонувати методи їхнього усунення з перспективами розвитку безпеки в контексті впровадження 5G.

9. Моделювання та симуляція кіберзахисту в телекомунікаційних системах

Необхідно побудувати модель телекомунікаційної мережі з акцентом на визначення слабких місць. Проаналізувати спеціалізоване програмне забезпечення (наприклад, симулятори мереж) для моделювання атак та оцінки ефективності заходів захисту. Описати результати симуляцій та сформулювати практичні рекомендації щодо посилення захисту.

10. Етичні та правові аспекти захисту інформації

Необхідно провести аналіз нормативно-правових актів, що регулюють захист інформації в телекомунікаційних системах в Україні та за кордоном. Розглянути етичні дилеми, пов'язані з впровадженням засобів масового моніторингу та збору даних. Провести комплексний аналіз з пропозиціями щодо вдосконалення законодавства та корпоративних стандартів етики.

11. Використання інструментів штучного інтелекту для аналізу аномалій у мережах

Необхідно дослідити сучасні алгоритми машинного навчання (кластеризація, нейронні мережі, методи підтримки векторних машин тощо), які застосовуються для виявлення аномалій у телекомунікаційних мережах. Вибрати одну з платформ (наприклад, TensorFlow або PyTorch) та дослідити прототип системи аналізу мережевого трафіку, що виявляє підозрілі патерни поведінки. Провести тестуванняв лабораторних умовах, використовуючи симульований трафік для імітації реальних атак; порівняйте результати з традиційними методами виявлення аномалій. Провести аналіз параметрів: точність, швидкість реагування та відсоток хибно-позитивних спрацьовувань системи. Також надайте рекомендації щодо її інтеграції в реальні мережеві інфраструктури.

12. Інтеграція технологій блокчейн у захист даних

Необхідно дослідити принципи роботи блокчейн-технологій, звертаючи увагу на ключові властивості – децентралізацію, незмінність та прозорість. Дослідити існуючі приклади використання блокчейн для забезпечення цілісності даних, зокрема у сфері телекомунікацій (наприклад, захист ідентичності абонентів або механізми аудиту даних). Розробити модель концептуальної інтеграції блокчейн-рішення у вже існуючу систему захисту даних. Розгляньте питання сумісності з існуючими протоколами, визначте можливі переваги і загрози від впровадження технології. За можливості створіти прототип або концепт-документ, що демонструє, як блокчейн може підвищити рівень безпеки інформації у телекомунікаційних мережах, і надайте рекомендації щодо масштабування рішення.

ПЕРЕЛІК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Карачка А. Ф. Технології захисту інформації : конспект лекцій. Тернопіль : ТНЕУ, 2017. 86 с.

2. Вишня В. Б., Гавриш О. С., Рижков Е. В. Основи інформаційної безпеки : навч. посіб. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.

3. Жилін А. В., Шаповал О. М., Успенський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / КПІ ім. Ігоря Сікорського. Київ : Політехніка, 2021. 213 с.

4. Гапак О. М., Балога С. І. Захист інформації в комп'ютерних системах : підручник. Ужгород : ДВНЗ «УжНУ», 2021. 184 с.

5. Захист інформації в телекомунікаційних системах : навч. посіб. / Конахович Г. Ф., Климчук В. П., Паук С. М. та ін. Київ : НАУ, 2009. 380 с.

6. Захист інформації в автоматизованих системах управління : навч. посіб. / уклад.: І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. Житомир : Вид-во ЖДУ ім. І. Франка, 2015. 226 с.

Електронне навчальне видання

Дмитро Валерійович Михалевський

Методичні вказівки до виконання самостійної роботи з дисципліни «Захист інформації в телекомунікаційних системах» зі спеціальності «Електроніка, електронні комунікації, приладобудування та радіотехніка» (освітня програма «Програмне забезпечення телекомунікаційних систем»)

Рукопис оформив: *Д. Михалевський*

Редактор: *Н. Кравчук*

Оригінал-макет виготовлено РВВ ВНТУ

Підписано до видання 5.08.2026
Гарнітура TimesNewRoman.
Зам. № Р2026-107.

Видавець та виготовлювач
Вінницький національний технічний університет,
Редакційно-видавничий відділ.
ВНТУ, ГНК, к. 114.
Хмельницьке шосе, 95,
м. Вінниця, 21021.
press.vntu.edu.ua;
Email: rvv.vntu@gmail.com
Свідоцтво суб'єкта видавничої справи
серія ДК No 3516 від 01.07.2009 р.