МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
Циклова комісія *комп'ютерних систем та мереж*
(повна назва циклової комісії)

Допустити до захисту
Голова випускової циклової комісії
комп'ютерних систем та мереж
(повна назва циклової комісії)
_____ *Ірина КРАВЧУК*
(підпис) (ім'я, ПРІЗВИЩЕ)
« 10 » 06 2025 р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ
ФАХОВИЙ МОЛОДШИЙ БАКАЛАВР

Тема: *Інформаційна безпека в комп'ютерній мережі*

Група: *3-012* Спеціальність: *123 «Комп'ютерна інженерія»*

Здобувач освіти _____ *Михайло НОВІКОВ*
(підпис) (ім'я, ПРІЗВИЩЕ)

Керівник роботи _____ *Марія КИСЛОВА*
(підпис) (ім'я, ПРІЗВИЩЕ)

Консультант з оформлення
пояснювальної записки _____ *Оксана ОСАДЧА*
(підпис) (ім'я, ПРІЗВИЩЕ)

Кривий Ріг 2025 р.

КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Відділення *комп'ютерної та програмної інженерії*
Циклова комісія *комп'ютерних систем та мереж*
Освітній ступінь *фаховий молодший бакалавр*
Спеціальність *123 «Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Голова випускової циклової комісії
комп'ютерних систем та мереж
(повна назва циклової комісії)
(підпис) *Ірина КРАВЧУК*
(ім'я, ПРІЗВИЩЕ)
« 10 » 06 2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ОСВІТИ

Новікову Михайлу Вадимовичу
(прізвище, ім'я, по батькові)

1.Тема роботи *Інформаційна безпека в комп'ютерній мережі*

Керівник роботи *Кислова Марія Алімівна – викладач, «спеціаліст вищої категорії», кандидат педагогічних наук.*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по коледжу від « *04* » *04* 2025 року № *50-ст*

2. Строк подання здобувачем освіти роботи з *01.03.2025* по *15.06.2025*

3. Вихідні дані до роботи *План розміщення кімнат. Існуюча структурна схема комп'ютерної мережі. Вибір систем захисту інформації.*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) *Постановка проблеми та її вирішення. Комп'ютерна мережа та аналіз її вразливостей. Розробка систем захисту.*

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Презентація Microsoft PowerPoint

6. Консультанти розділів роботи (проекту)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	*Узгодження технічного завдання*	*01.03.2025*	
2	*Огляд літератури по темі*	*15.03.2025*	
	кваліфікаційної роботи		
3	*Постановка проблеми та її вирішення*	*28.04.2025*	
4	*Комп'ютерна мережа та аналіз її*	*14.05.2025*	
	вразливостей		
5	*Розробка систем захисту*	*26.05.2025*	
6	*Оформлення пояснювальної записки*	*06.06.2025*	
7	*Захист кваліфікаційної роботи*		

Здобувач освіти _____ *Михайло НОВІКОВ*
(підпис) (ім'я, ПРІЗВИЩЕ)

Керівник роботи _____ *Марія КИСЛОВА*
(підпис) (ім'я, ПРІЗВИЩЕ)

StrikePlagiarism.com

Дата звіту 6/2/2025

Дата редагування ---

Документ прийнятий

Звіт подібності

метадані

Назва організації

Ukrainian national aviation university

Заголовок

Новіков М_3-012_2025_КПІ

Автор Науковий керівник / Експерт

Новіков-2Гринченко О

підрозділ

Криворізький Фаховий коледж

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

18.01%
18.01%
КП 1

0.87%
0.87%
КЦ

25
Довжина фрази для коефіцієнта подібності 2

9432
Кількість слів

79309
Кількість символів

РЕФЕРАТ

Пояснювальна записка до кваліфікаційної роботи «Інформаційна безпека в комп’ютерній мережі» викладена на 60 с., містить 13 рис., 18 використаних літературних джерел.

КОМП’ЮТЕРНА МЕРЕЖА, ЗАХИСТ ІНФОРМАЦІЇ, КРИПТОГРАФІЧНИЙ ЗАХИСТ, АНТИВІРУСНА ПРОГРАМА.

Кваліфікаційна робота присвячена аналізу системи захисту інформації та пропозиції щодо удосконалення системи захисту.

Широке поширення засобів обчислювальної техніки, збільшення обсягів збереженої інформації в обчислювальних системах обробки даних різко підвищили уразливість інформації і процесу її обробки. У зв'язку з цим проблема захисту інформаційно-програмного забезпечення обчислювальних систем стала однієї з головних проблем в області автоматизованої обробки даних.

Матеріали кваліфікаційної роботи рекомендується використовувати при проведені наукових досліджень, у навчальному процесі та в практичній діяльності фахівців з проектування систем захисту інформації.

Тема кваліфікаційної роботи є актуальною і має теоретичне і практичне значення.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА ТЕРМІНІВ

АС – автоматизована система.

ЛОМ – локальна обчислювальна мережа.

ОМ – обчислювальна мережа.

ОС – операційна система.

ОЗП – оперативно-запам’ятовуючий пристрій.

ПЗ – програмне забезпечення.

World Wide Web (WWW) – абстрактний інформаційний простір у мережі Інтернет. Є середовищем для обміну інформації (як правило *Web*-сторінки). Інтернет – глобальна комп'ютерна мережа заснована на стеці протоколів *TCP/IP*, що забезпечує зв'язок між комп'ютерами.

Інтерфейс (користувача) – сукупність програмних засобів, що забезпечують взаємодію користувача з комп'ютером.

Ethernet - базова технологія локальних обчислювальних мереж з комутацією пакетів, що використовує протокол *CSMA/CD*.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) – технологія

множинного доступу до загального передавального середовища в локальній комп'ютерній мережі з контролем колізій.

ВСТУП

В Україні значні трансформації в економіці, які включають розвиток фінансових інститутів та диверсифікацію форм власності, кардинально змінили підхід до захисту інформації. Раніше, в часи домінування державної власності, акцент був на секретних розвідувальних даних під контролем потужних спецслужб. Однак сьогодні, з повсюдним впровадженням цифрових технологій, особливо комп'ютерних систем, у всі сфери життя, інформаційна безпека набуває критичного значення.

Зростання кіберзагроз та важливість сертифікації

Сучасні виклики у сфері кібербезпеки зумовлені стрімким розвитком інформаційних технологій. Кібератаки можуть бути спрямовані на апаратне забезпечення (комп'ютери, периферійні пристрої), програмне забезпечення, бази даних та користувачів. Будь-який збій у комп'ютерній мережі не лише негативно впливає на моральний стан співробітників та керівництва, а й призводить до значних фінансових втрат.

В епоху електронних платежів та безпаперового документообігу серйозний збій у локальній мережі може повністю паралізувати роботу компанії чи банку. Тому захист даних у комп'ютерних мережах є однією з найважливіших проблем сучасної інформатики.

Наразі в інформаційній безпеці встановлено два ключові принципи, що забезпечують надійність мереж:

- Цілісність даних: Захист від помилок, що можуть призвести до втрати, несанкціонованого пошкодження або знищення інформації.
- Конфіденційність інформації: Забезпечення доступу до інформації лише уповноваженим користувачам.

Окремі галузі, такі як банківський сектор, державні установи, оборонні та спеціальні структури, вимагають посилених заходів безпеки та мають підвищені

вимоги до надійності інформаційних систем, залежно від характеру та важливості виконуваних ними завдань.

Метою роботи є проведення комплексного аналізу сучасних методів та технологій захисту інформації в комп'ютерних мережах. Для цього буде детально розглянуто основні аспекти функціонування комп'ютерних мереж, а також вивчено та уточнено ключові концепції систем безпеки. На основі отриманих знань буде проведено всебічний аналіз актуальних методів забезпечення інформаційної безпеки, що дозволить розробити практичні рекомендації для ефективного захисту даних.

РОЗДІЛ 1
ПОСТАНОВКА ПРОБЛЕМИ ТА ЇЇ ВИРІШЕННЯ

1.1 Загальна характеристика об'єктів управління

Ця робота зосереджена на технічному захисті інформації в комп'ютерних мережах. Основні завдання, що розглядаються, включають:

1. Аналіз поточного стану комп'ютерної мережі.

2. Оцінка поточних методів зберігання інформації в мережевих системах. 3. Розробка рекомендацій щодо вдосконалення систем захисту для комп'ютерних мережевих технологій.

Технологія побудови локальної мережі

В офісному середовищі використовується технологія *Fast Ethernet*. Ця технологія, розроблена *Xerox* у 1970-х роках і стандартизована *IEEE* 802.3 у 1980-х, базується на методі доступу до середовища *CSMA/CD* (*Carrier Sense Multiple Access with Collision Detection*).

Принцип роботи *CSMA/CD* полягає в тому, що мережева карта "прослуховує" мережу перед передачею даних, щоб переконатися, що вона вільна. Якщо середовище зайняте, адаптер відкладає передачу; в іншому випадку, він починає передачу. У випадку одночасної передачі даних двома адаптерами виникає колізія, і передача переривається. Адаптер отримує всі пакети в мережі для визначення

адресата.

Ethernet, *Fast Ethernet* та *Gigabit Ethernet* забезпечують пропускну здатність 10, 100 та 1000 Мбіт/с відповідно.

Основний недолік *Ethernet* полягає в ефективності доступу до середовища: при великій кількості одночасних передавачів зростає число колізій, що знижує пропускну здатність мережі, потенційно до нуля. Навіть при середньому навантаженні (30-40% від максимального) фактична швидкість передачі становить лише 70-80% від номінальної. Цей недолік частково нівелюється використанням мережевих комутаторів (світчів) замість концентраторів.

Переваги комутаторів та зворотна сумісність

Мережевий комутатор (світч) - це пристрій, що з'єднує кілька вузлів комп'ютерної мережі в межах одного сегмента. На відміну від концентратора, який розсилає трафік на всі підключені пристрої, комутатор направляє дані безпосередньо до отримувача. Це значно покращує продуктивність та безпеку мережі, запобігаючи обробці нецільових даних іншими сегментами.

Комутатори функціонують на канальному рівні моделі *OSI*, працюючи з *MAC* адресами мережевих вузлів. Для з'єднання різних мереж на мережевому рівні використовуються маршрутизатори.

При увімкненні комутатор починає з порожньої таблиці *MAC*-адрес (режим навчання). У цьому режимі дані з будь-якого порту передаються на всі інші порти. Комутатор аналізує кадри, визначає *MAC*-адресу відправника і заносить її в таблицю. Згодом, якщо кадр призначений для відомої *MAC*-адреси, він передається лише через відповідний порт. Якщо адреса невідома, кадр надсилається на всі інтерфейси, поки комутатор не сформує повну таблицю, локалізуючи трафік.

Значною перевагою різних версій *Ethernet* є їхня зворотна сумісність, що дозволяє взаємозамінне використання в мережі, часто без заміни існуючої кабельної інфраструктури.

Операційні системи та апаратне забезпечення

Всі клієнтські комп'ютери працюють під управлінням *Windows* 10. Сервери використовують операційну систему *Linux*. Все використовуване програмне

забезпечення є ліцензійним. Використання єдиної операційної системи на клієнтських машинах спрощує налаштування та подальше обслуговування.

Фізичне середовище комп'ютерної мережі - це матеріальна основа для передачі інформації. Для підключення офісних комп'ютерів використовується неекранована вита пара.

Мережева топологія

Використовувана топологія мережі – "зірка" або "розподілена зірка". У топології "зірка" всі комп'ютери підключені до центрального комутатора за допомогою окремих сегментів кабелю. Сигнал від комп'ютера-відправника

передається на всі інші комп'ютери через цей центральний пристрій. Ця топологія, що виникла на зорі обчислювальної техніки, передбачає централізований зв'язок між комп'ютерами.

Недоліки топології "зірка": для великих мереж значно збільшується споживання кабелю. Крім того, вихід з ладу центрального компонента (комутатора) призводить до паралічу всієї мережі.

Однак, якщо з ладу виходить лише один комп'ютер або кабель, що з'єднує його з комутатором, це впливає лише на даний пристрій, не порушуючи роботу решти мережі.

Серверна інфраструктура

Основний сервер – *Dell PowerEdge R*720*XD,* оснащений двома 6-ядерними процесорами *XEON E*5-2620 2.0 *GHz,* 32 ГБ оперативної пам'яті *DDR*4 та 12 жорсткими дисками *Western Digital Ultrastar DC HC*310 *SAS* об'ємом 12 ТБ кожен. На серверах встановлена операційна система *Linux*.

Файловий сервер є центральним елементом локальної мережі. Він хостить операційну систему та контролює потік даних у мережі. До сервера підключаються персональні робочі станції та всі спільні периферійні пристрої, такі як принтери та сканери.

Кожна робоча станція є звичайним персональним комп'ютером з власною операційною системою (*Windows* 10). На відміну від окремого ПК, робоча станція оснащена мережевою інтерфейсною картою та фізично підключена до сервера за допомогою кабелю. Крім того, на робочій станції працює мережева оболонка –

спеціальне програмне забезпечення, що дозволяє обмінюватися інформацією з файловим сервером, іншими робочими станціями та мережевими пристроями. Ця оболонка дозволяє робочим станціям використовувати файли та програми, що зберігаються на сервері, так само легко, як і власні локальні диски.

1.2 Вимоги до системи інформаційної безпеки

Розробка будь-якого проєкту, особливо в сфері кібербезпеки, вимагає чітко сформульованих вимог. Це є ключовим фактором успіху.

Основні категорії вимог до систем інформаційної безпеки включають: 1. Функціональні вимоги до систем захисту інформації.

2. Вимоги до системного обладнання.

3. Вимоги до системного програмного забезпечення.

4. Організаційна підтримка.

5. Вимоги до рівня інформаційної безпеки.

6. Вимоги до фізичного захисту системного обладнання.

7. Економічні вимоги.

8. Вимоги з охорони праці під час експлуатації систем захисту інформації. Детальні вимоги до системного обладнання:

1. Централізоване управління: Обладнання повинно забезпечувати можливість централізованого контролю над ключовими процесами мережі. 2. Якість та відповідність стандартам: Техніка має бути від перевірених виробників (як українських, так і міжнародних) та відповідати таким критеріям: - Ергономічність.

- Низьке енергоспоживання.
- Компактність після встановлення.
- Низьке тепловиділення.
- Низький рівень шуму.
- Простота та швидкість заміни.

3. Надійність: Середній час напрацювання на відмову (*MTBF*) повинен

становити не менше 25 000 годин.

4. Стійкість до перешкод: Захист від зовнішнього електромагнітного випромінювання.

5. Документація: Усе обладнання повинно супроводжуватися інструкціями з експлуатації українською мовою.

6. Відновлення даних: Апаратне забезпечення має підтримувати можливість відновлення інформації у випадку пошкодження основного носія. 7. Гаряча заміна: Критично важливі компоненти повинні підтримувати функцію гарячої заміни (*hot-swap*).

Вимоги до програмного забезпечення систем захисту інформації: Програмне забезпечення є невід'ємною частиною сучасної системи безпеки, і його вимоги варіюються залежно від умов впровадження.

Отже, програмне забезпечення повинно:

1. Контроль доступу: Забезпечувати розмежування прав доступу користувачів до мережевих ресурсів.

2. Віддалене управління: Надавати можливість дистанційного керування користувацькими комп'ютерами.

3. Моніторинг: Здійснювати моніторинг стану комп'ютерів користувачів під час робочого процесу.

4. Виявлення та запобігання вторгненням: Виявляти та блокувати будь-які спроби несанкціонованого втручання в роботу мережі.

5. Антивірусний захист: Забезпечувати захист інформації користувача від шкідливого програмного забезпечення (вірусів, троянських програм). 6. Шифрування: Впроваджувати механізми шифрування для особливо конфіденційної інформації користувачів.

Вимоги до організаційної підтримки:

Організаційні заходи та корпоративна культура відіграють ключову роль у забезпеченні інформаційної безпеки, підкреслюючи важливість етичної відповідальності кожного співробітника за збереження цілісності даних. Ці вимоги включають:

1. Регламентація використання ресурсів: Сформулювати чіткі правила для всіх рівнів користувачів щодо використання мережевих інформаційних ресурсів.
2. Механізми звітності: Розробити процедури звітності для користувачів на всіх рівнях.

3. Правила ідентифікації: Встановити правила вибору персональних ідентифікаційних кодів (паролів) для доступу до мережевих інформаційних ресурсів.

4. Підвищення обізнаності: Інформувати користувачів про відповідальність за недотримання вимог інформаційної безпеки, включаючи правові наслідки.
Вимоги до персоналу (кількість та кваліфікація):

При розробці системи інформаційної безпеки, ключові критерії до персоналу мають бути наступними:

1. Мінімальна кількість нового персоналу: Прагнути до мінімального залучення нових співробітників.

2. Відповідність кваліфікації: Рівень підготовки нових фахівців повинен відповідати виконуваним обов'язкам та бути підтвердженим національними або міжнародними сертифікатами.

3. Автономність: Рівень підготовки працівників має дозволяти їм самостійно переналаштовувати розроблені системи захисту та інтегрувати нові компоненти.
Вимоги до рівня інформаційної безпеки:

Рівень інформаційної безпеки має забезпечувати захист від усіх видів загроз, включаючи:

1. Навмисні дії користувачів.

2. Ненавмисні дії користувачів.

3. Навмисні дії мережевих адміністраторів.

4. Навмисні дії третіх осіб.

5. Катастрофи (наприклад, стихійні лиха, пожежі).

Захист каналів зв'язку потребує окремої уваги, оскільки сучасне середовище передачі даних (наприклад, кабельні з'єднання) часто є відкритим і захищене лише легкодоступними коробами.

Вимоги до фізичного захисту системного обладнання:

Враховуючи потенційні ризики, системне обладнання повинно мати захист від:

1. Викрадення зловмисниками.

2. Пошкодження внаслідок пожежі та неконтрольованого поширення вогню.

3. Механічних пошкоджень.

4. Затоплення.

Економічні вимоги:

Основні економічні вимоги до систем захисту інформації:

1. Економічна доцільність пропонованого обладнання та програмного забезпечення.

2. Наявність декількох варіантів для фінального розгляду проєкту. 3. Оптимальне співвідношення ціна/якість: Обладнання повинно мати низьку вартість, зберігаючи при цьому високі якісні характеристики.

Під час впровадження системи інформаційної безпеки її вплив на існуючі робочі процеси співробітників має бути мінімальним. Це означає, що співробітники не повинні відчувати значного дискомфорту від впровадження нової системи. Такий підхід скоротить час на адаптацію та допоможе виявити потенційних порушників, які, не знаючи про систему, можуть викрити себе під час спроби неправомірного втручання.

Вимоги з охорони праці та техніки безпеки при використанні систем захисту інформації:

Ця вимога підкреслює необхідність повного опису всіх аспектів безпеки запропонованої системи під час її експлуатації. Чіткий опис основних вимог дозволить заздалегідь оцінити всі можливі ризики, які можуть виникнути в процесі використання системи [14].

РОЗДІЛ 2
КОМП'ЮТЕРНА МЕРЕЖА ТА АНАЛІЗ ЇЇ

ВРАЗЛИВОСТЕЙ 2.1 Аналіз комп'ютерних мереж

Під час аналізу комп'ютерної мережі сервісного центру було встановлено, що вона базується на технології *Fast Ethernet,* використовуючи обладнання 3*COM* для передачі даних.

Вся критично важлива інформація зберігається централізовано на одному сервері. Це спрощує процес регулярного резервного копіювання, що є ключовим для відновлення даних. Завдяки системі резервного копіювання інформація на сервері може бути миттєво відновлена у разі пошкодження основного сховища, що запобігає втраті даних.

Централізоване управління файловими серверами дозволяє впроваджувати найсучасніші механізми безпеки для запобігання несанкціонованому доступу. Весь маршрутизаційний трафік комп'ютерної мережі контролюється системним адміністратором.

Особливості та обмеження *Ethernet*

Технологія *Ethernet*, включно з її сучасними імплементаціями (*Fast Ethernet*, *Gigabit Ethernet*, 10 *Gigabit Ethernet*), пропонує пропускну здатність 100 Мбіт/с, 1 Гбіт/с та 10 Гбіт/с відповідно. Проте, основним недоліком *Ethernet* є метод доступу до середовища – *CSMA/CD*. Коли два адаптери одночасно "чують тишу" в мережі та починають передачу, виникає колізія. В такому випадку обидві передачі перериваються, і адаптери повторюють спробу передачі через випадковий проміжок часу.

При великій кількості одночасних передавачів у мережі значно зростає кількість колізій, що призводить до зниження пропускної здатності. У критичних ситуаціях швидкість передачі даних може впасти майже до нуля. Навіть при середньому навантаженні (30-40% від максимальної пропускної здатності), фактична швидкість становить лише 70-80% від номінальної.

Цей недолік значною мірою нівелюється за рахунок використання комутаторів (світчів) замість концентраторів. Комутатор ізолює трафік між портами, що підключені до відправника та отримувача, від інших портів та адаптерів. Важливою перевагою різних версій *Ethernet* є їхня зворотна сумісність, що дозволяє їх взаємозамінне використання в одній мережі.

Операційні системи та обладнання

Усі клієнтські комп'ютери працюють під управлінням *Windows* 10, тоді як сервери використовують *Linux*. Все програмне забезпечення ліцензоване. Використання єдиної операційної системи на робочих станціях спрощує їх налаштування та подальше обслуговування.

Фізичне середовище комп'ютерної мережі, через яке передається інформація, представлене неекранованими витими парами, що використовуються для підключення офісних комп'ютерів.

Топологія мережі

Топологія комп'ютерної мережі сервісного центру відповідає "зірці" (Див. Рисунок 2.1).

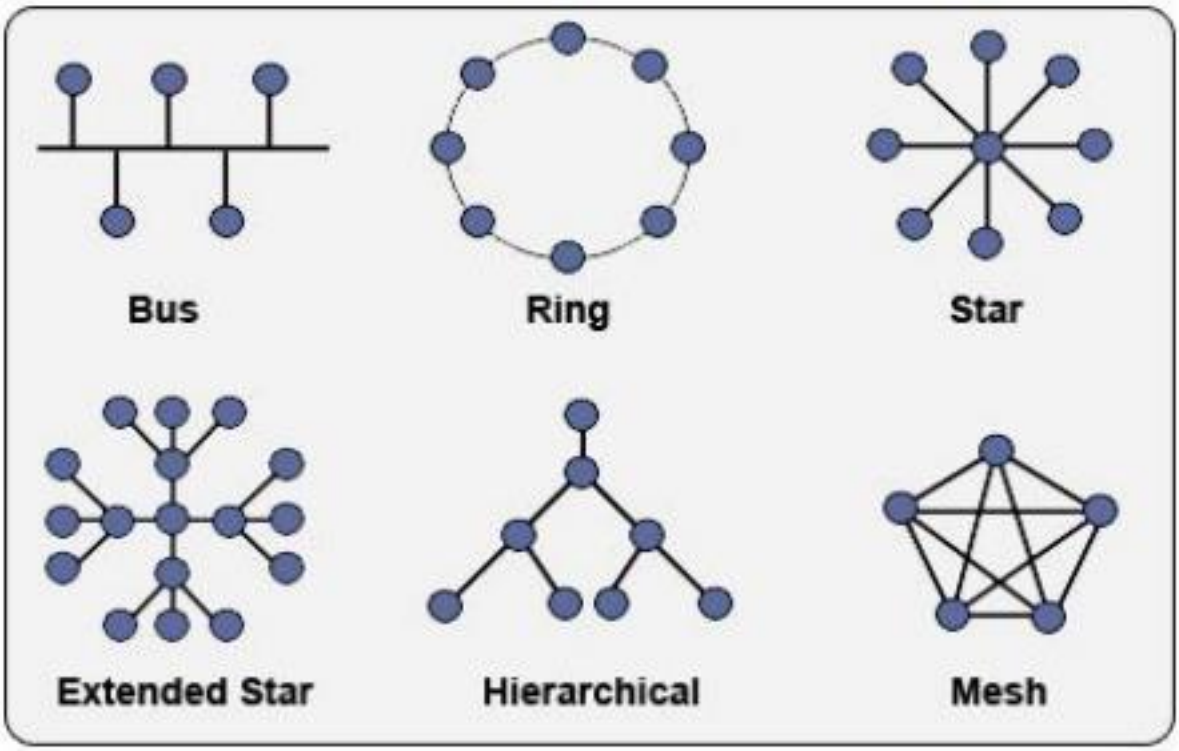

Рисунок 2.1 – Топологія комп’ютерної мережі

Кожна робоча станція та сервер має окреме підключення до центрального комутаційного центру. Це забезпечує незалежну роботу кожного з'єднання: вихід з ладу кабелю, підключеного до однієї робочої станції, не впливає на інші. Така схема спрощує налаштування кабельної системи, оскільки немає потреби враховувати відносне розташування комп'ютерів, доки довжина кабельного сегмента не перевищує максимально допустимого значення.

Переваги зіркової топології:

- Простота виявлення обривів кабелів: Якщо вузол не працює, проблему легко

локалізувати між портом концентратора (комутатора) та фізично підключеним до нього вузлом.

- Чітке визначення несправностей: Основні причини непрацездатності можуть бути пов'язані з терміналом, кабелем або портом комутатора. - Діагностика сервера: Якщо жоден мережевий вузол не отримує якісного з'єднання між сервером та комутатором, проблема може бути на стороні сервера. - Масштабованість: Зіркова топологія добре підходить для фізично розподілених мереж.

- Недоліки зіркової топології:

- Високе споживання кабелю: Кожен мережевий елемент потребує власного кабелю [3].

- Залежність від центрального елемента: Вихід з ладу комутатора паралізує всю мережу.

Для підключення пристроїв використовуються комутатори (Див. Рисунок 2.2).

Рисунок 2.2 – Комутатор. Зовнішній вигляд

Мережі, що базуються на зірковому принципі, вимагають спеціалізованої електроніки. Комутатор є ключовим комутаційним елементом такої мережі. Кожен комутатор зазвичай має від 4 до 24 портів для підключення комп'ютерів або інших комутаторів, при цьому до кожного порту підключається лише один пристрій.

Окрім посилення сигналу, комутатор зазвичай відновлює преамбулу пакетів та усуває перешкоди. Комутатор є ядром системи, що значною мірою визначає її функціонал та можливості. Навіть найпростіші комутатори мають індикатори стану портів, що дозволяє оперативно діагностувати проблеми, спричинені поганим контактом, пошкодженими кабелями тощо. Однією з головних особливостей такої структурованої мережі є її висока відмовостійкість: у випадку переривання зв'язку між двома елементами, інші елементи продовжують функціонувати [3].

Серверна інфраструктура

Основний сервер – *Dell PowerEdge R*720*XD*. Його конфігурація включає: - Два 6-ядерні процесори *XEON E*5-2620 2.0 *GHz*.

- 32 ГБ оперативної пам'яті *DDR*4.

- 12 жорстких дисків *Western Digital Ultrastar DC HC*310 *SAS* об'ємом 12 ТБ кожен.

- Операційна система: *Linux*.

Файловий сервер є серцем локальної мережі. Він хостить операційну систему та контролює потік даних у мережі. Персональні робочі станції та всі спільні периферійні пристрої (наприклад, принтери, сканери) підключені до цього сервера.

Кожна робоча станція – це стандартний персональний комп'ютер з власною операційною системою *Windows* 7, встановленою на диску. На відміну від автономного ПК, робоча станція оснащена мережевою інтерфейсною картою та фізично підключена до сервера за допомогою кабелю. Крім того, на робочій станції працює спеціалізоване програмне забезпечення – мережева оболонка. Вона дозволяє обмінюватися інформацією з файловими серверами, іншими робочими станціями та мережевими пристроями. Завдяки цій оболонці робочі станції можуть використовувати файли та програми, що зберігаються на сервері, так само легко, як і власні локальні диски.

KVM-перемикачі: Апаратні та програмні

KVM-перемикач (*Keyboard, Video, Mouse*) – це пристрій, призначений для

керування кількома комп'ютерами за допомогою одного набору пристроїв введення (клавіатура, монітор, миша).

Спочатку *KVM*-перемикачі забезпечували лише перемикання сигналів монітора, клавіатури та миші. Згодом з'явилися моделі з підтримкою перемикання аудіо та *USB*-пристроїв.

Окрім безпосереднього перемикання сигналів, *KVM*-перемикач повинен імітувати присутність пристроїв на відключеному порту, щоб відключений комп'ютер не генерував помилки, пов'язані з їх опитуванням. Це можливо завдяки підтримці стандартів, таких як *D-sub*, *PS*/2 та протоколів обміну *USB*.

Існують два типи *KVM*-перемикачів: апаратні та програмні. Приклад апаратного *KVM*-перемикача наведено на Рисунку 2.3.

Рисунок 2.3 - *KVM*-перемикач

Програмний *KVM*-перемикач – це програмне забезпечення з клієнт-серверною архітектурою. Воно дозволяє виконувати ті ж функції, що й апаратний *KVM*, а також має додаткові можливості, такі як керування необмеженою кількістю ПК та обмін даними через буфери обміну між різними системами [3].

2.2 Виявлення каналів витоку інформації

У сучасних автоматизованих системах, особливо при зростанні їх складності, зростає ймовірність появи помилок на рівні програмного забезпечення, архітектури, алгоритмів та схемотехніки. Причинами цього можуть бути як технічні, так і людські фактори — рівень кваліфікації персоналу, умови праці, наявність досвіду тощо. Людські помилки залишаються одним із головних джерел потенційних загроз: це можуть бути помилки при введенні інформації, хибна

інтерпретація даних або некоректне виконання дій. Умовно їх поділяють на: - логічні — неправильне прийняття рішень,

- перцептивні — хибне сприйняття інформації,

- моторні — помилки при фізичному виконанні дій.

Частота таких помилок варіюється від 1–2% до 15–40% і більше, залежно від складності завдань та системи.

Крім випадкових, значну загрозу становлять навмисні дії зловмисників. Мотиви можуть бути різними: від матеріальної вигоди або особистого невдоволення до бажання продемонструвати свої навички, як це часто буває при

хакерських атаках. Оскільки дослідження психологічних мотивацій виходить за рамки цієї роботи, аналіз загроз ведеться виключно з технічної точки зору. Для виявлення потенційних каналів витоку важливо розглянути, як саме здійснюється введення, виведення, зберігання та обробка інформації в системі, а також яким чином може бути отримано доступ до об'єктів захисту без авторизації. Типові канали, через які інформація може бути отримана або викрадена: 1. Користувацький термінал;

2. Термінал адміністратора;

3. Термінал оператора системного управління;

4. Пристрої виведення інформації (монітори, дисплеї);

5. Засоби фіксації інформації (принтери, скріншоти, фото);

6. Засоби завантаження ПЗ у систему;

7. Фізичні носії даних (*USB*, диски тощо);

8. Зовнішні канали зв’язку (мережі, інтернет тощо).

Без належного контролю, автентифікації користувачів та обмеження доступу до терміналів, зловмисник може легко скористатися функціоналом системи. Навіть фізичний доступ до обладнання може дозволити візуально спостерігати за даними, копіювати або змінювати файли, знищувати резервні копії чи викрадати носії інформації.

Окрему небезпеку становить неконтрольоване встановлення програмного забезпечення, що може містити шкідливі компоненти: змінювати критичні

алгоритми, красти дані або запускати троянські програми. Такі програми можуть таємно копіювати інформацію на зовнішні пристрої чи передавати її мережею. Мережеве середовище також може бути використане для впровадження вірусів, шпигунських програм тощо. Часто обхід системи відбувається через функціональний термінал, який не має належного рівня захисту.

Критичним ризиком є ситуації, коли внутрішні користувачі, маючи легальний доступ до частини інформації, можуть навмисно чи випадково отримувати доступ до інших, заборонених розділів. Такі користувачі здатні викривлювати, видаляти або поширювати конфіденційні дані, що підриває ефективність будь-яких заходів

програмного захисту, якщо фізичний доступ до обладнання або кабелів не контролюється.

Методи, якими можуть скористатися порушники:

- Використання часу інших користувачів (*time-sharing*);

- Аналіз трафіку або перехоплення даних через ті самі канали зв’язку; - Підбір паролів методом перебору або використання вразливостей ОС; - Підключення до лінії зв’язку між терміналом і процесором комп’ютера без зупинки роботи легального користувача — з подальшою імітацією його дій [13].

2.3 Класифікація сучасних методів та засобів захисту інформації

У сучасних умовах забезпечення інформаційної безпеки передбачає комплексний підхід, що охоплює як технічні рішення, так і програмні, організаційні, правові та етичні заходи. Основні засоби реалізації політики захисту інформації поділяються на наступні групи:

1. Технічні засоби захисту — це фізичні компоненти, що використовуються для запобігання витоку або несанкціонованого доступу до інформації. Вони включають:

- Апаратні рішення — вбудовані в пристрої або підключені до систем обробки даних (СОД) через стандартні інтерфейси, наприклад, модулі перевірки

парності, апаратний контроль доступу до пам’яті, спеціальні захищені регістри;

- Окремі фізичні пристрої та системи безпеки — охоронна сигналізація, електронні замки, пристрої контролю доступу до приміщень та захисту від вторгнень.

2. Програмне забезпечення — це спеціалізовані програми, призначені для виявлення, запобігання та реагування на інциденти інформаційної безпеки. Вони охоплюють:

- антивірусні програми;
- системи виявлення вторгнень (*IDS*/*IPS*);
- засоби шифрування даних та автентифікації користувачів;

- програми для контролю доступу та моніторингу активності.

Експерти з інформаційної безпеки дійшли висновку, що жоден із методів захисту окремо не забезпечує надійного захисту. Ефективна система безпеки повинна поєднувати всі зазначені інструменти в єдиний комплекс. З огляду на це, сформовано структуру основних напрямів захисту інформації у локальних мережах (рис. 2.4):

Рисунок 2.4 – Методи та засоби захисту інформації в локальній мережі

1. Фізичні бар’єри — засоби, що унеможливлюють фізичний доступ до носіїв інформації чи пристроїв, у яких вона зберігається (контроль доступу до серверних кімнат, робочих місць, кабельних трас тощо).

2. Контроль доступу — механізми регулювання прав користувачів щодо доступу до системних ресурсів, даних і функцій. Включає:

- Ідентифікацію та автентифікацію користувачів і пристроїв;
- Авторизацію дій, відповідно до встановлених політик (доступ за розкладом, до певних файлів або функцій);
- Реєстрацію та аудит дій користувачів;
- Реакцію на порушення: блокування, повідомлення, аварійне завершення сесій.

3. Шифрування та анонімізація — забезпечують конфіденційність і цілісність інформації при її передачі каналами зв’язку, захист від перехоплення та *DDoS*-атак. Паролі, цифрові сертифікати, *VPN*, *TLS* — все це приклади таких засобів.

4. Моніторинг та аудит — системи нагляду за станом інформаційної інфраструктури, які дозволяють фіксувати всі події доступу, зміни конфігурацій, спроби втручання та інші інциденти. Це дозволяє своєчасно виявити загрози та забезпечити реагування.

5. Політика примусу — забезпечується нормативними документами, внутрішніми регламентами та законодавством. Передбачає матеріальну, дисциплінарну чи кримінальну відповідальність за порушення правил обробки захищеної інформації.

Захист інформації реалізується через поєднання таких підходів:

- Технічний підхід — фізичні та програмні засоби безпеки;
- Процедурний підхід — регламентовані дії та правила користувачів;
- Організаційно-правовий підхід — нормативна документація, відповідальність персоналу;
- Етичний підхід — формування корпоративної культури безпеки,

підвищення обізнаності та відповідальності працівників.

Серед організаційних заходів варто виділити:

- Створення чіткої структури відповідальності;
- Визначення політик та процедур інформаційної безпеки;
- Навчання персоналу;
- Регламентація проєктування, інсталяції, тестування та експлуатації інформаційних систем.

Законодавчі механізми захисту базуються на нормативно-правовій базі держави: закони, підзаконні акти, стандарти, які регулюють обробку інформації та відповідальність за її розголошення або незаконне використання.

Морально-етичні гарантії спираються на норми професійної етики, що формуються у спільноті фахівців ІТ-сфери. Хоча ці норми не мають юридичної сили, їх порушення може спричинити репутаційні втрати.

Усі розглянуті заходи умовно поділяються на:

1. Формалізовані — ті, що діють автоматично за встановленими алгоритмами без участі людини;
2. Неформальні — базуються на свідомій поведінці осіб, що працюють із системою, та внутрішніх правилах організації.

2.4 Розробка моделі загроз

Щоб ефективно захистити інформаційні ресурси, необхідно розуміти потенційні наслідки їх втрати. Важливим є дотримання балансу між вартістю захисту та цінністю самої інформації. Тому варто впроваджувати підходи для оцінки значущості інформації з урахуванням її бізнес- або операційної цінності[1].

Основні властивості, що визначають цінність інформації в контексті інформаційної безпеки, залишаються незмінними — це конфіденційність, цілісність, доступність та спостережуваність.

- Конфіденційність — гарантія того, що доступ до інформації мають лише

авторизовані користувачі та системи.

- Цілісність — забезпечення захисту інформації від несанкціонованих змін, як на фізичному, так і на логічному рівні.

- Доступність — гарантує можливість легального доступу до інформації в потрібний момент.

- Спостережуваність — здатність контролювати, хто і як обробляє інформацію, з фіксацією відповідних подій[2].

Загроза — це потенційна подія або дія, яка може негативно вплинути на одну або кілька вищезгаданих характеристик інформації. Наприклад, витік радіаційних даних становить загрозу конфіденційності, пожежа — цілісності та доступності, а відмова мережевого обладнання — доступності[3].

Типи загроз:

1. Витоки через побічні (технічні) канали — акустичні, оптичні, радіохвильові, електромагнітні.

2. Використання спеціальних впливів (електромагнітні імпульси, наводки) для порушення функцій захисту.

3. Несанкціонований доступ: підключення сторонніх пристроїв, злам облікових даних, використання шкідливого ПЗ (віруси, трояни), соціальна інженерія тощо[4]. Усі загрози можна поділити на:

- Навмисні — дії зловмисників;

- Ненавмисні — людські помилки, технічні збої [5].

Вони, у свою чергу, реалізуються через відповідні канали впливу або доступу, що потрібно враховувати при побудові моделі загроз.

Категорії інформаційних загроз:

1. Порушення добросовісності — шахрайські дії з боку користувачів або персоналу.

2. Втрати контролю або спостереження — відсутність логування, недосконалий аудит.

3. Порушення конфіденційності — витік через канали, втрата паролів, злам

акаунтів.

4. Втрати доступності — збої систем, *DDoS*-атаки, пошкодження обладнання[6]. Загрози цілісності

Хоч опис загроз цілісності схожий на опис загроз конфіденційності, їхня природа відмінна. Якщо у випадку конфіденційності критично уникати доступу, то у випадку цілісності — уникати зміни даних.

Типова загроза — несанкціоноване редагування даних. Наприклад, троянські програми, які вносять зміни до документів або системних файлів, діючи від імені користувача[7].

Порушити цілісність також можуть:

- помилки персоналу,
- віруси,
- апаратні збої.

Механізми захисту:

1. Регулярне резервне копіювання;

2. Використання кодів контролю цілісності (наприклад, хешів);
3. Верифікація автентичності повідомлень і транзакцій;
4. Резервування систем і каналів передачі даних[8].

Загрози спостережуваності

На відміну від попередніх властивостей, спостережуваність — це позитивна умова, яка забезпечує контроль і прозорість дій у системі. Якщо відсутній контроль над подіями, це може свідчити про потенційні порушення[9].

Ключові інструменти:

- Журналювання — запис усіх дій користувачів і системних подій; -

Аудит — аналітика записаних подій для виявлення порушень. Цілі аудиту:

1. Надання зворотного зв'язку для користувачів та адміністраторів; 2. Можливість відновлення послідовності подій;
3. Виявлення інцидентів інформаційної безпеки;

4. Надання матеріалів для розслідувань[9].

Загрози конфіденційності

Основними причинами витоку інформації є:

1. Втрата контролю над системами захисту;

2. Використання каналів витоку, які не враховані системою безпеки[10]. Якщо система моніторингу або захисту не виявляє несанкціонованого доступу, то ці канали можуть стати «чорними дірами» безпеки. До прикладу, неочевидні способи передавання даних через буфер обміну, службові протоколи або побічні сигнали (наприклад, миготіння індикаторів на маршрутизаторах)[10]. Загрози доступності

Доступність — це можливість легального доступу до ресурсів тоді, коли це потрібно. Вона забезпечується:

- Надійною інфраструктурою;
- Можливістю швидкої заміни обладнання;
- Своєчасним резервним копіюванням;
- Гнучкістю системи до збоїв[11].

Рекомендовані заходи підтримки:

1. Технічна підтримка користувачів;
2. Супровід програмного забезпечення;
3. Контроль змін у конфігурації;
4. Резервне копіювання даних;
5. Фізичний захист носіїв інформації;
6. Документування процедур;
7. Оперативне планування роботи [12].

2.5 Забезпечення безпеки комп’ютерної мережі

У контексті захисту даних у комп’ютерних мережах ключовими ризиками залишаються порушення класифікації доступу та цілісності інформації, що може призвести до її втрати або небажаного редагування. Основні загрози можна класифікувати наступним чином:

1. Відмова апаратного забезпечення:

- Пошкодження або вихід з ладу кабельної інфраструктури;
- Порушення функціонування мережевого обладнання;
- Збій у роботі дискових масивів;
- Несправності у системах резервного копіювання;
- Вихід з ладу серверів, робочих станцій, мережевих адаптерів тощо.

2. Втрата даних через збої в роботі персональних пристроїв:

- Помилки у функціонуванні апаратних компонентів (наприклад, фотоелектричних сенсорів), які можуть призвести до втрати або спотворення інформації;
- Зараження системи шкідливим програмним забезпеченням, яке може пошкодити або знищити дані.

3. Загрози, пов’язані з несанкціонованим доступом:

- Несанкціоноване копіювання, знищення або фальсифікація інформації;

- Розголошення конфіденційних даних стороннім особам, з порушенням принципів інформаційної безпеки.

4. Втрата інформації через неналежне зберігання цифрових документів: - Недотримання правил архівації та зберігання призводить до неможливості відновлення важливих даних.

5. Людський фактор – помилки персоналу та користувачів:

- Випадкове редагування, пошкодження або видалення інформації; - Некоректне використання апаратного чи програмного забезпечення, що може спричинити втрату даних або їх спотворення.
- Для забезпечення надійного захисту даних застосовуються три основні категорії засобів безпеки, відповідно до типів потенційних загроз: - Фізичний захист: включає захист електроживлення, кабельних мереж, дискових сховищ, засобів передачі даних тощо.
- Програмні засоби захисту: антивірусне ПЗ, системи контролю доступу,

засоби шифрування, міжмережеві екрани.

- Адміністративні заходи: впровадження політик безпеки, контроль доступу до систем, інструкції для персоналу, розробка планів реагування на інциденти. Варто зазначити, що такий поділ є умовним, адже сучасні тенденції спрямовані на інтеграцію апаратних і програмних засобів безпеки. Найпоширенішими є рішення, що поєднують контроль доступу, шифрування даних, захист від шкідливих програм і моніторинг мережевої активності. Одним із найефективніших методів запобігання втраті даних під час короткочасних перебоїв електроживлення є використання джерел безперебійного живлення (ДБЖ). Сучасні моделі ДБЖ відрізняються за функціональністю та потужністю — вони можуть підтримувати роботу як окремих пристроїв, так і цілих локальних мереж, надаючи час для завершення критичних операцій або збереження інформації. Крім того, багато моделей виконують функцію стабілізатора напруги, захищаючи обладнання від перепадів в електромережі. Чимало сучасних мережевих пристроїв — таких як сервери, маршрутизатори, комутатори — обладнані системами резервного живлення.

31

У міжнародній практиці поширеним підходом є використання аварійних генераторів або дублюючих ліній живлення, підключених до різних електропідстанцій. Це дозволяє забезпечити безперервне живлення навіть у випадку виходу з ладу одного з джерел живлення [1].

32

РОЗДІЛ 3
РОЗРОБКА СИСТЕМ ЗАХИСТУ

3.1 Методи та засоби несанкціонованого отримання інформації з автоматизованих систем

У сучасному цифровому світі, де персональні комп'ютери широко поширені та взаємодіють через локальні та глобальні мережі, питання інформаційної безпеки набуває особливого значення. Часто цей термін безпосередньо стосується захисту даних, що обробляються в автоматизованих системах (АС) та

циркулюють у комп'ютерних мережах, від несанкціонованого витоку.

Деякі експерти з кібербезпеки виділяють витік інформації через комп'ютерні мережі в окремий канал, відмінний від інших технічних каналів (наприклад, радіо чи акустичних). Однак, на відміну від пасивного витоку через радіо чи акустичні канали (що може бути випадковим шумом, спричиненим недоліками обладнання), витік інформації через комп'ютерну мережу, як правило, є наслідком цілеспрямованих дій зловмисників. Вони використовують недосконалості програмного та апаратного забезпечення АС для доступу до її ресурсів та процесів.

Втім, незалежно від конкретних методів та засобів, які використовує зловмисник для несанкціонованого отримання інформації з АС, кінцевим результатом завжди є генерація електромагнітного поля в певному середовищі, яке зловмисник може перехопити. Це поле, по суті, є копією вихідної інформації, яка з технічної та юридичної точки зору не відрізняється від оригіналу. У випадках, коли зловмисник має фізичний доступ до АС, він може просто викрасти носій інформації (наприклад, жорсткий диск), що призводить до того ж результату. З огляду на постійне зниження вартості сучасного комп'ютерного обладнання, юридичні наслідки крадіжки самого носія можуть бути незначними, на відміну від наслідків крадіжки інформації, що на ньому зберігається.

Підсумовуючи, витік інформації з АС через недосконалість апаратних та програмних рішень можна з певними застереженнями віднести до фізичного

каналу. Однак, більш точно це слід класифікувати як сучасне приховане фізичне проникнення (ПФП), що є не технічним засобом, а агентним методом отримання інформації. Зокрема, зловмисники часто вдаються до так званої соціальної інженерії.

Соціальна інженерія: Використання психології для доступу

Соціальна інженерія — це використання психологічних маніпуляцій для прихованого отримання конфіденційної інформації (наприклад, паролів, імен користувачів, кодів доступу) від власників для доступу до АС. "Сила" таких відомих хакерів, як Кевін Мітник і Роско, полягала не лише в їхній технічній підготовці, але й у майстерному застосуванні методів соціальної інженерії.

Персонал, як і апаратне забезпечення, програмне забезпечення, дані та документація, є невід'ємною частиною будь-якої АС. Однак, детальне вивчення всіх аспектів вилучення інформації за допомогою соціальної інженерії виходить за межі цієї роботи. Тому, зважаючи на актуальність проблеми несанкціонованого доступу до інформації в АС, ми обмежимося коротким описом технічних аспектів проблеми, не торкаючись її гуманітарних складових [11].

Класифікація методів та засобів несанкціонованого доступу

Методи та засоби отримання інформації з АС без дозволу можуть бути класифіковані за різними критеріями: за типом доступу, рівнем доступу, характером дій зловмисника, кількістю доступів, спрямованістю дій та ступенем серйозності (Див. Рисунок 3.1).

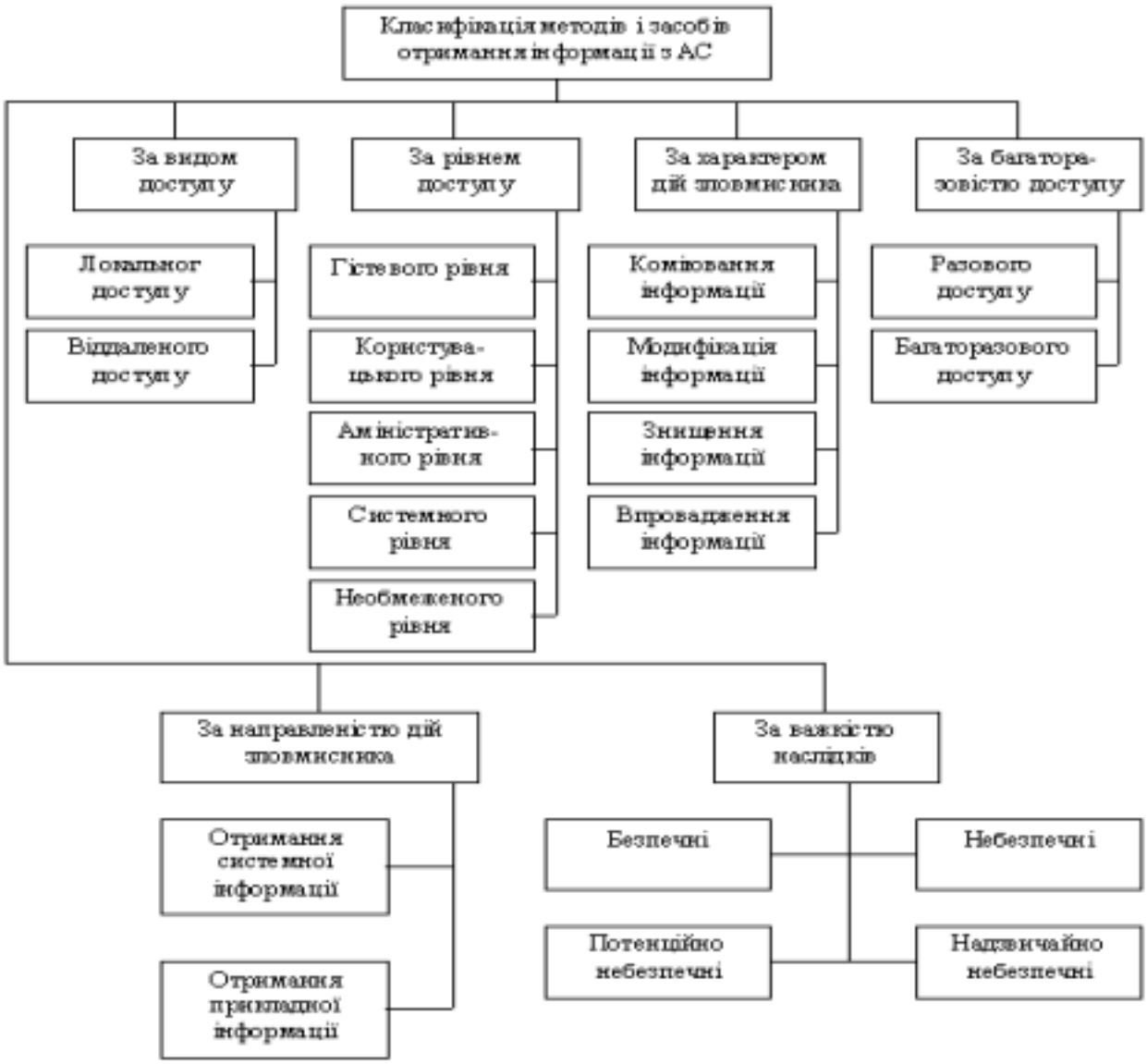

Рисунок 3.1 - Класифікація несанкціонованих методів та засобів

За типом доступу всі методи та інструменти можна розділити на дві основні категорії:

1. Локальний (фізичний) доступ до АС.
2. Віддалений доступ (через комп'ютерну мережу).

Якщо зловмисник має локальний доступ, достатні ресурси та час, захист інформації стає вкрай складним, якщо не неможливим, навіть для найбільш надійних систем. Хоча віддалений доступ можна досить надійно захистити, абсолютна безпека не може бути гарантована для систем, фізично підключених до мережі передачі даних.

Залежно від рівня доступу, несанкціоновані методи та засоби часто поділяються на ті, що використовують права:

- Гостя (наприклад, "*Guest*" у *Windows*).
- Користувача.
- Адміністратора (наприклад, "*Administrator*" у *Windows*, "*root*" у *Unix* системах).
- Системні (наприклад, "*System*" у *Windows*).
- Необмежені (наприклад, "*Enterprise Administrator*" у *Windows*). Багато сучасних операційних систем мають вбудовані облікові записи з певними рівнями доступу, при цьому змінювати дозволи вбудованих облікових записів зазвичай неможливо.

За характером дій зловмисника, методи та засоби можуть бути спрямовані на:

- Копіювання інформації.
- Модифікацію інформації.
- Знищення інформації.
- Впровадження нової інформації.

У випадку впровадження інформації, АС володіє функціями, відмінними від традиційних методів зберігання даних, оскільки вона не лише зберігає дані, але й містить програмне забезпечення для їх обробки та обміну. Ця функція активно використовується зловмисниками. Часто їхньою метою при отриманні доступу до

певної АС є не стільки несанкціоноване отримання вже наявної інформації, скільки впровадження шкідливого програмного забезпечення (наприклад, бекдорів) або збереження власної конфіденційної інформації без відома власника системи.

Кількість доступів та їх наслідки

Залежно від кількості доступів, існують методи та засоби для отримання: - Одноразового несанкціонованого доступу.

- Багаторазового несанкціонованого доступу.

У першому випадку запобігти несанкціонованим діям складніше, але виявити їх легше, оскільки зловмисники не дбають про приховування факту проникнення. У другому випадку запобігання спрощується, але виявлення ускладнюється,

оскільки головною проблемою зловмисника, що планує багаторазове проникнення, є приховування всіх слідів такого проникнення.

Спрямованість дій зловмисника

За спрямованістю методів та засобів, що використовуються зловмисниками для несанкціонованого отримання інформації з ПК, їх поділяють на ті, що спрямовані на:

- Отримання системної інформації (файли паролів, ключі шифрування, списки облікових записів, мережеві адресні плани тощо).

- Фактичне отримання прикладної інформації.

Багато зловмисників, які компрометують системи контролю доступу, підключені до глобальної мережі, не зацікавлені в прикладній інформації, що зберігається на цих системах. Їх цікавить лише обсяг системної інформації, до якої вони отримують доступ. Зазвичай такі зловмисники використовують скомпрометовані АС як проміжні вузли для проникнення в інші АС або для несанкціонованого зберігання власної інформації.

Ступінь серйозності наслідків

Залежно від тяжкості наслідків, спричинених методами та засобами, що використовуються зловмисниками для несанкціонованого отримання інформації, їх можна розділити на:

- Ризики безпеки (наприклад, сканування портів, спроби підключення). - Потенційні ризики (доступ до вмісту підсистеми зберігання даних, спроби підбору паролів).

- Небезпечні ризики (отримання високих привілеїв доступу, модифікація інформації в АС, копіювання системної та прикладної інформації, встановлення власного програмного забезпечення).

- Надзвичайно небезпечні ризики (знищення інформації, блокування доступу легітимних користувачів до АС).

Локальний доступ та його вразливості

Як зазначалося раніше, якщо зловмисник має локальний доступ до АС і сприятливі умови, він може обійти практично будь-який захист. Для суттєвого

зменшення можливості отримання локального доступу до цільової АС необхідно вжити низку технічних та організаційних заходів: від проектування архітектури АС з урахуванням усіх вимог безпеки до встановлення систем відеоспостереження, сигналізації та контролю доступу.

Проте, на практиці, більшість організацій, які обробляють конфіденційну інформацію, часто ігнорують хоча б один фактор, що може стати ціллю для зловмисників. Досвід показує, що якщо організації не вживають усіх можливих заходів для захисту від несанкціонованого локального доступу до своїх АС та їх компонентів, їхні секрети рано чи пізно стануть надбанням зацікавлених сторін.

Розглянемо детальніше методи та інструменти, які можуть бути використані локально для несанкціонованого доступу до інформації.

По-перше, зловмисники можуть вдатися до одного з найдавніших методів, від якого жодна система не може бути повністю захищена — крадіжки. Крадіжка інформації, її носіїв, окремих компонентів АС, а в сучасних умовах мініатюризації — і всієї АС, була і залишається одним із найпоширеніших способів несанкціонованого отримання інформації. При цьому кваліфікація злодіїв може бути мінімальною. Правоохоронні органи та постраждалі організації часто зосереджуються на матеріальних збитках.

Крадіжка може полягати не лише у фізичному вилученні, а й у заміні

компонента АС на аналогічний. Наприклад, кваліфікований фахівець під певним приводом проникає в офіс, швидко вивчає модель жорсткого диска, пропонуючи "допомогу" недосвідченому співробітнику. Потім зловмисник знаходить несправний жорсткий диск аналогічної моделі, проникає в офіс і замінює цільовий диск на несправний. Такий інцидент не викликав би підозр, якби організація не вела суворий облік серійних номерів компонентів АС (що, на жаль, часто ігнорується), а зловмисник зміг приховати факт проникнення до приміщення (що не є великою проблемою для досвідченого хакера).

Крім того, у багатьох випадках крадіжка може включати копіювання всього жорсткого диска безпосередньо на інший носій. Навіть якщо оригінальний диск захищений (наприклад, шифруванням), зловмисник може встановити інший,

більший жорсткий диск, скопіювати весь вміст оригінального диска на свій носій, а потім передати його фахівцю вищого рівня для подальшої обробки. У таких випадках доступ до скопійованої інформації стає лише питанням часу.

Важливо зазначити, що крадіжка інформації часто маскується під крадіжку майна. Наприклад, зловмисник може викрасти все офісне обладнання, хоча насправді його цікавить лише вміст жорстких дисків комп'ютера керівника. Часто керівники організації просять підлеглих контролювати запити, що не охоплюють усіх правил захисту даних, дозволяючи доступ до будь-яких файлів на основі цих запитів. Наприклад, більшість керівників не усвідомлюють, що всі файли, які вони відкривають зІнтернету, у *Microsoft Word* та інших офісних програмах, копіюються до папки *Windows Temp* на їхньому локальному диску.

Використання відкритих сеансів та підбір паролів

Другий поширений метод несанкціонованого отримання інформації через локальний доступ – це використання відкритого сеансу легітимного користувача. Можливості зловмисника тут залежать від тривалості доступу до АС, прав легітимного користувача та відсутності контролю з боку користувача або його колег. Особлива небезпека такого підходу полягає в тому, що для експерта з кібербезпеки використання зловмисником відкритого сеансу легітимного користувача, швидше за все, не викличе підозр (особливо якщо "свої" користувачі, займаючи керівні посади, викликають менше занепокоєння у адміністраторів

безпеки). Часто самі користувачі мимоволі сприяють несанкціонованому доступу, розміщуючи паролі у доступних місцях на робочому місці (наприклад, на моніторі або клавіатурі). У таких випадках "захищена" система нічим не відрізняється від тієї, де легітимні сеанси користувачів залишаються відкритими.

Схожий підхід полягає у підборі легітимного пароля. Наприклад, організація може мати сувору політику паролів, де після кількох невдалих спроб обліковий запис блокується, що унеможливлює випадковий підбір пароля. У цьому випадку всі користувачі, залишаючи робоче місце, повинні тимчасово блокувати свої системи. Однак деякі користувачі можуть встановлювати улюблену заставку, що дозволяє обійти основну операційну систему та пароль. Виявляється, що такі

користувачі часто вибирають прості послідовності паролів, наприклад "1111", або свої імена, що значно спрощує завдання підбору легітимного пароля користувача. Зазвичай, для отримання пароля легітимного користувача, зловмисник відкриває сеанс під іменем цього або іншого користувача, а потім копіює системні файли. Зокрема, в системах *Windows*, зловмисники можуть скопіювати файли з розширенням *.PWL* з основної папки *Windows*, а потім використовувати будь-який метод для відкриття цих файлів.

Нарешті, зловмиснику з локальним доступом до АС часто не потрібні навіть помірні навички для несанкціонованого доступу до інформації. У багатьох випадках достатньо простих операцій, таких як завантаження операційної системи в режимі очікування. Такі системи можуть завантажуватися з дискет або компакт дисків. Особливим різновидом цього методу є маніпуляція функцією автозапуску в *Windows*. Використовуючи цю вразливість, зловмисник може запустити потрібну програму навіть у системі *Windows* 10, захищеній екраном запуску з паролем. Наприклад, за допомогою простого пакетного файлу, зловмисник може перезавантажити комп'ютер з *Windows* за кілька хвилин та отримати список усіх файлів, що зберігаються на диску, а також файлів *PWL* та *SAM* [17].

3.2 Актуальні етапи побудови сучасної системи захисту інформації

Після визначення необхідності впровадження системи захисту інформації,

доцільно дотримуватись поетапного підходу, що охоплює як технічні, так і організаційні заходи.

1. Вибір та впровадження технічних засобів інформаційної безпеки: - Обрати серверну платформу з можливістю масштабування та резервування даних (наприклад, створення *RAID*-масивів для забезпечення відмовостійкості); - Розгорнути інтегровану систему пожежної сигналізації з автоматичним оповіщенням;

- Реалізувати системи охоронної сигналізації, відеоспостереження та контролю доступу (СКУД);

- Визначити та впровадити заходи щодо заземлення серверного обладнання відповідно до нормативних вимог.

2. Підбір програмних засобів захисту:

- Здійснити порівняльний аналіз та вибір сучасного антивірусного ПЗ з поведінковим аналізом та захистом від *zero-day* загроз;

- Обрати ефективні засоби міжмережевого екранування (брандмауери), зокрема ті, що підтримують *DPI* (глибокий аналіз пакетів);

- Впровадити системи віддаленого моніторингу, управління інфраструктурою та *SIEM*-рішення (системи управління подіями інформаційної безпеки);

- Визначити програмні засоби шифрування для захисту критично важливої інформації як у стані спокою, так і під час передачі.

3. Організаційно-правові заходи інформаційної безпеки:

- Визначити політику створення, зберігання та оновлення паролів, включно з використанням двофакторної автентифікації;

- Розробити модель розмежування прав доступу відповідно до принципу найменших привілеїв (*least privilege*);

- Ознайомити персонал із чинними національними та міжнародними стандартами безпеки інформації (*ISO*/*IEC* 27001, *GDPR* тощо) [6].

3.3 Вибір та класифікація систем брандмауерного захисту

Брандмауер — це апаратно-програмний засіб, який регламентує трафік між різними сегментами мережі відповідно до заданих політик безпеки. Його завдання — дозволяти, блокувати, шифрувати або переспрямовувати трафік на основі встановлених правил, часто із застосуванням проксі-серверів або засобів глибокого аналізу.

Типи реалізації:

Брандмауери можуть існувати у вигляді:

- окремих фізичних пристроїв (апаратні фаєрволи),

- програмного забезпечення (наприклад, в ОС або на кінцевих пристроях), - спеціалізованих проксі-рішень (рівня застосунків).

Класифікація за типом контролю з'єднань:

- Статичні (*packet-filtering*) — виконують базову фільтрацію трафіку на основі *IP*-адрес, портів та протоколів без збереження стану з’єднань; - Станові (*stateful inspection*) — здійснюють аналіз активних з’єднань та приймають рішення на основі контексту, підвищуючи ефективність захисту від атак типу *DoS* або порушення протоколів.

Класифікація за рівнями взаємодії:

- Брандмауери мережевого рівня. Використовуються для фільтрації пакетів згідно з *IP*-адресами й *TCP*/*UDP* портами. Перевага — швидкість обробки; недолік — відсутність інтелектуального аналізу трафіку та звітності про події.

- Брандмауери рівня застосунків (*Application Layer Firewall* / *Proxy*). Аналізують вміст переданих даних та контролюють трафік для конкретних застосунків (*HTTP, FTP, SMTP* тощо). Забезпечують високу безпеку, але можуть знижувати продуктивність. Вимагають потужного обладнання для ефективної роботи.

- Брандмауери канального рівня. Схожі на проксі-рівень, однак підтримують ширший набір протоколів без необхідності спеціального програмного забезпечення для кожного з них. Є універсальнішими та продуктивнішими в

умовах змішаного трафіку [6].

3.4 Вибір антивірусного програмного забезпечення

Для ефективної протидії вірусам необхідно розуміти їхню природу. Комп'ютерний вірус – це шкідлива програма, створена для саморозмноження та поширення в комп'ютерному середовищі. Потрапивши на ваш комп'ютер через програму чи файл, вірус може з часом інфікувати інші файли та програми. Якщо комп'ютер підключено до локальної чи глобальної мережі, вірус може поширитися на інші пристрої. Хоча творці вірусів керуються різними мотивами, наслідки їхніх

дій, як правило, схожі: пошкодження програм та документів, що часто призводить до їх втрати, а в деяких випадках – до повного знищення інформації на жорстких дисках.

Стратегії захисту від вірусів

Для захисту від вірусних загроз можна застосовувати такі підходи: - Універсальний захист даних: Забезпечує страховку від пошкодження фізичних дисків, збоїв програм або помилок користувача.

- Профілактичні заходи: Знижують ймовірність зараження.

- Спеціалізоване антивірусне програмне забезпечення.

Універсальні засоби захисту даних не обмежуються лише антивірусним захистом і поділяються на два основні типи:

- Резервне копіювання інформації: Створення копій файлів та системних областей диска.

- Обмеження доступу: Запобігання несанкціонованому використанню інформації, особливо вірусами, які можуть змінювати програми та дані, викликаючи збої та помилки.

Три лінії захисту та методи реалізації

Захист від комп'ютерних вірусів базується на трьох основних лініях

оборони: - Профілактика зараження вірусами.

- Блокування вірусної атаки, якщо вірус вже проник на ПК.

- Запобігання руйнівним наслідкам, якщо атака все ж таки відбулася.

Ці три лінії захисту реалізуються за допомогою трьох типів методів: -

Програмні методи захисту.

- Апаратні методи захисту.

- Організаційні методи захисту.

Захист від вірусів: Резервне копіювання та антивірусне ПЗ

Резервне копіювання є основним засобом захисту цінних даних. У випадку втрати інформації з будь-якої причини, диск може бути переформатований і підготовлений до повторного використання. Необхідне програмне забезпечення встановлюється на "чистий", відформатований диск з дистрибутивних носіїв.

Повне відновлення комп'ютера здійснюється шляхом відновлення даних з резервного носія.

При резервному копіюванні важливо пам'ятати, що всі логіни та паролі для доступу до онлайн-сервісів необхідно зберігати окремо, не на самому комп'ютері. Зазвичай вони зберігаються в журналі технічного обслуговування, бажано в сейфі керівника підрозділу.

При розробці плану резервного копіювання необхідно передбачити зберігання резервних копій окремо від ПК. Зберігання інформації на окремому жорсткому диску в тому ж комп'ютері створює лише ілюзію безпеки. Відносно новим і надійним способом зберігання цінних, але неконфіденційних даних є використання мережевих папок на віддаленому сервері в Інтернеті. Деякі сервіси пропонують безкоштовне місце (до кількох МБ) для зберігання даних користувачів.

Резервні копії конфіденційних даних слід зберігати на зовнішніх носіях у сейфі, бажано в окремому приміщенні. Розробляючи план резервного копіювання для організації, рекомендується створювати щонайменше дві резервні копії, що зберігаються в різних місцях, і чергувати їх. Наприклад, щодня протягом тижня копіювати дані на набір резервних носіїв *A*, а потім наступного тижня – на набір *B*

тощо.

Допоміжними засобами захисту інформації є антивірусні програми та апаратний захист. Наприклад, просте замикання перемички на материнській платі може запобігти стиранню перепрограмованого ПЗП (флеш-*BIOS*) від будь-яких зовнішніх втручань, будь то вірус, зловмисник чи необережний користувач.

Типи антивірусних програм та їхні функції

Існує безліч антивірусних програм з різним функціоналом:

1. Створення образів жорсткого диска: Запис образу жорсткого диска на зовнішній носій (наприклад, флешку). У випадку проблем з даними в системній області жорсткого диска, збережений "образ диска" дозволяє відновити більшість, якщо не всі, дані. Цей інструмент також запобігає втраті даних у разі збою обладнання та некоректного форматування жорсткого диска.

2. Регулярна перевірка на віруси: Автоматичне сканування запускається при кожному ввімкненні комп'ютера та підключенні зовнішніх дисків. Важливо пам'ятати, що антивірусні програми виявляють віруси шляхом порівняння їхнього коду з базою даних відомих вірусних сигнатур. Якщо база даних застаріла, а вірус новий, сканери не зможуть його виявити. Тому регулярне оновлення антивірусного програмного забезпечення є критично важливим для надійного захисту. Ідеальна частота оновлень – кожні два тижні; раз на три місяці – прийнятно.

3. Контроль змін властивостей файлів: Деякі комп'ютерні віруси змінюють розмір та інші властивості заражених файлів під час реплікації. Програми моніторингу можуть виявляти таку активність і попереджати користувача.

4. Контроль доступу до жорстких дисків: Оскільки найнебезпечнішою поведінкою, пов'язаною з комп'ютерними вірусами, є зміна даних на жорсткому диску, антивірусні програми можуть контролювати доступ до нього та попереджати користувачів про підозрілу активність.

Хоча загальні заходи інформаційної безпеки важливі, їх недостатньо для повного захисту від вірусів. Необхідно використовувати спеціальні антивірусні програми, які можна класифікувати на кілька типів:

- Детектори: Виявляють файли, заражені відомими вірусами.

- Лікарі (бактеріофаги): Здатні "лікувати" заражені файли, відновлюючи програму до стану до зараження.

- Аудитори: Програми, що контролюють зміни у файлах та системних областях диска.

- Лікарі-аудити: Гібриди аудиторів та лікарів, здатні не лише виявляти зміни, а й автоматично їх відкочувати.

- Фільтри: Резидентні програми, що блокують спроби вірусу реплікуватися та завдавати шкоди, сповіщаючи користувача.

- Вакцини (програми імунізації): Модифікують програми та диски таким чином, щоб вірус "думав", що вони вже заражені. Проте, цей метод виявився вкрай неефективним і більше не застосовується.

Програми-аудитори на кожному етапі роботи зберігають інформацію про стан програм та системних областей диска (завантажувальний сектор та таблиця розділів жорсткого диска), припускаючи, що вони наразі не інфіковані. Згодом, за допомогою програми аудиту, стан цих областей можна порівнювати з початковим, і у випадку виявлення невідповідностей користувач буде повідомлений [11]. Огляд популярного антивірусного програмного забезпечення *ESET NOD*32

Антивірус *ESET NOD*32 (Див. Рисунок 3.2) — це високоефективне та швидке антивірусне рішення, що мінімізує навантаження на систему та забезпечує захист від усіх видів вірусів та шпигунського програмного забезпечення. *ESET NOD*32 інтегрує всі функції сучасної комп'ютерної безпеки, а за деякими параметрами перевершує більшість популярних антивірусних продуктів.

Рисунок 3.2 – Два продукти *Eset*

Зокрема, *ESET NOD*32 має потужний евристичний аналізатор, що дозволяє виявляти невідомі віруси. *ESET*, заснована у 1992 році, є міжнародним розробником програмного забезпечення в галузі комп'ютерної безпеки та визнається одним із лідерів сучасної антивірусної індустрії. Компанія має розгалужену партнерську мережу у 80 країнах та регіональні офіси у 12 країнах. Штаб-квартира *ESET* розташована в Сан-Дієго, Каліфорнія, США.

Флагманським продуктом *ESET* є антивірусна система *ESET NOD*32. Протягом багатьох років *ESET NOD*32 здобув рекордну кількість нагород за свою надійність: за останні 9 років *ESET NOD*32 не пропустив жодного відомого вірусу в тестах *VB*. За даними австрійської тестової лабораторії *AV-Comparatives, ESET NOD*32 *Antivirus* був визнаний найкращим продуктом 2006 року. *ESET NOD*32 захищає інформацію та дані від шкідливого програмного забезпечення в Інтернеті та електронній пошті, а також від відомих та нових загроз. Він забезпечує надійний захист від вірусів, троянських програм, черв'яків, шпигунського та рекламного ПЗ, а також фішингових атак.

Технологія *ThreatSense* використовує складну, але збалансовану систему розширеної евристики та аналізу сигнатур для виявлення невідомих загроз, забезпечуючи високий рівень виявлення без уповільнення роботи системи.

*ESET NOD*32 має модульну структуру, що забезпечує гнучке управління антивірусними рішеннями. До складу рішення входять резидентні модулі, одним з найважливіших є Антивірусний монітор (*AMON*). Він завжди має бути активним, використовувати найновіші версії вірусних баз та сигнатур, та відстежувати всі потенційно небезпечні операції на комп'ютері.

Продукти *ESET* для робочих станцій:

- *ESET Internet Security*: Комплексне програмне забезпечення для захисту комп'ютера від усіх видів електронних загроз. Поєднує антивірусні, антишпигунські модулі, персональний брандмауер та антиспам. Кожен модуль *ESET Internet Security* налаштований на взаємодію з іншими частинами програми, що забезпечує повний захист комп'ютера та ефективне використання системних ресурсів. Усі функції управляються через єдиний графічний інтерфейс, що спрощує

налаштування та використання. *ESET Internet Security* запобігає проникненню, виявляє та видаляє шкідливе програмне забезпечення (рекламне ПЗ, руткіти, шпигунські програми, трояни, віруси, черв'яки та інші загрози), з якими користувачі можуть зіткнутися.

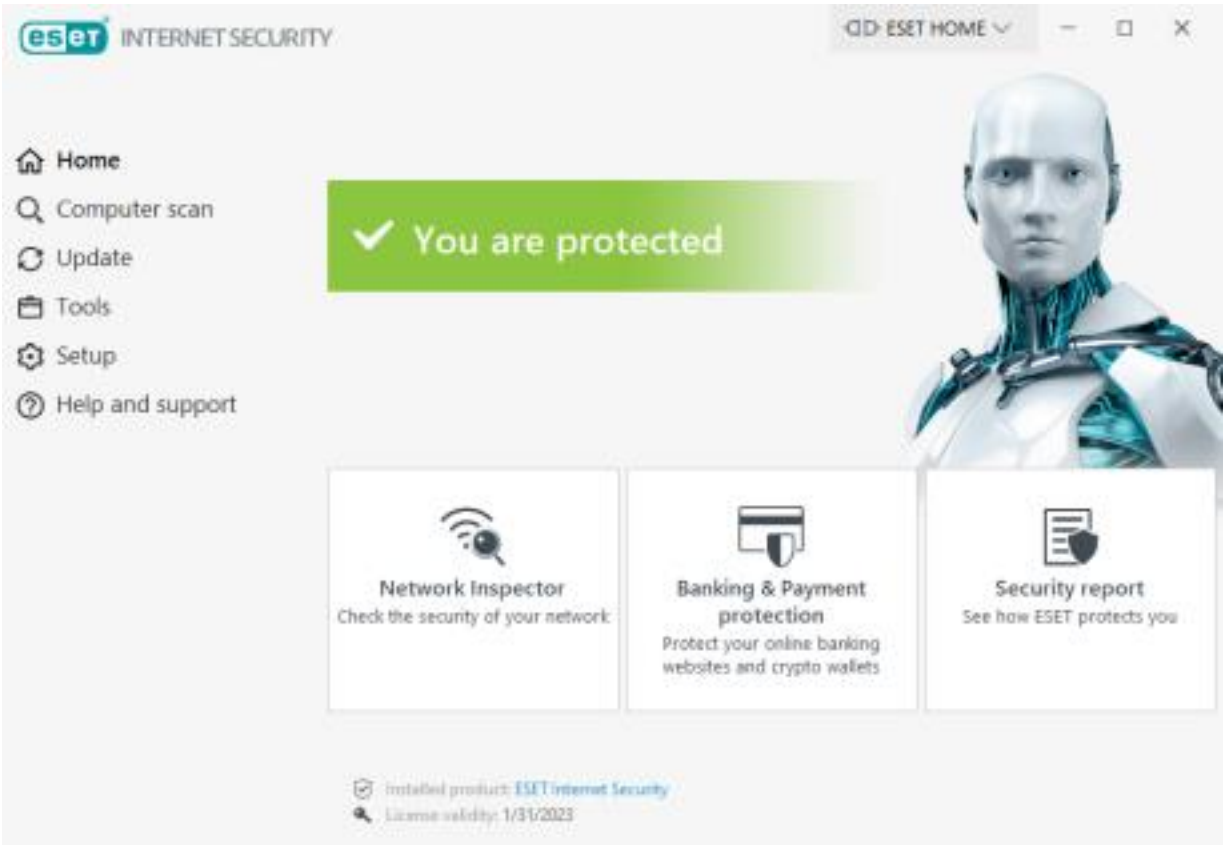

Рисунок 3.3 – Головне вікно *Eset Internet Security*

ESET Internet Security базується на відзначеному нагородами евристичному механізмі аналізу *ThreatSense* та підтримує антивірусний механізм *ESET NOD*32, забезпечуючи надійний захист від найпоширеніших загроз.

Основні переваги *ESET Internet Security*:

- Блокує понад 70% нових онлайн-загроз.

- Захист електронної пошти: Новий блокувальник спаму, шахрайства та інших небажаних листів.

- Запобігає проникненню, виявляє та знищує всі типи шпигунського програмного забезпечення.

- Повна безпека: Двосторонній брандмауер захищає комп'ютер від вхідних та вихідних з'єднань.

- Оптимізація використання комп'ютера: Знижує навантаження на пам'ять та системні ресурси.

Системні вимоги:

- Процесор: 32-розрядний (*x*86) та 64-розрядний (*x*64) *Intel*®, *AMD*®. -

Операційна система: *Microsoft Windows*® 11, 10, 8.1, 8, 7.

- *NOD*32 *Administrator*: Призначений для захисту робочих станцій *Windows*, підключених до локальної мережі.

- *NOD*32 *Standard Edition*: Одне з найкращих рішень для захисту особистої інформації на домашньому комп'ютері.

Avast

Avast – це безкоштовна антивірусна програма, що вимагає безкоштовної реєстрації протягом 30 днів після першого запуску (виконується безпосередньо в програмі). Окрім безкоштовної, доступна також більш повна платна версія.

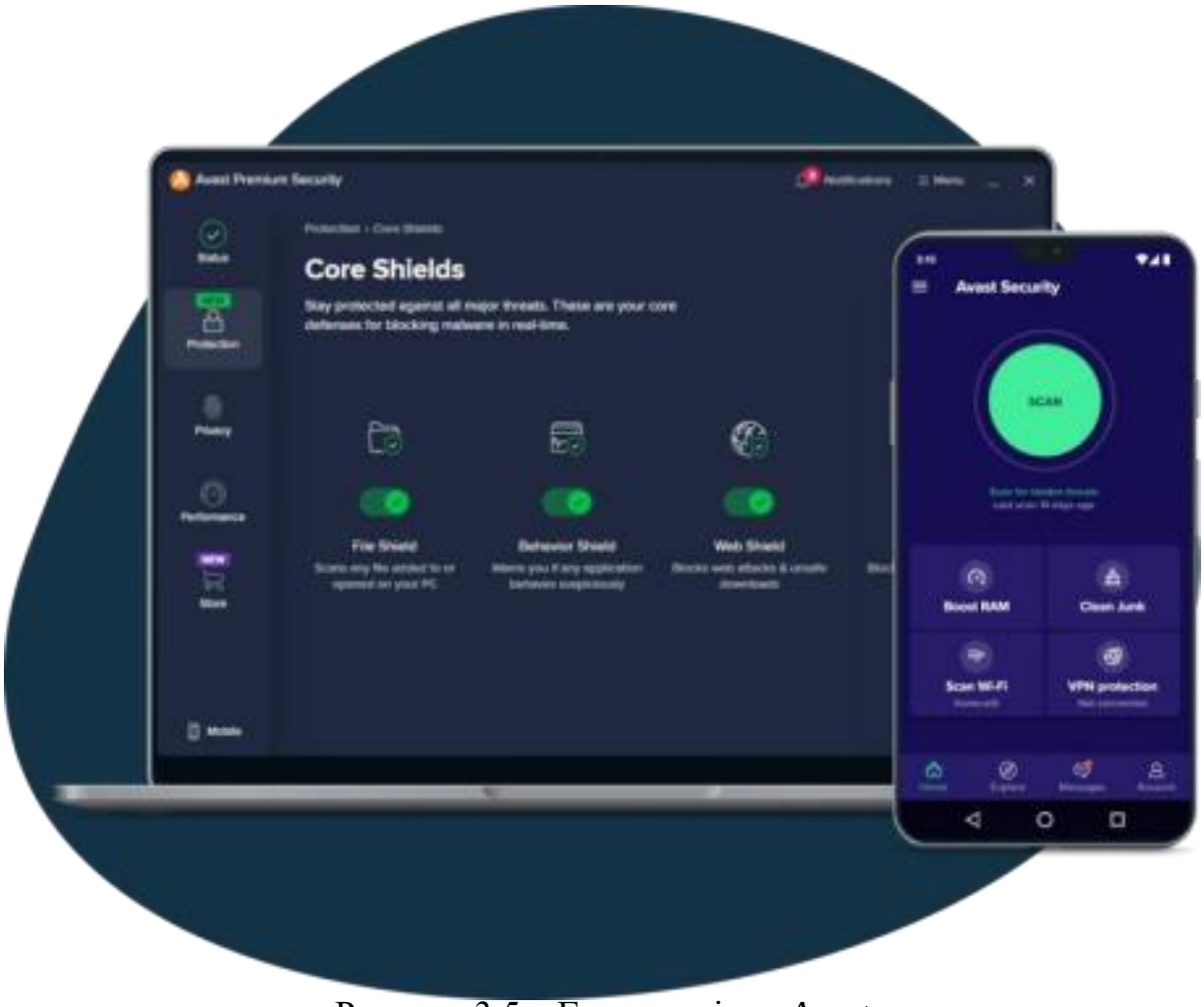

Рисунок 3.5 – Головне вікно *Avast*

Основні характеристики *Avast*:

- Розширене виявлення вірусів, троянських програм, черв'яків, мережевих руткітів та шпигунського програмного забезпечення.

- Евристичний аналіз: Здатність виявляти шкідливе програмне забезпечення, що не виявляється традиційними сигнатурними методами.

- Перевірка електронної пошти (вхідної та вихідної), *P*2*P*-з'єднань та веб трафіку.

- Глибока інтеграція в систему.

- Ігровий режим: Автоматично виявляє програми, що працюють у повноекранному режимі, та вимикає спливаючі сповіщення.

- Невеликі автоматичні або заплановані оновлення вірусних баз даних. Можливість "ручного" оновлення.

Захисник *Windows*

Захисник *Windows* (*Microsoft Windows Defender*) (Див. Рисунок 3.6) – це безкоштовне, повнофункціональне антивірусне та антишпигунське програмне забезпечення від *Microsoft*, що забезпечує захист комп'ютера від онлайн-загроз у режимі реального часу.

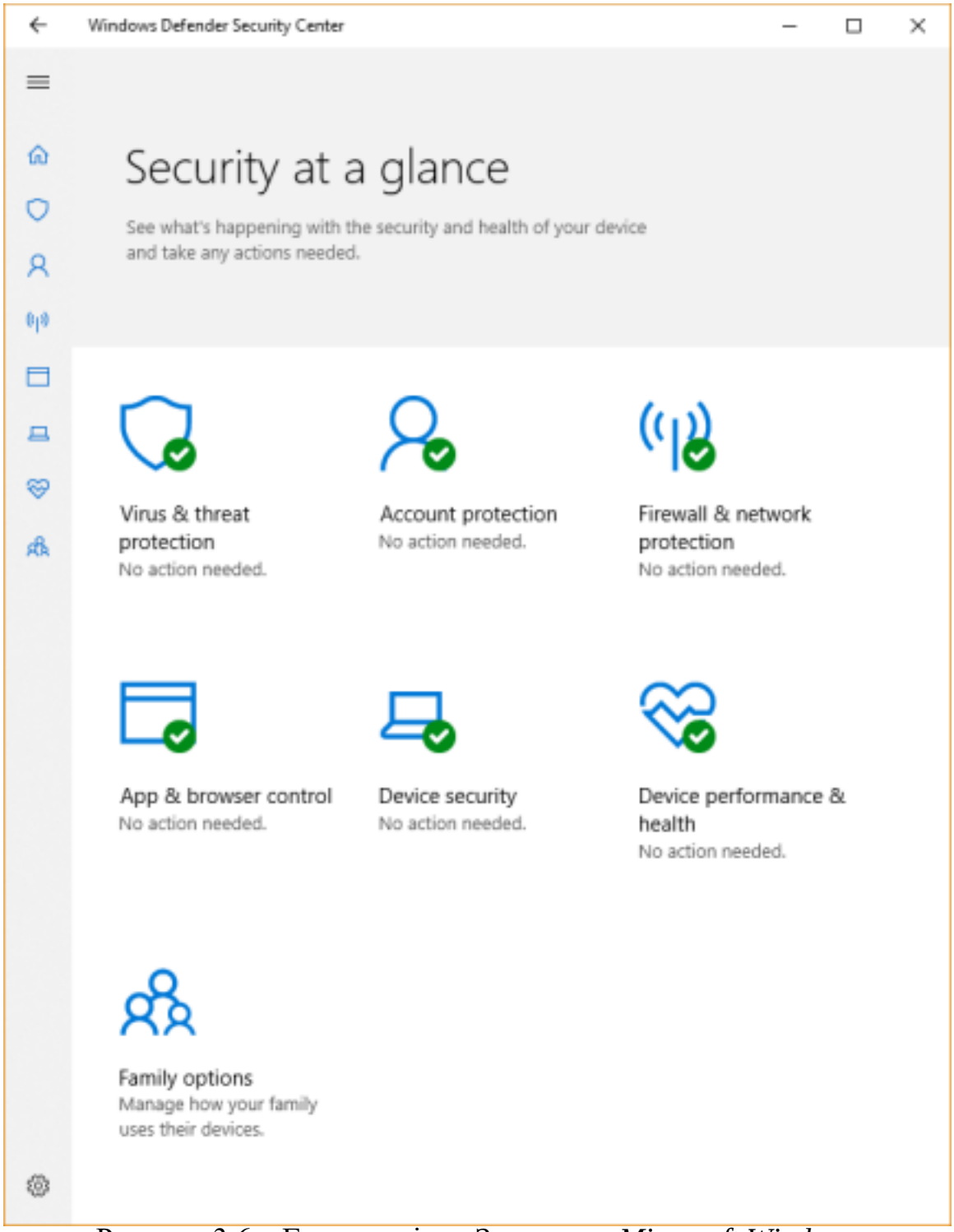

Рисунок 3.6 – Головне вікно Захисника *Microsoft Windows*

Він має дуже простий інтерфейс, що робить його легким у використанні навіть для новачків. Це безкоштовний антивірусний пакет від *Microsoft*, розроблений для захисту від вірусів, шпигунського ПЗ, руткітів та троянських коней, і доступний лише на комп'ютерах під управлінням *Windows*.

Захисник *Windows* замінює попередні антивірусні рішення *Microsoft*, такі як

Microsoft Security Essentials та *Windows Live OneCare*. Хоча *Windows Live OneCare* не займав високих позицій у рейтингах, Захисник *Windows* показав значні покращення.

Антивірус *Microsoft* локалізовано в Україні та доступний для українських користувачів. Некомерційні користувачі ліцензійних версій операційної системи *Windows* можуть завантажити його безкоштовно.

Захисник *Windows* забезпечує захист у режимі реального часу від вірусів, шпигунського ПЗ та інших шкідливих програм. Згідно з незалежними тестами, це одне з найкращих антивірусних рішень для приватних користувачів: *AV Comparatives.org* присвоїв Захиснику *Windows* найвищий рейтинг "*Advanced+*" у своїх тестах продуктивності та виявлення загроз у листопаді та грудні 2019 року.

З моменту свого глобального випуску у вересні 2009 року (під назвою *Microsoft Security Essentials*), Захисник *Windows* отримав позитивні відгуки від багатьох користувачів та експертів. Незалежні дослідження підтверджують, що він забезпечує надійний захист від вірусів та атак для персональних комп'ютерів, а в деяких випадках навіть ефективніший за платні продукти.

У грудні 2009 року безкоштовний *Microsoft Security Essentials* та комерційний продукт *Microsoft Forefront Client Security* взяли участь у порівняльному тестуванні антивірусних програм для *Windows* 7 від авторитетного журналу *Virus Bulletin*. Обидва антивірусні рішення виявили 100% вірусів у глобальній вірусній базі даних,
що використовувалася в тесті.

Захисник *Windows* захищає ПК від усіх відомих загроз, працюючи в режимі реального часу у фоновому режимі, не уповільнюючи роботу системи та не відволікаючи користувача. Інформація про нові віруси та шкідливі програми автоматично завантажується до бази даних Захисника *Windows*, забезпечуючи актуальність захисту [13].

3.5 Програмне забезпечення для шифрування повідомлень

У сучасному світі, де конфіденційність інформації стає дедалі важливішою, використання програмного забезпечення для шифрування є обов'язковим.

Розглянемо найпопулярніші рішення.

Декарт *Secret Keeper* (раніше *Private Descartes*)

Ця програма є надійним інструментом для захисту даних. Вона створює зашифровані файли (один або декілька) на диску, використовуючи алгоритм *AES* з 256-бітним шифруванням, для безпечного зберігання конфіденційної інформації.

Декарт *Secret Keeper* дозволяє шифрувати файли будь-якого типу, включаючи документи *Microsoft Word, Excel* та *PowerPoint*. Це запобігає несанкціонованому перегляду та модифікації інформації, забезпечуючи її цілісність та конфіденційність.

GoSecureSoftware Ltd. *SecureDisk*

SecureDisk від *GoSecureSoftware Ltd*. – це потужний продукт для шифрування нового покоління, що забезпечує 100% захист жорсткого диска, включаючи операційну систему, завдяки автентифікації перед завантаженням. ТОВ "ТЕХНОЛОГІЯ" *Paragon Encrypted Disk*

Paragon Encrypted Disk від ТОВ "ТЕХНОЛОГІЯ" призначений для захисту особистої та конфіденційної інформації від несанкціонованого доступу. *RSA Software Encryption System Professional*

Професійна програмна система шифрування *RSA* надає можливість шифрувати файли за допомогою пароля або файлу-ключа. Ця програма ідеально підходить для захисту будь-якої конфіденційної інформації як на локальному комп'ютері, так і при обміні даними через будь-який тип мережі, включаючи локальні мережі та Інтернет.

VeraCrypt

VeraCrypt — це абсолютно безкоштовний продукт, що володіє такою ж надійністю та функціональністю, як і комерційні рішення. Програма забезпечує

криптографічний захист будь-якої інформації: ділових документів, особистих фотографій та відео, програм, баз даних тощо.

VeraCrypt найчастіше використовується для захисту віртуальних дисків. На сьогодні цей метод вважається одним із найзручніших та найнадійніших способів забезпечення безпеки комп'ютерної інформації. Принцип роботи полягає в тому, що файли, створені цією програмою, можуть бути змонтовані як віртуальний диск

у вашій системі. Після цього ви можете використовувати їх як звичайні розділи жорсткого диска: копіювати будь-які об'єкти, встановлювати програмне забезпечення тощо. Інформація фізично зберігається у захищеному контейнері. При доступі вона автоматично розшифровується, а при записі – невидимо для користувача шифрується.

Окрім традиційних файлів-контейнерів, *VeraCrypt* також реалізує інші методи захисту інформації. Перш за все, це приховані розділи (*hidden volumes*). При використанні цієї опції інформація розміщується в нерозподіленій області жорсткого диска, до якої неможливо отримати доступ за допомогою стандартних інструментів операційної системи. Крім того, програма дозволяє зашифрувати системний диск, що вимагає автентифікації перед завантаженням *Windows*, тим самим підвищуючи безпеку всієї системи.

Важливою особливістю програми є її простота використання. Інтерфейс *VeraCrypt* інтуїтивно зрозумілий та лаконічний. Крім того, він перекладений багатьма мовами, включаючи українську. Варто також зазначити, що програма має портативний режим (*portable mode*). Ця функція дозволяє встановити її на флеш накопичувач та використовувати для безпечного перенесення інформації між комп'ютерами.

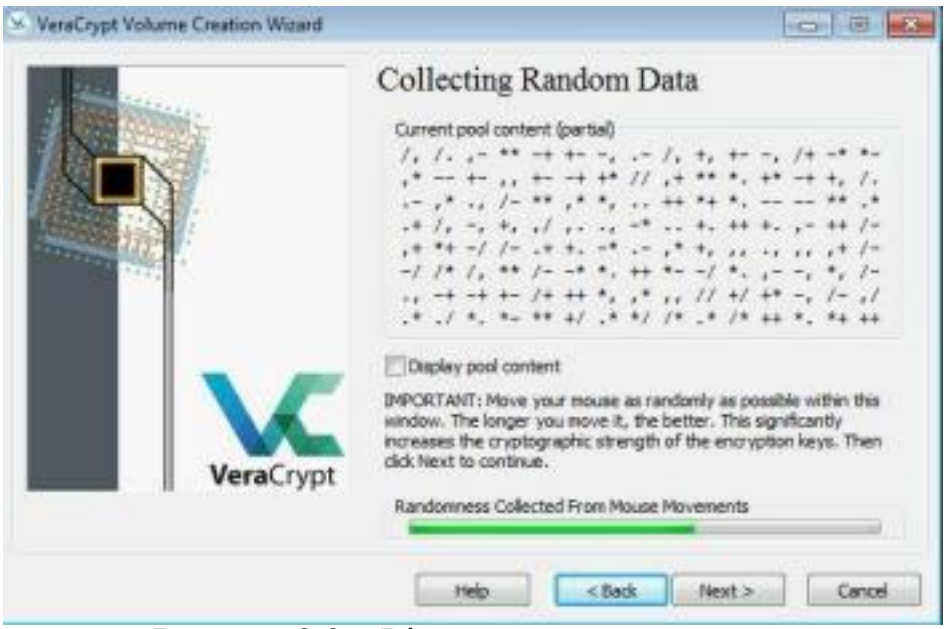

Рисунок 3.9 – Вікно програми *Veracrypt*

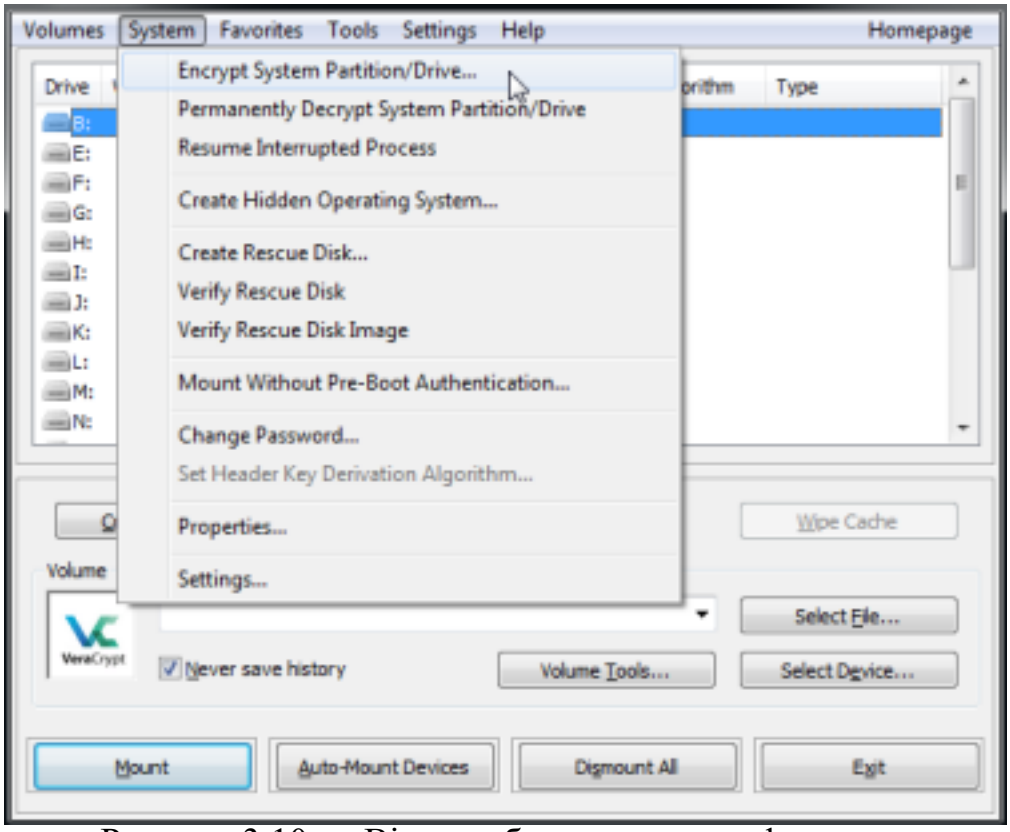

Рисунок 3.10 — Вікно вибору методу шифрування

Шифрування *USB*-накопичувачів

У деяких випадках необхідне шифрування флеш-накопичувачів. Якщо ви переносите важливі дані на флешку, яку не можна надавати третім особам, просте

шифрування даних забезпечить їх безпечне зберігання. Це можна зробити різними способами. Наприклад, можна скористатися архіватором *WinRAR* та архівувати дані з паролем. Також для шифрування флешок існують спеціалізовані програми.

USB Safeguard

USB Safeguard — це безкоштовний аплет, який легко шифрує ваші конфіденційні дані за допомогою алгоритму *AES*-256, забезпечуючи найвищий рівень безпеки. Для шифрування та розшифрування потрібен спеціальний ключ, відомий лише вам. Тому, навіть якщо флешка втрачена або вкрадена, інформація на ній залишається в безпеці (Див. Рисунок 3.11).

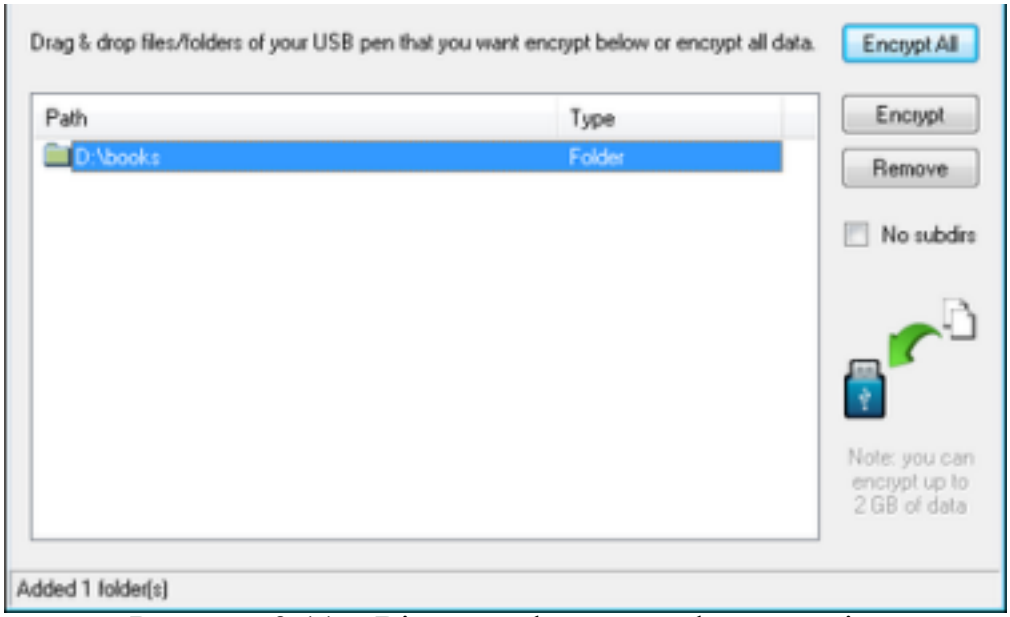

Рисунок 3.11 – Вікно шифрування флеш-носіїв

Щоб зашифрувати дані за допомогою *USB Safeguard*, просто завантажте його з офіційного веб-сайту та скопіюйте файл на флеш-накопичувач, що містить конфіденційну інформацію. При першому запуску програма запропонує створити унікальний ключ шифрування, а потім дозволить вибрати файли та папки для шифрування. Просто перетягніть потрібні об'єкти у вікно програми та натисніть "Зашифрувати все" (*Encrypt All*). Після шифрування всіх даних система запропонує два методи видалення вихідних даних (просте видалення та незворотне видалення), щоб запобігти їх відновленню за допомогою спеціалізованих програмних продуктів.

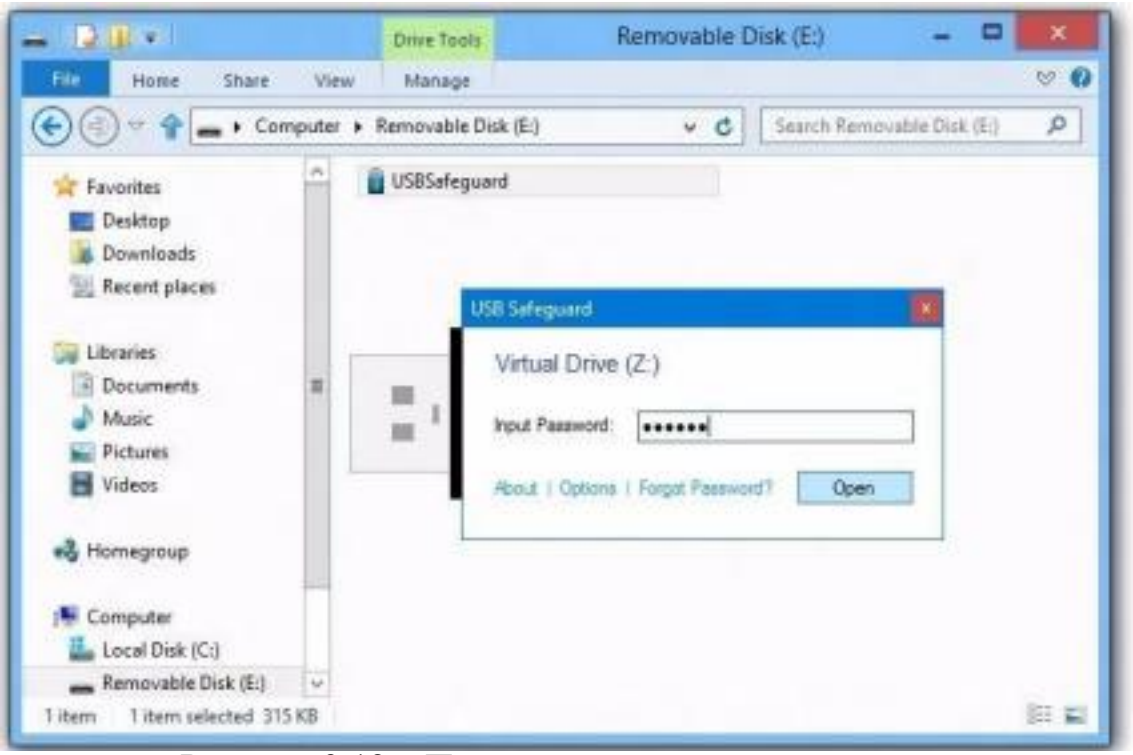

Рисунок 3.12 – Приклад використання програми

Для відновлення даних просто запустіть *USB Safeguard*, введіть ключ, виберіть файли та папки, які потрібно відновити (вони вже будуть у списку програми), та натисніть "Розшифрувати все" (*Decrypt All*). Після цього програма відновить дані, і ви зможете ними користуватися [2].

3.6 Пропозиції щодо підвищення ефективності системи інформаційної безпеки

Для посилення захисту інформаційної інфраструктури рекомендовано впровадити комплексне антивірусне рішення — *ESET Internet Security* на всіх робочих станціях. Дане програмне забезпечення забезпечує багаторівневий захист, що включає антивірус, антишпигунські функції, антиспам, брандмауер, а також модулі для виявлення фішингу та захисту онлайн-банкінгу.

У разі наявності встановленого стороннього антивірусного ПЗ, доцільно попередньо видалити його з метою запобігання конфліктам між системами безпеки. Для цього необхідно виконати такі дії:

«Пуск → Панель керування → Програми та компоненти», у списку

встановленого ПЗ обрати відповідну антивірусну програму та натиснути «Видалити». Окрім встановлення самого продукту, слід також придбати офіційну ліцензію, яка гарантує отримання регулярних оновлень сигнатур вірусів і підтримку з боку розробника. Наприклад, ліцензія на 2 робочі пристрої терміном дії 1 рік на момент підготовки даної роботи коштує 927 грн [4].

Після встановлення *ESET Internet Security*, у процесі активації необхідно вказати користувацькі облікові дані, отримані під час придбання ліцензії. У відповідних полях слід ввести:

- у рядку «Ім’я користувача» — значення, вказане в ліцензійній угоді;
- у рядку «Пароль» — відповідний ключ доступу до оновлень.

Застосування даного програмного забезпечення у поєднанні з політиками регулярного оновлення та контролю доступу дозволяє суттєво підвищити загальний рівень кіберзахисту організації.

ВИСНОВКИ

На основі проведеного дослідження сформульовано такі ключові положення:

1. Інформаційна безпека є критично важливою складовою сучасної цифрової інфраструктури та визначальним фактором сталого функціонування як окремих організацій, так і суспільства в цілому.

2. Локальні обчислювальні мережі (ЛОМ) залишаються одними з основних об’єктів для атак з боку зловмисників, що потребує постійного удосконалення стратегій кіберзахисту.

3. Ефективна система захисту інформації реалізується через структурований підхід, який включає: аудит мережі (виявлення вразливостей і визначення цінності даних), моделювання потенційних загроз, ідентифікацію можливого профілю порушника, а також вибір відповідних заходів протидії.

4. Технічні методи кіберзахисту охоплюють: впровадження сучасних систем сигналізації, встановлення сенсорів розбиття скла, відеонагляд та контроль фізичного доступу до об'єктів, що обробляють критичну інформацію.

5. До основного програмного забезпечення для забезпечення інформаційної

безпеки належать: багаторівневі антивірусні рішення, системи мережевих екранів (брандмауерів), засоби шифрування даних та сервіси для моніторингу безпеки.

6. Організаційно-правові заходи охоплюють регламентацію політик доступу, управління паролями, підвищення обізнаності користувачів, а також дотримання національних і міжнародних норм у сфері захисту інформації, з обов'язковим регулярним оновленням політик безпеки.

7. У ході дослідження було здійснено аналіз програмних засобів захисту, зокрема антивірусного ПЗ, що є одним з ключових компонентів комплексного захисту локальної мережі, та сформульовано рекомендації щодо їх впровадження для підвищення загального рівня інформаційної безпеки.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *ISO/IEC* 27001:2022. *Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements*. – Женева : *ISO,* 2022. – 50 с.

2. *NIST SP* 800-53 *Revision* 5. *Security and Privacy Controls for Information Systems and Organizations* / *National Institute of Standards and Technology*. – Гейтерсберг : *NIST,* 2020. – 482 с.

3. *ISO/IEC* 27002:2022. *Information Security, Cybersecurity and Privacy Protection – Code of Practice for Information Security Controls*. – Женева : *ISO,* 2022. – 120 с.

4. *RFC* 2196: *Site Security Handbook* / *B. Fraser, ed*. – *Internet Engineering Task Force* (*IETF*), 1997. – 154 с.

5. *Microsoft*: *Security Best Practices for Network Infrastructure*. – [Електронний ресурс]. – Режим доступу: *https://learn.microsoft.com* (дата звернення: 30.05.2025).

6. *Cisco Guide to Harden Cisco IOS Devices*. – [Електронний ресурс]. – Режим доступу: *https://www.cisco.com* (дата звернення: 30.05.2025).

7. *OWASP Top* 10 – 2021: *The Ten Most Critical Web Application Security Risks*. – [Електронний ресурс]. – Режим доступу: *https://owasp.org* (дата звернення: 30.05.2025).

8. *Kaspersky IT Encyclopedia*: *Network Security*. – [Електронний ресурс]. – Режим доступу: *https*://*encyclopedia.kaspersky.com* (дата звернення: 30.05.2025). 9. Теслюк В.М., Базильчук Я.Ю. Бездротові інформаційні технології. – Львів : Видавництво Львівської політехніки, 2019. – 312 с.

10. Копець С.В. Основи інформаційної безпеки в мережах. – К. : Ліра-К, 2021. – 248 с.

11. Андрієнко М.С. Бездротові мережі та їх захист. – Харків : ХНУРЕ, 2020. – 192 с.

12. Теліженко М.М. Комп’ютерні мережі. Навчальний посібник. – Київ : Каравела, 2021. – 288 с.

13. Савченко О.Ф., Гончар Т.А. Захист бездротових сенсорних мереж: виклики та рішення. – Вісник НТУУ «КПІ». Серія: Інформатика, управління та обчислювальна техніка. – 2022. – №3. – С. 42–49.

14. Паламарчук В.С. Захист інформації у відкритих мережах. – Київ : Академвидав, 2022. – 216 с.

15. Білоус О.В. Криптографічний захист у безконтактних мережах. – Системи управління та автоматики. – 2023. – №2. – С. 34–42.

16. Жуков І.О. Інформаційна безпека в комп’ютерних мережах: навч. посіб. – Харків : ХНУРЕ, 2021. – 200 с.

17. Захист інформації в комп’ютерних системах і мережах / за ред. І.О. Марченка. – Харків : ХНУРЕ, 2023. – 276 с.

18. Безрукий В.С. Адміністрування та безпека локальних комп’ютерних мереж. – К. : Ліра-К, 2020. – 310 с.

КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

РЕЦЕНЗІЯ

на кваліфікаційну роботу

випускника спеціальності: 123 «Комп'ютерна інженерія»

відділення: комп'ютерної та програмної інженерії

циклова комісія: комп'ютерних систем та мереж

Михайло НОВІКОВ
(ім'я, прізвище)

1. Актуальність теми: Обрана тема кваліфікаційної роботи «Інформаційна безпека в комп'ютерній мережі» є актуальною.

2. Кваліфікаційна робота відповідає темі, затвердженій наказом.

3. Завдання на виконання кваліфікаційної роботи виконано у повному обсязі.

4. В результаті виконання кваліфікаційної роботи було обране програмне забезпечення для захисту комп'ютерної мережі.

5. Якість виконання пояснювальної записки та ілюстративного (графічного) матеріалу відповідає вимогам Державних стандартів.

6. В кваліфікаційній роботі зроблений акцент на дані отримані на практиці («живі» експерименти).

7. Кваліфікаційна робота заслуговує оцінку «добре».

Рецензент к.т.н.
(науковий ступінь, посада)

«05» 06 2025 р. _____ Сергій ЦВІРКУН
(підпис) (ім'я, прізвище)

З рецензією ознайомлений _____ Михайло НОВІКОВ
(підпис) (ім'я, прізвище)