МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
(повна назва випускної кафедри)

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему:

КОМП'ЮТЕРНА МЕРЕЖА ПІДПРИЄМСТВА ТА АНАЛІЗ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ЗАХИСТУ ДАНИХ

Виконав:
студент групи 2*КІ-23* зі спеціальності
123 – «Комп'ютерна інженерія»
Олексій СЕЛІОНОВ
Науковий керівник:
к.т.н Роксолана БРЕУС
(науковий ступінь, вчене звання, прізвище та ініціали)

Черкаси, 2025

АНОТАЦІЯ

Дипломна робота присвячена аналізу комп’ютерної мережі підприємства та оцінці програмного забезпечення для захисту даних. У роботі розглянуто теоретичні основи побудови комп’ютерних мереж, типи загроз інформаційній безпеці та сучасні технології кіберзахисту.

Проведено аналіз структури комп’ютерної мережі реального підприємства, досліджено програмне забезпечення, що використовується для захисту інформації, та визначено рівень його ефективності.

Розроблено рекомендації щодо вдосконалення системи захисту, включаючи модернізацію апаратного забезпечення, впровадження сучасних засобів резервного копіювання, а також підвищення рівня кіберстійкості підприємства шляхом поліпшення політики інформаційної безпеки.

Практична значущість роботи полягає у можливості впровадження отриманих результатів для підвищення рівня захищеності інформаційних ресурсів підприємства в умовах зростаючих кіберзагроз.

Ключові слова: КОМП’ЮТЕРНА МЕРЕЖА, КІБЕРБЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА, ЗАХИСТ ДАНИХ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ЗАГРОЗИ, ШИФРУВАННЯ, ПІДПРИЄМСТВО.

ABSTRACT

The thesis is devoted to the analysis of a corporate computer network and the evaluation of data protection software. The paper examines the theoretical foundations of computer network design, types of information security threats, and modern cybersecurity technologies.

The author analyzes the network structure of a real-world enterprise, investigates the data protection software currently in use, and evaluates its effectiveness.

Recommendations are developed to improve the security system, including hardware upgrades, implementation of modern backup tools, and enhancement of the company's information security policy to increase overall cyber resilience.

The practical significance of the study lies in the applicability of the obtained results for improving the security of enterprise information resources under the growing threat of cyberattacks.

Keywords**:** COMPUTER NETWORK, CYBERSECURITY, INFORMATION SECURITY, DATA PROTECTION, SOFTWARE, THREATS, ENCRYPTION, ENTERPRISE.

ЗМІСТ

ВСТУП

У сучасних умовах стрімкого розвитку цифрових технологій питання захисту інформації набуває першочергового значення для будь-якого підприємства. Комп'ютерні мережі стали основою функціонування інформаційної інфраструктури організацій, а безперебійна та захищена передача даних – ключовим фактором забезпечення ефективної діяльності. Однак одночасно зі зростанням обсягів оброблюваної інформації та ускладненням мережевих архітектур зростає і кількість загроз, пов'язаних з несанкціонованим доступом, витоком, спотворенням чи втратою даних. У цьому контексті вивчення засобів захисту комп'ютерних мереж та аналіз програмного забезпечення, яке забезпечує конфіденційність, цілісність і доступність даних, є вкрай актуальним.

Актуальність теми полягає у необхідності забезпечення надійного захисту інформаційних ресурсів підприємств в умовах цифровізації бізнес-процесів, розвитку кіберзагроз та збільшення використання хмарних технологій. Підвищення рівня кібербезпеки є важливим завданням для функціонування підприємства будь-якого масштабу, а впровадження сучасних засобів захисту інформації – ключем до збереження конкурентоспроможності.

Метою даної роботи є розроблення рекомендацій щодо вдосконалення системи захисту комп'ютерної мережі підприємства шляхом аналізу існуючих загроз, оцінювання ефективності застосовуваного програмного забезпечення та впровадження сучасних технологій кібербезпеки.

Для досягнення поставленої мети у роботі необхідно виконати наступні завдання:

- розглянути теоретичні основи побудови комп'ютерних мереж і принципи їх захисту;
- класифікувати загрози інформаційній безпеці в мережевих середовищах;

– проаналізувати програмне забезпечення для забезпечення безпеки даних;

– дослідити структуру комп’ютерної мережі конкретного підприємства;

– виявити вразливості та загрози, що можуть впливати на інформаційні потоки підприємства;

– оцінити ефективність використаних засобів захисту;

– сформулювати практичні рекомендації щодо модернізації системи захисту даних.

Об’єктом дослідження є комп’ютерна мережа сучасного підприємства як інфраструктурна основа функціонування інформаційної системи.

Предметом дослідження є програмно-апаратні засоби та організаційні методи захисту даних у комп’ютерній мережі підприємства.

Методи дослідження, включають: аналіз наукових джерел, метод порівняння, моделювання, експертне оцінювання, SWOT-аналіз, системний підхід до вивчення структури та вразливостей мережі, аналітичне оцінювання ефективності засобів захисту.

Практичне значення одержаних результатів полягає в можливості впровадження запропонованих заходів із вдосконалення системи захисту даних у підприємницькій діяльності, що дозволить мінімізувати ризики кіберзагроз, знизити потенційні втрати від витоків інформації та підвищити загальний рівень кіберстійкості підприємства.

Апробація результатів дослідження здійснювалась у формі доповіді на Всеукраїнській науково-практичній конференції студентів та молодих науковців «Цифрова безпека в умовах кіберреальності» (м. Черкаси, березень 2025 року).

Кваліфікаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 80 сторінок комп’ютерного тексту (без урахування додатків).

РОЗДІЛ 1 ОСОБЛИВОСТІ КОМП'ЮТЕРНИХ МЕРЕЖ І ЗАХИСТУ ДАНИХ

1.1 Поняття та класифікація комп'ютерних мереж

Комп'ютерна мережа є сукупністю взаємопов'язаних між собою апаратних та програмних засобів, призначених для забезпечення передачі, зберігання, обробки та спільного використання інформації між комп'ютерами, серверами та іншими пристроями [1]. Основною метою створення мережі являється ефективний обмін даними, підвищення продуктивності, централізоване адміністрування та спільний доступ до ресурсів (файлів, принтерів, баз даних тощо) [2].

Сучасні комп'ютерні мережі поділяються за різними ознаками, проте всі вони мають спільні складові елементи [3], серед яких:

- вузол (Node) – це будь-який активний пристрій у мережі, що може приймати, передавати або обробляти інформацію (наприклад, комп'ютери, сервери, маршрутизатори, принтери).
- Канал зв'язку (Communication Channel) – фізичне або логічне середовище, яким передаються дані між вузлами. До каналів зв'язку належать виті пари, оптоволоконні кабелі, радіоканали тощо.
- Протокол (Protocol) – набір правил і стандартів, що визначають формат, порядок і методи передачі даних між пристроями. Наприклад, TCP/IP, HTTP, FTP.
- Сервіс (Service) – програмний або мережевий ресурс, що надається клієнтам, наприклад, електронна пошта, доступ до бази даних, веб-сервер [4].

Для ефективного функціонування комп'ютерної мережі всі ці елементи повинні працювати узгоджено згідно з визначеною архітектурою та стандартами [5].

Окрім понятійного апарату, важливим етапом розуміння побудови комп'ютерної мережі є візуалізація її типових структурних компонентів. Це

дозволяє наочно побачити, яким чином взаємодіють між собою елементи мережі та якою є їхня функціональна взаємозалежність [6].

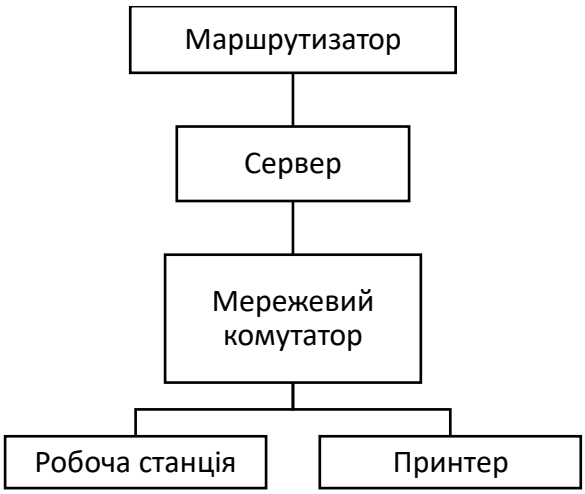


Рисунок 1.1 – Схематичне зображення типової локальної комп’ютерної мережі (LAN)

Структура типової локальної мережі підприємства базується на топології типу «зірка», як зображено на рис. 1.1, де всі вузли підключені до центрального комутатора. Комутатор забезпечує маршрутизацію внутрішнього трафіку між робочими станціями, сервером і периферійними пристроями, такими як принтери [7]. Зовнішнє з’єднання із мережею Інтернет забезпечує маршрутизатор, який також виконує функції міжмережевого екрана та керує трафіком на основі заданих політик безпеки [8].

Ця базова схема є типовою для більшості малих і середніх підприємств, оскільки вона забезпечує ефективне керування, надійність і простоту розгортання інфраструктури. Водночас така структура дозволяє масштабувати мережу без суттєвих змін її архітектури.

Одним з ключових критеріїв класифікації комп’ютерних мереж є географічна протяжність зони покриття, що безпосередньо впливає на принципи побудови мережі, вибір технічних засобів та особливості адміністрування. Залежно від масштабу, мережі умовно поділяються на три основні типи: локальні (LAN), міські (MAN) та глобальні (WAN) [9].

Як видно з табл. 1.1, локальні мережі (LAN) є найпоширенішими в межах підприємств і офісів, де забезпечується висока швидкість, простота

обслуговування та мінімальні витрати на побудову. Міські мережі (MAN), в основному, використовуються для об’єднання установ в межах одного міста чи району, тоді як глобальні мережі (WAN) охоплюють території національного та міжнародного масштабу й потребують спеціалізованих рішень щодо безпеки та надійності [10].

Таблиця 1.1 – Порівняльна характеристика комп’ютерних мереж за географічним масштабом

№	Характеристика	LAN (локальна)	MAN (міська)	WAN (глобальна)
1	Радіус покриття	До 1 км	До 50 км	Від 50 км до кількох тисяч км
2	Тип з’єднання	Ethernet, Wi-Fi	Оптоволоконні, DSL	Супутникові, MPLS, VPN
3	Швидкість передачі	100 Мбіт/с – 10 Гбіт/с	10 Мбіт/с – 1 Гбіт/с	1 Мбіт/с – 1 Гбіт/с
4	Вартість побудови	Низька	Середня	Висока
5	Обслуговування	Простіше	Помірна складність	Висока складність
6	Типова сфера застосування	Офіси, підприємства, навчальні заклади	Міські структури, університетські кампуси	Міждержавні об’єднання, банки, телекомунікації

Топологія комп’ютерної мережі визначає схему фізичного або логічного з’єднання мережевих пристроїв. Від вибору топології залежить не лише швидкість обміну даними, а й стабільність, масштабованість, зручність адміністрування та вартість побудови мережі [11]. Сучасні мережі можуть реалізовувати одну з кількох базових топологій або їх комбінацію – залежно від завдань підприємства, масштабів діяльності та технічних можливостей [12].

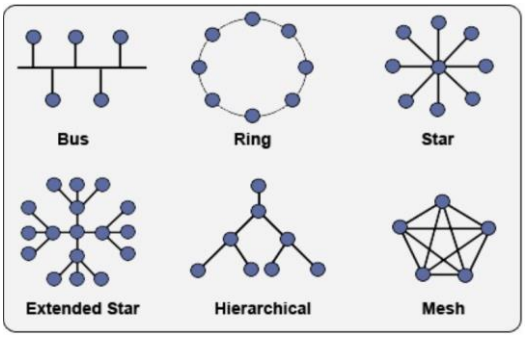


Рисунок 1.2 – Типи мереж за топологією

До основних топологій, що знайшли практичне застосування у сучасних мережах, належать: шина, зірка, кільце, дерево та сітка (mesh). Типи мереж за топологією представлено на рис.1.2. Кожна з них має характерні риси, переваги та недоліки [13].

З табл. А.1, представленої в додатку А, можна зробити висновок, що найпоширенішою у корпоративному середовищі є топологія зірки, оскільки вона поєднує надійність з простотою впровадження. Топологія шини нині використовується рідко через складність масштабування, тоді як кільце застосовується у спеціалізованих мережах з критичними вимогами до порядку передавання даних. Дерево дозволяє створювати великі багаторівневі мережі, а сітка – забезпечити максимальну відмовостійкість, хоча й потребує значних витрат на реалізацію [14].

Окрім географічного масштабу та топології, важливою характеристикою комп'ютерної мережі є тип управління інформаційними процесами, що визначає логіку взаємодії пристроїв, розподіл ролей між ними та архітектуру самої системи. За цим критерієм мережі поділяють на централізовані, децентралізовані, однорангові (P2P) та клієнт-серверні [15].

Кожен із підходів має свої переваги й обмеження, які впливають на масштабованість, ефективність захисту, витрати на обслуговування та рівень контролю над даними. Порівняння архітектур комп'ютерних мереж за способом управління представлено в табл. А.2 додатку А.

У централізованих мережах усі рішення та обробка даних зосереджені в одному центрі, що забезпечує зручне управління, але створює критичну залежність від працездатності головного вузла. Децентралізовані мережі забезпечують вищу відмовостійкість, але потребують складнішої координації [16].

Однорангові архітектури добре підходять для невеликих локальних мереж або тимчасових з'єднань, тоді як клієнт-серверна модель є найбільш поширеною в корпоративному середовищі, завдяки чіткому розподілу ролей та централізованому контролю безпеки [17].

У системі інформаційного обміну між пристроями ключову роль відіграє стандартизована еталонна модель взаємодії відкритих систем (Open Systems Interconnection model – OSI) [18]. Ця модель розроблена Міжнародною організацією зі стандартизації (ISO) та описує структуру мережевої взаємодії у вигляді семирівневої ієрархії, в якій кожен рівень виконує специфічні функції та взаємодіє з сусідніми. Структура моделі OSI представлена в табл. 1.2.

Таблиця 1.2 – Структура моделі OSI

№	Рівень	Назва рівня	Функції
1	7	Прикладний (Application)	Забезпечення доступу до мережевих сервісів користувачам (ел. пошта, FTP)
2	6	Представлення (Presentation)	Кодування, шифрування, стиснення даних
3	5	Сеансовий (Session)	Керування діалогом, установлення та підтримка з’єднань
4	4	Транспортний (Transport)	Розбиття даних на сегменти, контроль помилок, відновлення
5	3	Мережевий (Network)	Визначення маршруту, IP-адресація, передача пакетів
6	2	Канальний (Data Link)	Формування кадрів, визначення MAC-адрес, виявлення помилок на рівні кадрів
7	1	Фізичний (Physical)	Передача бітів через фізичне середовище (кабель, радіохвилі)

Джерело: створено автором на основі даних [10]

Модель OSI є концептуальною основою для розробки протоколів і архітектур комп’ютерних мереж [19]. Вона дозволяє уніфікувати принципи побудови мереж, а також забезпечити взаємодію різних апаратних і програмних засобів незалежно від виробника. Визначення коефіцієнтА ефективності передавання даних показано в формулі 1.1.

$$\eta = \frac{V_{\text{кор}}}{V_{\text{ном}}}, \qquad (1.1)$$

де:

- η – коефіцієнт ефективності передавання даних,
- $V_{\text{кор}}$ – корисна швидкість передачі (корисна інформація без службових даних),

- $V_{ном}$– номінальна швидкість каналу (вся передана інформація включно з накладними витратами).

Якщо номінальна швидкість каналу складає 100 Мбіт/с, а з урахуванням усіх службових даних, перезаписів, фреймінгу та шифрування, реальна корисна швидкість складає лише 72 Мбіт/с.

$$\eta = \frac{72}{100} = 0{,}72 \text{ або } 72\%$$

Це означає, що лише 72% канальної пропускної здатності реально використовується для передавання корисної інформації, а решта витрачається на технічні накладні витрати.

Отже, модель OSI дозволяє не лише описати логіку побудови мереж, але й оцінити ефективність функціонування мережевої інфраструктури за допомогою конкретних метрик [20]. У практиці адміністрування, показник ефективності η\etaη застосовується для оптимізації конфігурацій, вибору протоколів та оцінки доцільності модернізації обладнання [21].

1.2 Протоколи та технології комп'ютерних мереж

Ефективне функціонування комп'ютерних мереж є неможливим без суворого дотримання узгоджених правил обміну інформацією між пристроями. Саме такі правила описуються мережевими протоколами [22].

Мережевий протокол – це формалізований набір правил, що визначають формат, порядок, спосіб передавання та обробки даних у мережі [23]. Протоколи забезпечують взаєморозуміння між відправником і одержувачем, навіть якщо вони використовують різне обладнання чи програмне забезпечення. Кожен рівень мережевої моделі (наприклад, OSI або TCP/IP) оперує своїми специфічними протоколами [24].

Найбільш поширеним і базовим набором протоколів, що лежить в основі сучасного Інтернету, є стек TCP/IP (Transmission Control Protocol / Internet

Protocol). Цей набір був розроблений у 1970-х роках Агентством передових оборонних дослідницьких проєктів США (DARPA) і наразі став де-факто стандартом глобальної мережевої взаємодії [25].

TCP/IP включає два основні компоненти:

— IP (Internet Protocol) – відповідає за адресацію пристроїв у мережі та маршрутизацію пакетів даних.

— TCP (Transmission Control Protocol) – забезпечує надійність передавання, контроль послідовності, підтвердження доставки, виявлення втрат і повторну передачу даних [26].

Наприклад, під час відкриття веб-сторінки TCP ділить інформацію на сегменти, відправляє їх до сервера, контролює, щоб усі вони прибули в цілості, а IP відповідає за доставку цих сегментів по маршруту до відповідного вузла [27].

Стек TCP/IP є багаторівневою системою, аналогічною до моделі OSI, але має спрощену структуру з чотирма рівнями [28]:

1. Прикладний (Application)
2. Транспортний (Transport)
3. Мережевий (Internet)
4. Мережевий доступ (Link/Network Access)

Інтеграція протоколів у стек TCP/IP дозволяє забезпечити уніфіковану комунікацію в різнорідних мережах – від локальних до глобальних, від фіксованих до мобільних. Надійність, масштабованість і відкритість стандартів TCP/IP зумовили його домінування у сучасному цифровому середовищі [29].

Для реалізації ефективної взаємодії в комп’ютерних мережах використовується низка транспортних і мережевих протоколів, які відповідають за різні аспекти передавання даних – від маршрутизації до контролю помилок. Найбільш поширеними протоколами цієї групи є TCP, UDP, IP та ICMP [30].

— IP (Internet Protocol) – базовий мережевий протокол, що здійснює адресацію та маршрутизацію пакетів між вузлами мережі. Він не гарантує доставку, цілісність або послідовність пакетів – лише спрямовує їх у відповідне місце призначення за допомогою IP-адрес.

— TCP (Transmission Control Protocol) – протокол транспортного рівня, який гарантує надійне, впорядковане та контрольоване передавання даних між вузлами. Використовується в додатках, де важлива цілісність – наприклад, передавання веб-сторінок, електронної пошти, файлів [1].

— UDP (User Datagram Protocol) – легковаговий протокол транспортного рівня без встановлення з'єднання. Він забезпечує швидке, але ненадійне передавання даних без підтвердження доставки. Підходить для реального часу: потокове відео, голосові виклики (VoIP), онлайн-ігри.

— ICMP (Internet Control Message Protocol) – допоміжний протокол, що використовується для діагностики та обміну службовими повідомленнями (наприклад, у командах ping, traceroute). Він допомагає визначити доступність вузлів та швидкість реакції [31].

Особливе значення для порівняльного аналізу мають TCP і UDP – два основні протоколи транспортного рівня [32].

Таблиця 1.3 – Порівняння протоколів TCP і UDP

№	Критерій	TCP	UDP
1	Тип з'єднання	Орієнтований на з'єднання (встановлення сесії)	Без з'єднання (немає сесії)
2	Гарантія доставки	Так – підтвердження доставки кожного пакета	Ні – пакети можуть бути втрачені
3	Порядок доставки	Гарантовано зберігається	Не гарантується
4	Швидкість	Нижча через контроль та підтвердження	Вища, оскільки відсутні механізми контролю
5	Контроль помилок	Вбудований: контрольна сума, повторна передача	Мінімальний, лише контрольна сума
6	Накладні витрати	Високі	Мінімальні
7	Сценарії використання	Веб-трафік, FTP, електронна пошта	Відео/аудіо стримінг, VoIP, онлайн-ігри

Дані табл. 1.5 показують, що TCP забезпечує стабільне та контрольоване середовище для передавання даних, однак із дещо нижчою швидкістю через додаткові перевірки. Натомість UDP призначений для застосувань, де пріоритетом є швидкість та низька затримка, навіть за умови можливої втрати деякої частини інформації [33].

Правильний вибір між TCP та UDP залежить від вимог до надійності, часової чутливості та ресурсної економії мережевого додатку або сервісу [34].

У сучасних комп'ютерних мережах забезпечення конфіденційності, цілісності та автентичності даних неможливе без використання криптографічних протоколів [35]. Вони реалізують алгоритми шифрування, керування ключами та перевірки автентичності під час передачі інформації мережею. До найбільш поширених протоколів цієї групи належать HTTPS, SSL/TLS та IPSec [36].

- HTTPS (HyperText Transfer Protocol Secure) – захищений варіант протоколу HTTP, що працює у зв'язці з SSL або TLS. Він забезпечує шифрування переданих даних між веб-браузером і сервером, тим самим запобігаючи перехопленню або зміні інформації під час комунікації [37].
- SSL (Secure Sockets Layer) / TLS (Transport Layer Security) – криптографічні протоколи, що забезпечують захищене передавання даних у мережах. TLS є новішою і безпечнішою версією SSL, яка підтримує автентифікацію серверів, шифрування трафіку та перевірку цілісності переданих повідомлень.
- IPSec (Internet Protocol Security) – набір протоколів, призначених для захисту IP-комунікацій через шифрування та автентифікацію на мережевому рівні. Використовується в корпоративних VPN, міжмережевих з'єднаннях і захищених тунелях.

Найбільш показовою є робота SSL/TLS протоколу, яка реалізується через так званий handshake – процедуру встановлення захищеного з'єднання між клієнтом і сервером. Цей процес включає автентифікацію, обмін ключами шифрування та узгодження криптографічних алгоритмів [38].

Хмарні обчислення (cloud computing) стали ключовою технологією сучасної цифрової інфраструктури, трансформуючи підходи до зберігання, обробки та передачі даних у комп'ютерних мережах. Замість традиційної моделі, де обчислення виконуються локально, хмарна модель передбачає використання віддалених серверів, до яких здійснюється доступ через Інтернет або інші мережеві з'єднання.

В умовах розподілених мереж хмарні сервіси дозволяють:

- зменшити витрати на апаратне забезпечення;
- масштабувати ресурси в режимі реального часу;
- забезпечити високу доступність та резервування даних;
- централізувати управління і безпеку [39].

Типові хмарні сервіси поділяються на:

- IaaS (інфраструктура як сервіс) – віртуальні сервери, сховища;
- PaaS (платформа як сервіс) – середовище для розробки і тестування;
- SaaS (програмне забезпечення як сервіс) – готові веб-застосунки (CRM, офісні сервіси) [40].

Важливим критерієм ефективності взаємодії між користувачем і хмарною інфраструктурою є ступінь використання пропускної здатності мережевого каналу, що значною мірою визначає швидкість доступу до ресурсів і загальний рівень продуктивності системи [41].

Рівень використання пропускної здатності каналу:

$$\eta = \frac{D_{\text{викор}}}{D_{\text{макс}}} \times 100\%, \qquad (1.2)$$

де:

- η – відсотковий рівень використання каналу,
- $D_{\text{викор}}$ – обсяг трафіку, який реально передано за певний період (наприклад, за 1 хвилину),
- $D_{\text{макс}}$ – максимально можлива пропускна здатність каналу за той самий період.

Якщо припустити, що хмарна система обробляє запити віддалених користувачів через канал із максимальною пропускною здатністю 100 Мбіт/с, то фактично протягом хвилини було передано 68 Мбіт корисних даних.

$$\eta = \frac{68}{100} \times 100\% = 68\%$$

Це означає, що лише 68% потенціалу каналу використовується, тоді як решта залишається незадіяною або витрачається на службовий трафік, очікування та пакети з помилками. У віртуалізованому середовищі, де трафік має змішаний характер (запити, відповіді, оновлення, резервування), цей показник дозволяє оптимізувати мережеву інфраструктуру, балансувати навантаження та обґрунтовувати необхідність розширення каналу [42].

Використання хмарних технологій створює нові виклики для адміністраторів: необхідність управління трафіком, моніторингу пропускної здатності, захисту даних у стані передавання та гарантування якості сервісу (QoS). Формула 1.2 є одним з базових інструментів для оцінки ефективності таких систем.

1.3 Загрози інформаційній безпеці в комп'ютерних мережах

Інформаційна безпека є однією з ключових складових функціонування сучасних комп'ютерних мереж, що охоплюють як корпоративні, так і глобальні інформаційні системи. З огляду на стрімкий розвиток цифрових технологій та зростаючу залежність від інформаційних ресурсів, зростає потреба у надійному захисті інформації від внутрішніх і зовнішніх загроз. Забезпечення цілісності, конфіденційності та доступності даних стає обов'язковою умовою ефективного функціонування будь-якої інформаційної інфраструктури [43].

Під поняттям інформаційної безпеки розуміють стан захищеності інформації та інформаційних систем від випадкового або навмисного втручання, що може призвести до її модифікації, знищення, блокування доступу або несанкціонованого розголошення. Такий стан забезпечується за допомогою комплексу організаційних, технічних, правових і програмних заходів.

У центрі концептуального підходу до інформаційної безпеки перебуває так звана CIA-модель, що базується на трьох основоположних принципах: конфіденційність (Confidentiality), цілісність (Integrity) та доступність (Availability).

Конфіденційність означає, що доступ до інформації мають виключно уповноважені суб’єкти. Цей принцип реалізується через механізми ідентифікації, автентифікації, авторизації, а також шляхом шифрування даних. Його порушення може призвести до витоку комерційної, персональної чи службової інформації, що має правові та економічні наслідки.

Цілісність передбачає збереження точності, повноти та несфальсифікованості інформації. Це означає, що дані не можуть бути змінені або знищені без належного дозволу, а будь-які спроби несанкціонованого втручання мають бути виявлені. Технічні засоби забезпечення цілісності включають хешування, цифрові підписи, контрольні суми, системи виявлення змін та журналювання подій [44].

Доступність передбачає, що інформація та інформаційні сервіси повинні бути доступними для уповноважених користувачів у момент виникнення потреби. У цьому контексті важливими є такі засоби, як резервне копіювання, відновлення після збоїв, побудова відмовостійких систем, застосування кластеризації та захист від атак типу відмова в обслуговуванні (DDoS).

Сукупне дотримання зазначених принципів дає змогу сформувати надійну систему інформаційної безпеки, здатну протистояти як технічним, так і організаційним загрозам. У процесі проєктування та адміністрування комп’ютерних мереж принципи CIA використовуються як методологічна основа для формування політик безпеки, вибору інструментів захисту та оцінки поточного стану інформаційного середовища.

Ефективне забезпечення інформаційної безпеки в комп’ютерних мережах вимагає глибокого розуміння джерел і типів загроз, що можуть впливати на цілісність, конфіденційність і доступність інформації. Загрози – це потенційні події або дії, здатні спричинити порушення нормального функціонування інформаційної системи, викликати втрату даних, порушення роботи мережі або компрометацію критичних сервісів.

Загрози класифікуються за різними критеріями, проте найбільш поширеним є поділ на внутрішні, зовнішні, програмні та фізичні. Детальна

класифікація загроз інформаційній безпеці в комп'ютерних мережах представлена в табд. А.3 додатка А. Такий підхід дозволяє комплексно охопити всі вектори ризику та формалізувати підходи до їхнього виявлення й нейтралізації [45].

Зазначена класифікація дозволяє не лише систематизувати можливі загрози, а й орієнтувати політики інформаційної безпеки на упередження, виявлення і реагування залежно від джерела ризику. Зокрема, для внутрішніх загроз доцільним є впровадження контролю доступу та логування дій користувачів; для зовнішніх – застосування міжмережевих екранів, систем виявлення вторгнень та захищених протоколів обміну; для програмних – регулярне оновлення ПЗ та антивірусний захист; для фізичних – резервне копіювання, захист приміщень і безперебійне живлення [46].

Комплексний підхід до класифікації загроз дає змогу побудувати багаторівневу модель захисту, орієнтовану на реальні сценарії ризиків.

Інформаційні системи та комп'ютерні мережі постійно зазнають впливу як цілеспрямованих, так і випадкових атак, які порушують основні принципи інформаційної безпеки: конфіденційність, цілісність і доступність. Розуміння природи мережевих атак, їхніх цілей і способів реалізації є основою для формування ефективної системи захисту. Характеристика поширених атак на комп'ютерні мережі представлена в табл. А.4 додатка А.

Найбільш поширеними в практиці є такі типи атак, як DoS/DDoS, фішинг, man-in-the-middle (MITM) і sniffing. Вони мають різну природу – від технічних до соціоінженерних – та потребують різних методів протидії.

Зазначені атаки реалізуються зловмисниками як автономно, так і в комбінації. Наприклад, sniffing може передувати MITM-атаці або стати її частиною. А фішинг, що на перший погляд є позатехнічним методом, часто є початковим етапом глибшого вторгнення до системи.

Суть процесу полягає у тому, що зловмисник, розміщений у каналі між клієнтом і сервером, перехоплює трафік, зберігаючи можливість змінювати або

підробляти дані, залишаючись при цьому непоміченим. Найчастіше ця атака реалізується в незашифрованих або слабо захищених мережах.

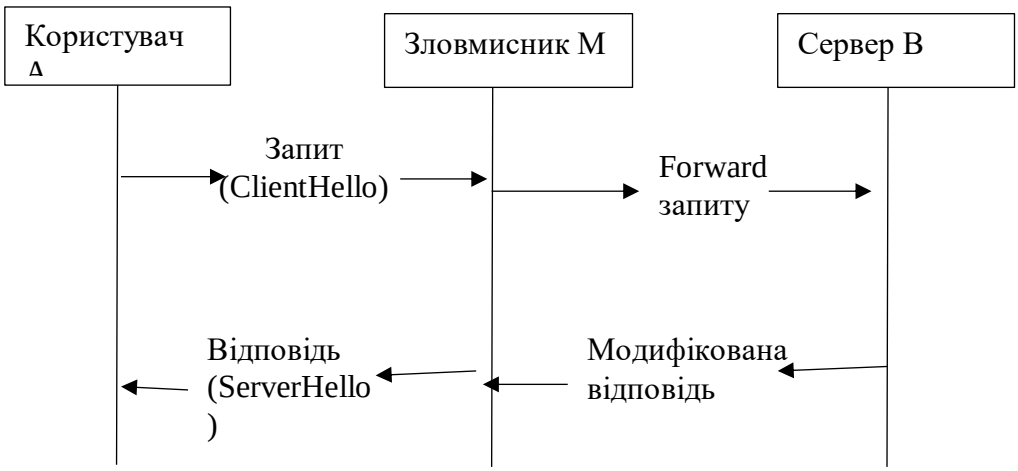


Рисунок 1.3 – Текстовий алгоритм роботи атаки "людина посередині" (MITM)

Захист від подібних атак передбачає впровадження сучасних засобів шифрування (TLS, IPsec), багатофакторної автентифікації, інструментів моніторингу трафіку, а також політик безпеки, орієнтованих на виявлення аномалій [41].

Операційні системи (ОС) та прикладне програмне забезпечення є одними з найбільш критичних компонентів інформаційної інфраструктури, оскільки вони забезпечують керування апаратними ресурсами, реалізацію мережевих протоколів, збереження та обробку даних. Вразливості в цих компонентах можуть стати об’єктом експлуатації зловмисників і призвести до порушення цілісності, конфіденційності чи доступності інформації.

Під вразливістю слід розуміти слабке місце в логіці програмного коду, архітектурі системи або в її налаштуваннях, яке може бути використане для компрометації системи.

Основні категорії вразливостей:

- логічні помилки (наприклад, порушення прав доступу);
- переповнення буфера (buffer overflow);
- помилки обробки винятків;
- помилки конфігурації;

- використання застарілого ПЗ з відомими дефектами;
- вразливості до виконання довільного коду (remote code execution).

Операційні системи Windows і Linux, хоча й мають відмінні архітектурні підходи, залишаються об'єктами цільових атак через виявлені або потенційні вразливості [48].

Серед прикладів вразливостей у Windows можна виділити наступні:

1. EternalBlue (CVE-2017-0144) – критична вразливість у протоколі SMBv1, яка дозволяє віддалене виконання коду без автентифікації. Була використана в атаках WannaCry і NotPetya. Вразливість полягала в помилці обробки мережевого трафіку та наявності відкритих портів без належної перевірки.

2. Remote Desktop Services (BlueKeep, CVE-2019-0708) – уразливість у службі RDP, яка дозволяла неавторизоване виконання коду на віддалених комп’ютерах. Спричиняла загрозу масового поширення шкідливого ПЗ.

3. Windows Registry Misconfigurations – помилки в налаштуваннях реєстру, які дозволяють обхід UAC або ескалацію привілеїв.

У Linux розрізняють наступні вразливості [57]:

1. Dirty COW (CVE-2016-5195) – помилка в системному виклику copy-on-write, яка дозволяла локальним користувачам отримати права root, модифікуючи файли, доступ до яких мав бути обмеженим. Ця вразливість існувала понад 9 років до її виявлення.

2. Sudo Vulnerability (CVE-2019-14287) – вразливість у команді sudo, яка дозволяла обхід обмежень і виконання команд з найвищими привілеями навіть без відповідних прав доступу.

3. Shellshock (CVE-2014-6271) – критична вразливість в оболонці Bash, яка дозволяла зловмиснику запускати довільні команди через маніпуляції з environment variables. Вона охоплювала мільйони серверів і вбудованих пристроїв.

Незалежно від типу операційної системи, основними причинами експлуатації вразливостей залишаються:

– несвоєчасне оновлення компонентів ОС;

– недосконаліть механізмів контролю доступу;

– людський фактор (використання стандартних паролів, нехтування політиками безпеки) [49];

– відсутність засобів виявлення та реагування на інциденти.

Усі ці фактори підкреслюють необхідність побудови проактивної системи кіберзахисту, яка поєднує моніторинг, аудит, автоматизовані оновлення та застосування моделей управління ризиками.

1.4 Законодавчі та нормативні акти у сфері кібербезпеки

Забезпечення інформаційної безпеки на глобальному рівні вимагає уніфікованих нормативів, які дають змогу систематизувати підходи до захисту інформаційних ресурсів, незалежно від типу організації, її галузі чи географічного розташування. В цьому контексті провідну роль відіграють міжнародні стандарти, що регламентують вимоги до захищеності інформаційних систем, механізмів управління ризиками, правового регулювання та обробки персональних даних [50].

Серед найбільш авторитетних документів варто виокремити: ISO/IEC 27001, NIST SP 800-53 та General Data Protection Regulation (GDPR).

— ISO/IEC 27001 – міжнародний стандарт системи управління інформаційною безпекою (СУІБ), який визначає вимоги до встановлення, впровадження, моніторингу, аналізу та вдосконалення СУІБ. Орієнтований на системний підхід до управління ризиками інформаційної безпеки.

— NIST SP 800-53 – керівництво Національного інституту стандартів і технологій США щодо вибору та впровадження контролів безпеки у федеральних інформаційних системах. Містить деталізовану структуру захисних заходів за категоріями.

— GDPR (Загальний регламент захисту даних) – регламент Європейського Союзу, який встановлює правила обробки, зберігання та передачі

персональних даних фізичних осіб. Хоча цей документ має правовий характер, він тісно пов'язаний з технічними стандартами безпеки.

Для кращого розуміння відмінностей і взаємодоповнюваності цих документів доцільно проаналізувати їхні ключові положення. Порівняння ключових положень стандартів ISO/IEC 27001, NIST SP 800-53, GDPR представлено у табл. А.5 додатка А.

Зазначені стандарти не виключають одне одного, а в багатьох випадках застосовуються комплексно. Наприклад, компанія може впровадити СУІБ відповідно до ISO/IEC 27001, використовуючи практичні засоби контролю з NIST SP 800-53, при цьому дотримуючись вимог GDPR щодо захисту персональних даних.

Таке поєднання дозволяє формувати надійну, відповідальну та регульовану систему кіберзахисту, що відповідає міжнародним практикам і юридичним вимогам.

Україна, як держава, що активно розвиває цифрову інфраструктуру, постала перед необхідністю створення комплексної нормативно-правової бази для забезпечення кібербезпеки на всіх рівнях – від державного до інституційного. Законодавче регулювання у цій сфері формується з урахуванням міжнародних стандартів та поточної геополітичної ситуації, що обумовлює підвищену увагу до захисту інформаційного простору.

Базовим нормативним актом у сфері кібербезпеки є Закон України «Про основні засади забезпечення кібербезпеки України», ухвалений у 2017 році. Цей документ закріплює засади державної політики у сфері кібербезпеки, визначає основні принципи, напрями, суб’єктів та механізми взаємодії між державними органами, об’єктами критичної інфраструктури, операторами телекомунікацій і недержавними структурами. Закон також містить вимоги до організації системи управління інформаційною безпекою на рівні суб’єктів господарювання, які повинні впроваджувати внутрішні політики захисту, відповідно до рівня критичності їхніх інформаційних ресурсів.

Окрему увагу в законі приділено критичній інформаційній інфраструктурі. Суб'єкти, що відносяться до цієї категорії, зобов'язані забезпечити стійкість, безперервність та відновлюваність роботи своїх інформаційних систем у разі кіберінцидентів. Це, зокрема, передбачає впровадження моніторингових інструментів, систем раннього виявлення загроз, а також обов'язкову звітність перед відповідними державними структурами [51].

Практичні аспекти реалізації положень закону конкретизуються у Постанові Кабінету Міністрів України № 518 від 19 липня 2016 року «Про затвердження Положення про функціонування державної системи кіберзахисту». Цей документ встановлює організаційну структуру, повноваження учасників, порядок реагування на кіберінциденти, а також вимоги до захисту телекомунікаційних мереж та інформаційних систем. У постанові описується функціонування державної системи кіберзахисту, до якої входять Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національний банк, Міністерство оборони та інші уповноважені органи.

Згідно з положеннями постанови, кожен оператор державної або критичної інформаційної інфраструктури зобов'язаний забезпечити реалізацію комплексу заходів: впровадження систем захисту, виявлення вторгнень, сегментування мереж, застосування актуальних оновлень безпеки, ведення журналів подій та обов'язкову взаємодію з національними кіберінституціями. Також визначено процедури інформування державних органів про виявлені загрози чи інциденти, що становлять небезпеку для національної безпеки.

Сукупність зазначених документів формує нормативну базу, яка забезпечує як стратегічне планування, так і оперативне реагування на кіберзагрози. Водночас законодавство України у сфері кібербезпеки перебуває у процесі постійного вдосконалення, зокрема шляхом гармонізації з міжнародними стандартами, такими як ISO/IEC 27001, NIST SP 800-53, а також відповідними директивами Європейського Союзу.

У контексті забезпечення інформаційної безпеки в комп’ютерних мережах важливим елементом правового регулювання виступає захист персональних даних користувачів, працівників, клієнтів і громадян, інформація про яких обробляється у цифровому середовищі. В Україні ця сфера регламентується Законом України «Про захист персональних даних» № 2297-VI від 1 червня 2010 року (із наступними змінами), який визначає правові та організаційні засади обробки персональних даних, а також встановлює обов’язки володільців і розпорядників таких даних.

Згідно з положеннями закону, персональні дані визначаються як відомості або сукупність відомостей про фізичну особу, яка ідентифікована або може бути ідентифікована. Закон передбачає, що обробка персональних даних має здійснюватися виключно з дотриманням принципів законності, справедливості, пропорційності, доцільності та обмеженості строком зберігання. Основою для обробки персональних даних є надання згоди суб’єкта або інша законна підстава, встановлена чинним законодавством.

Закон зобов’язує володільців баз персональних даних впроваджувати організаційно-технічні заходи, спрямовані на захист інформації від несанкціонованого доступу, знищення, випадкової втрати або незаконної обробки. До таких заходів належать: шифрування, контроль доступу, багаторівнева аутентифікація, захист комунікаційних каналів, резервне копіювання тощо. Важливу роль також відіграє обов’язок ведення обліку операцій з даними та повідомлення Уповноваженого Верховної Ради України з прав людини у випадках порушення прав суб’єктів персональних даних [52].

Особливу увагу приділено транскордонному передаванню персональних даних: воно дозволяється лише за умови забезпечення відповідного рівня захисту у країні призначення або при наявності згоди особи. Закон також передбачає санкції за його порушення, включаючи адміністративну та цивільну відповідальність.

Таким чином, Закон «Про захист персональних даних» є важливим інструментом правового забезпечення конфіденційності інформації у сфері

комп’ютерних мереж. Його положення є складовою ширшого комплексу заходів інформаційної безпеки, зокрема у контексті реалізації принципу конфіденційності, який є частиною триєдиної моделі CIA (Confidentiality, Integrity, Availability).

РОЗДІЛ 2 АНАЛІЗ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ЗАХИСТУ ДАНИХ

2.1 Програмне забезпечення для мережевого захисту

У практиці організації захисту комп'ютерних мереж значну роль відіграє програмне забезпечення, що виконує функції міжмережевих екранів (фаєрволів), засобів маршрутизації, виявлення вторгнень, моніторингу активності користувачів та контролю трафіку. Таке програмне забезпечення має підтримувати сучасні протоколи, масштабованість, налаштування політик безпеки, можливості резервування і централізованого керування.

До найпопулярніших на практиці рішень у сфері мережевого захисту належать:

- pfSense – потужний open-source фаєрвол, який підтримує маршрутизацію, VPN, балансування навантаження, IDS/IPS та інші функції корпоративного рівня;
- Cisco ASA (Adaptive Security Appliance) – апаратно-програмний комплекс від Cisco з високим рівнем надійності, орієнтований на середній і великий бізнес;
- Kerio Control – універсальний шлюз безпеки з веб-інтерфейсом, зручний для малого бізнесу та віддаленого адміністрування;
- MikroTik RouterOS – професійна маршрутизуюча операційна система з вбудованим фаєрволом і великою кількістю модулів;
- FortiGate – рішення з інтегрованим захистом від загроз, управлінням додатками, DPI-аналізом та SD-WAN;
- Zentyal – серверна платформа для малого бізнесу з вбудованими модулями мережевого захисту, сумісна з Windows-доменами.

Практичний досвід використання цих рішень показує значні відмінності за функціональністю, гнучкістю конфігурації, продуктивністю та вартістю

впровадження. Наведена нижче таблиця відображає ключові параметри порівняння програмного забезпечення для мережевого захисту [53].

З метою реалізації програмного захисту на рівні шлюзу було обрано open-source рішення pfSense, яке поєднує функції фаєрвола, VPN-сервера, маршрутизатора та засобу керування трафіком. Програмне забезпечення було розгорнуто у віртуальному середовищі з використанням VirtualBox, що дозволяє моделювати реальну мережеву інфраструктуру без додаткових фізичних витрат.

На першому етапі здійснено завантаження дистрибутива pfSense з офіційного сайту проєкту. Встановлення проводилося у віртуальній машині, якій було виділено 2 ядра CPU, 1 ГБ оперативної пам’яті та два мережевих інтерфейси: один у режимі NAT (WAN), інший – у режимі внутрішньої мережі (LAN). Це дозволяє змоделювати повноцінну маршрутизацію між зовнішнім і внутрішнім сегментами мережі.

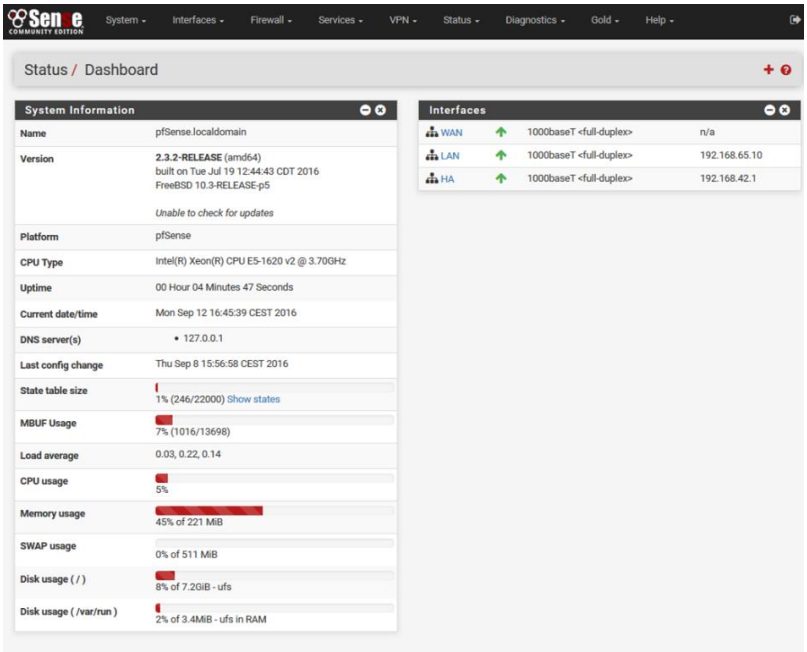


Рисунок 2.1 – Інтерфейс встановлення pfSense у віртуальному середовищі

Після завершення встановлення виконано первинну конфігурацію мережевих інтерфейсів безпосередньо через термінал pfSense. WAN-інтерфейс автоматично отримав IP-адресу від хоста (через NAT), тоді як LAN-інтерфейсу було вручну призначено адресу 192.168.1.1/24, зображено на рис. 2.1.

Після цього було здійснено вхід до веб-інтерфейсу за адресою https://192.168.1.1, де користувачеві запропоновано пройти покроковий майстер налаштування (Setup Wizard). У рамках цього процесу були вказані:

- назва хоста (наприклад, pf.local);
- локальний домен;
- DNS-сервери;
- параметри WAN-підключення (DHCP);
- пароль адміністратора.

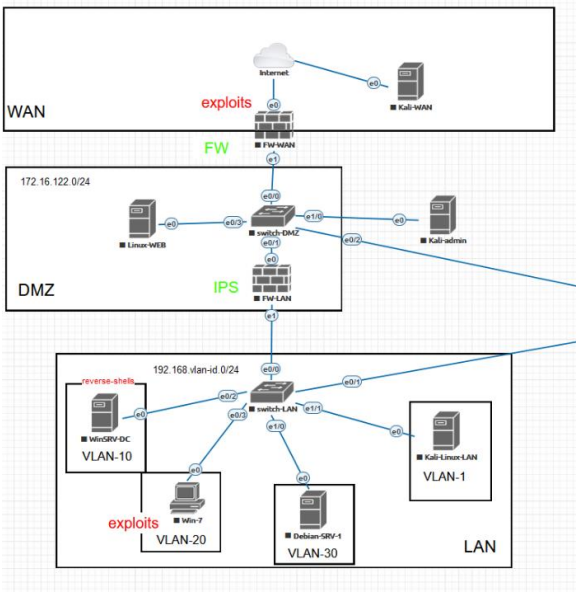


Рисунок 2.2 – Конфігурація мережевого інтерфейсу WAN/LAN у веб-інтерфейсі pfSense

Наступним кроком було увімкнення DHCP-сервера для LAN-мережі, що дозволяє автоматично видавати адреси внутрішнім клієнтам. Для забезпечення безпеки було застосовано правило блокування всіх вхідних підключень на WAN-інтерфейсі та дозвіл лише встановлених з’єднань [25].

В результаті реалізовано ізольовану, захищену мережу з централізованим контролем трафіку, що дозволяє протестувати створення фільтрів, порт-форвардинг, VPN-тунелі та систему виявлення вторгнень (IDS).

Надалі буде виконано налаштування правил фільтрації трафіку з метою практичної реалізації політики доступу відповідно до вимог підприємства.

2.2 Антивірусне програмне забезпечення

Одним із ключових завдань адміністратора безпеки є розробка та впровадження правил фільтрації трафіку, які визначають, які мережеві пакети мають бути дозволені, а які – заблоковані. У межах реалізації функцій міжмережевого екрану (фаєрвола) правила мають певний пріоритет, порядок обробки та логіку спрацювання, що безпосередньо впливає на безпеку та швидкодію системи [54].

У середовищі pfSense усі пакети, що проходять через маршрутизатор, перевіряються за заздалегідь заданими критеріями: IP-адреса джерела і призначення, порт, протокол, інтерфейс та інші параметри. Якщо жодне правило не спрацьовує, пакет блокується за замовчуванням.

Окрім логічної структури правил, важливе значення має і затримка передавання трафіку, яка виникає внаслідок накладних витрат на перевірку, маршрутизацію та фільтрацію. Цей параметр критично важливий для застосувань, де потрібна мінімальна затримка (реального часу, VoIP, відеоконференції) [55].

Затримка обчислюється за наступною формулою:

$$T = \frac{S}{BW} + L\%, \qquad (2.1)$$

де:

- T – загальна затримка передавання (секунди),
- S – розмір пакета (біт),
- BW – пропускна здатність каналу (біт/сек),
- L – додаткова маршрутизуюча затримка (секунди).

Якщо пакет має розмір 1 500 байт (12 000 біт), пропускна здатність каналу становить 10 Мбіт/с, а маршрутизуюча затримка – 2 мс, отримаємо:

$$T = \frac{12000}{10000000} + 0{,}002 = 0{,}0032\text{сек} = 3{,}2\text{мс}$$

Цей показник є прийнятним для більшості стандартних додатків, але при перевищенні 50–100 мс необхідно проводити оптимізацію правил, черговість обробки пакетів або модернізацію обладнання.

На практиці створення правил у pfSense здійснюється через веб-інтерфейс у вкладці Firewall > Rules, де кожне правило має такі параметри: дія (Pass / Block / Reject), інтерфейс, IP-адреси, порти, протокол, опис і логування. Додавання надто великої кількості правил або їх неефективне розташування може вплинути на швидкодію системи.

Антивірусне програмне забезпечення є ключовим компонентом забезпечення захисту кінцевих пристроїв у комп'ютерній мережі. Його основна мета – виявлення, блокування та нейтралізація шкідливих програм до моменту їх активації або під час їх спроби змінити системні файли, ключі реєстру або мережеві налаштування.

У рамках практичного дослідження було відібрано п'ять антивірусних рішень, які широко застосовуються як у корпоративному, так і в приватному секторі. До переліку увійшли:

– ESET Internet Security – антивірус зі збалансованим захистом і низьким навантаженням;

– Avast Free Antivirus – безкоштовне рішення з базовим захистом і великою кількістю додаткових модулів;

– Bitdefender Total Security – багатофункціональний продукт із хмарною аналітикою;

– Microsoft Defender – вбудоване рішення в Windows 10/11, що активно вдосконалюється останніми роками.

З метою порівняння антивіруси було протестовано за такими критеріями [56]:

– рівень виявлення загроз – на основі незалежного тестування AV-Test та AV-Comparatives;

– системне навантаження – використання ресурсів CPU, RAM під час повного сканування;

– частота оновлень сигнатур – інтервал оновлень та швидкість реагування на нові загрози;

– інтеграція з операційною системою – зручність використання, сумісність, автоматизація захисту. Порівняльна характеристика антивірусних рішень представлено в табл. А.6 додатка А.

Як свідчать результати табл. А.6 додатка А, ESET та Bitdefender забезпечують ефективний баланс між захистом і швидкодією, тоді як Kaspersky демонструє найвищий рівень виявлення, проте із помітним навантаженням на ресурси. Microsoft Defender, попри дещо нижчий рівень виявлення, значно покращився останніми роками та став базовим рішенням для захисту систем без додаткових витрат.

На практиці вибір антивіруса залежить від сценарію використання. Наприклад, для підприємств із великою кількістю клієнтських ПК критичним є низьке навантаження, тоді як для фінансових структур пріоритетом є максимальний захист і поведінковий аналіз загроз.

З метою емпіричної оцінки функціональності антивірусного ПЗ було проведено запуск сканування системи на прикладі двох найбільш поширених рішень: ESET Internet Security та Microsoft Defender. Сканування здійснювалося в ізольованому середовищі, що містило тестові загрози типу EICAR-файлів, а також симуляції шкідливих скриптів. Інтерфейси запуску ручного сканування в обох антивірусах представлено на рис. 2.3.

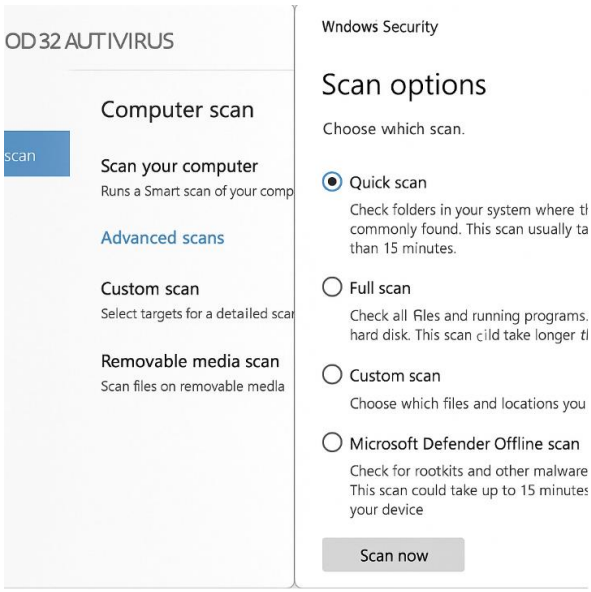


Рисунок 2.3 – Інтерфейс запуску сканування в ESET, Defender

Зліва показано процес вибору об’єктів перевірки у програмі ESET – користувач може обрати окремі диски, папки або зовнішні пристрої, встановити глибину аналізу, застосувати евристичні методи та поведінкову блокаду. Справа зображено вікно Microsoft Defender, де доступні параметри швидкого, повного або вибіркового сканування системи з інтеграцією у Windows Security Center.

В обох випадках запуск сканування потребує мінімальної взаємодії з користувачем, що дозволяє здійснювати захист навіть некваліфікованим працівникам. Обидві системи забезпечують виведення результатів у реальному часі, ведення журналу подій та миттєве ізолювання загроз.

Оцінка ефективності антивірусного програмного забезпечення є ключовим етапом у виборі рішення для впровадження на підприємстві. Основним критерієм оцінки є відсоток виявлення реальних загроз, який дозволяє визначити рівень надійності системи захисту в умовах практичного застосування.

Для розрахунку використовується така формула:

$$E = \frac{N_{\text{виявл.}}}{N_{\text{реальн.}}} \times 100\%, \qquad (2.2)$$

де:

– E – відсоток ефективності сканування,

- $N_{\text{виявл.}}$ – кількість виявлених шкідливих об’єктів,
- $N_{\text{реальн.}}$ – фактична кількість загроз, що були надані на перевірку.

У рамках дослідження було створено тестове середовище з п’ятьма типами загроз [57]:

1. Тестовий файл EICAR;
2. Скрипт-майнер (обфускований PowerShell);
3. Архівований троян типу dropper;
4. Емулятор кейлогера;
5. Шкідливий .doc-файл із макросом VBA.

Кожен антивірус провів повне сканування директорії, де містилися ці об’єкти. Результати сканування п’яти типів вірусів представлені в табл. 2.2.

Таблиця 2.1 – Результати сканування 5 типів вірусів

№	Антивірус	EICAR	Скрипт-майнер	Троян (архів)	Кейлогер	VBA-макрос	Всього виявлено	Ефективність, %
1	ESET	+	+	+	+	+	5	100 %
2	Avast	+	+	–	+	+	4	80 %
3	Kaspersky	+	+	+	+	+	5	100 %
4	Bitdefender	+	+	+	+	–	4	80 %
5	Microsoft Defender	+	–	–	+	+	3	60 %

* *Примітка: знак + означає виявлення та блокування об’єкта, – – не виявлено.*

Джерело: створено автором на основі даних [58]

Результати табл. 2.1 свідчать про те, що найвищий рівень виявлення загроз демонструють ESET та Kaspersky, які виявили всі надані типи шкідливих файлів. Bitdefender продемонстрував хороші результати, однак не розпізнав шкідливий макрос у .doc-файлі. Avast не виявив троян у зашифрованому архіві, а Microsoft Defender, хоч і має покращену функціональність, виявив лише три з п’яти загроз.

У практичному середовищі така різниця може мати критичне значення: навіть одна не виявлена загроза, особливо типу dropper або кейлогера, здатна спричинити втрату даних або компрометацію всієї мережі. Тому вибір

антивіруса має базуватися не лише на рейтингах, а й на результатах тестування у конкретному робочому середовищі.

2.3 Шифрування даних та засоби аутентифікації

У сучасних інформаційних системах шифрування є базовим методом забезпечення конфіденційності даних під час їх зберігання та передавання. Програмні засоби шифрування дозволяють реалізувати захист як для окремих файлів, так і для цілих логічних дисків, тому вони активно використовуються в корпоративних мережах, хмарних сховищах та на мобільних пристроях.

У рамках практичного аналізу було розглянуто та протестовано три поширені рішення: VeraCrypt, AxCrypt і BitLocker. Кожне з них має свої особливості, алгоритми шифрування, рівень інтеграції з операційною системою та призначення.

Таблиця 2.2 – Порівняння програм шифрування даних

№	Програма	Алгоритми шифрування	Інтеграція з ОС	Тип шифрування	Складність налаштування	Призначення
1	VeraCrypt	AES, Serpent, Twofish	Часткова	Повне шифрування дисків, томів	Висока	Захист локальних носіїв
2	AxCrypt	AES-128, AES-256	Інтеграція з Провідником Windows	Шифрування окремих файлів	Низька	Робота з документами, офісними файлами
3	BitLocker	AES	Повна (Windows Pro+)	Шифрування системних дисків	Середня	Корпоративне середовище Windows

Джерело: створено автором на основі даних [61]

VeraCrypt дозволяє створювати зашифровані логічні томи або шифрувати цілі фізичні розділи. Це програмне забезпечення підтримує кілька криптографічних алгоритмів та їх комбінації. Процес налаштування вимагає технічних знань, однак забезпечує високий рівень безпеки. У практичному

середовищі VeraCrypt було використано для створення зашифрованого тому обсягом 4 ГБ на змінному носії.

AxCrypt забезпечує просте та зручне шифрування окремих файлів у середовищі Windows. Його перевагою є інтеграція з контекстним меню Провідника, що дозволяє шифрувати дані в один клік. Підходить для користувачів, які не потребують складних конфігурацій, але прагнуть убезпечити окремі документи.

BitLocker, у свою чергу, є вбудованим рішенням у редакціях Windows Pro та Enterprise. Він забезпечує прозоре шифрування системного диска та підтримує апаратне шифрування на базі TPM. Підходить для централізованого керування політиками безпеки в організаціях.

У межах практичного дослідження було здійснено шифрування логічного тому обсягом 4 ГБ за допомогою програмного забезпечення VeraCrypt. Для цього створено окремий файл-контейнер з вибором алгоритму шифрування (AES, Serpent або Twofish), після чого проведено монтування тому для подальшої роботи з даними. На рис. 2.4 зображено інтерфейс VeraCrypt під час процесу монтування зашифрованого тому.

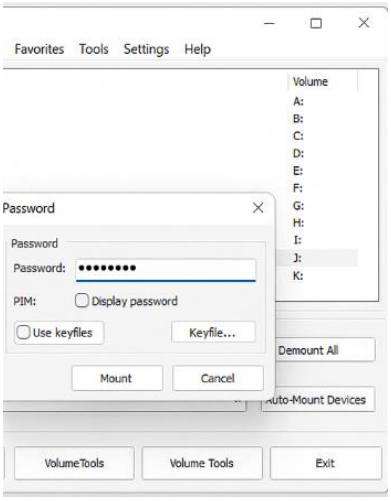


Рисунок 2.4 – Інтерфейс VeraCrypt при монтуванні зашифрованого тому.

Користувач обирає вільну літеру диску, вказує розташування контейнера, вводить пароль і, за потреби, використовує додаткові ключі. Після успішного

монтування том стає доступним у системі як звичайний диск, однак усі дані автоматично шифруються/дешифруються під час запису або читання.

Для оцінки продуктивності було виміряно час повного шифрування 4 ГБ даних із використанням трьох різних алгоритмів. Результати представлені на рис. 2.5. Найменший час показав алгоритм AES (приблизно 7 хв), тоді як Serpent та Twofish виявилися менш ефективними, продемонструвавши 9 та 11 хв відповідно.

Ці результати підтверджують доцільність використання AES як оптимального компромісу між безпекою та швидкодією. Обраний алгоритм шифрування безпосередньо впливає на швидкість доступу до даних, а відтак – на загальну продуктивність інформаційної системи.

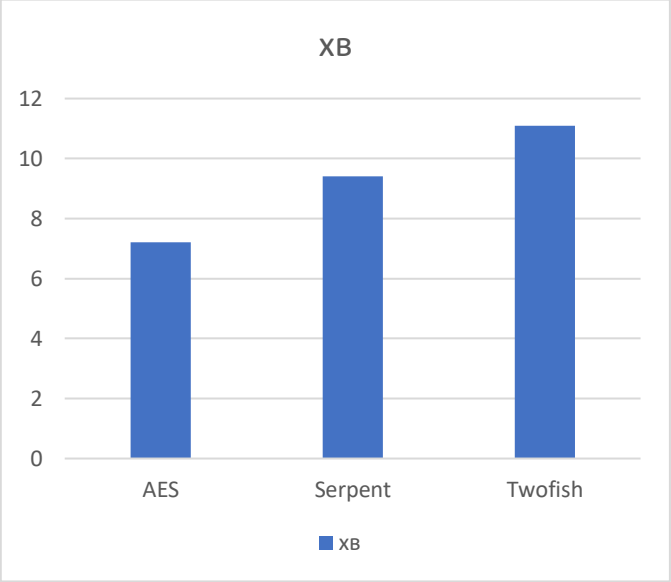


Рисунок 2.5 – Статистика часу шифрування для тома 4 ГБ.

Автентифікація – це процес перевірки особи, яка намагається отримати доступ до комп'ютерної системи або ресурсу. На практиці застосовуються як базові, так і комбіновані методи перевірки користувача, що забезпечують різний рівень безпеки. У сучасних мережах найбільш поширеними є такі методи:

— Парольна аутентифікація – використання статичних секретних комбінацій; поширена, але вразлива до атак типу brute-force або фішингу [62];

— Одноразовий пароль (OTP) – код, який генерується додатком або надсилається на мобільний пристрій і діє впродовж короткого періоду часу;

— Біометрична аутентифікація – використання фізіологічних характеристик користувача (відбиток пальця, розпізнавання обличчя, райдужки тощо);

— USB-ключі безпеки (U2F, YubiKey) – апаратні пристрої, що зберігають криптографічний токен та активуються під час входу.

Кращу безпеку забезпечує комбінована аутентифікація, коли одночасно застосовуються два або більше факторів з різних категорій (знання, володіння, властивість). Найпоширеніший сценарій – це комбінація паролю та OTP-коду.

Для формалізації надійності системи застосовується оцінка ймовірності компрометації, тобто ймовірності того, що зловмисник зможе подолати обидва рівні захисту:

$$P = P_1 \times P_2 \qquad (2.3)$$

де:

- P – ймовірність компрометації всієї системи;
- P_1 – ймовірність зламу або підбору паролю;
- P_2 – ймовірність перехоплення або генерації правильного OTP.

Наприклад, якщо ймовірність вгадати пароль становить 1 до 1 000 (0,001), а згенерувати OTP-код вчасно – 1 до 10 000 (0,0001), то сумарна ймовірність:

$$P = 0{,}001 \times 0{,}0001 = 0{,}0000001 = 0{,}00001\%$$

Це свідчить про значне зниження ризику при використанні двофакторної моделі порівняно з однофакторною. У реальних умовах для ще більшої безпеки додаються апаратні токени, геолокаційні обмеження та поведінковий моніторинг.

2.4 Захист хмарних технологій

Хмарні сервіси стали невіддільною частиною сучасної IT-інфраструктури завдяки доступності, масштабованості та зниженню витрат на локальне обладнання. Однак з перенесенням даних у хмару виникає потреба у посиленому

контролі безпеки: забезпеченні конфіденційності, цілісності, доступності та юридичної відповідності (compliance).

У рамках дослідження були розглянуті чотири найбільш поширені хмарні платформи:

— Google Workspace – корпоративна платформа Google з поштою, хмарним сховищем, офісним пакетом та адмініструванням;

— Microsoft 365 – набір сервісів Microsoft, включаючи OneDrive, Teams, SharePoint та офісні додатки;

— Amazon AWS – хмарна інфраструктура як сервіс (IaaS/PaaS), що дозволяє гнучке управління ресурсами [63];

— Dropbox Business – популярне хмарне сховище з фокусом на зручність спільної роботи.

З метою порівняння безпеки хмарних сервісів було проаналізовано чотири ключові аспекти:

- шифрування даних під час зберігання і передавання;
- резервне копіювання (автоматичне, багаторівневе);
- запобігання витоку даних (DLP);
- багатофакторна аутентифікація (MFA).

Результати таблиці А.7 додатку А свідчать, що всі сервіси реалізують базові вимоги до безпеки, зокрема шифрування і багатофакторну аутентифікацію. Водночас найбільш повну систему контролю витоку даних (DLP) мають Google Workspace, Microsoft 365 та Amazon AWS, які дозволяють створювати політики за ключовими словами, файлами та геолокацією доступу. Dropbox, натомість, більше орієнтований на малий бізнес, тож його DLP-можливості обмежені.

У межах дослідження було протестовано Google Workspace – хмарну платформу Google, що використовується у корпоративному та освітньому середовищі.

На рис. 2.6 продемонстровано сторінку керування безпекою в Google Workspace, де адміністратор або користувач має змогу активувати двоетапну

перевірку (2-Step Verification). Для цього необхідно перейти до розділу «Безпека» → «Двоетапна перевірка», після чого Google запропонує підтвердження пароля та налаштування другого чинника автентифікації. Це може бути SMS-код, push-повідомлення в додатку Google Authenticator, фізичний ключ безпеки або запит на смартфон [64].

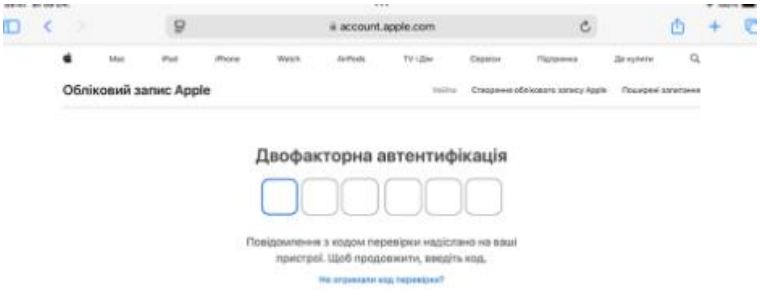


Рисунок 2.6 – Увімкнення двофакторної автентифікації для облікового запису

Наявність двофакторної автентифікації дозволяє значно зменшити ризики, пов’язані з компрометацією облікових даних, особливо у випадках використання слабких паролів або внаслідок фішингових атак.

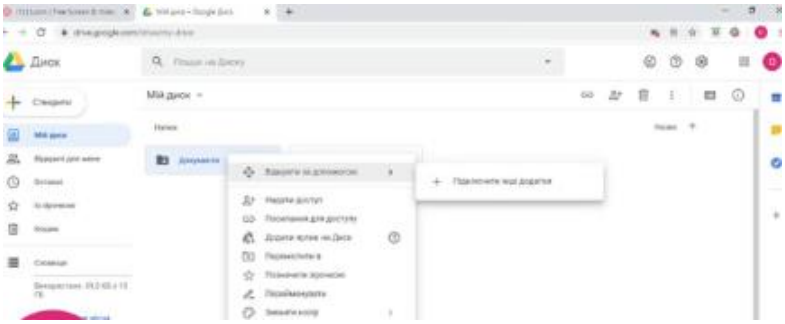


Рисунок 2.7 – Журнал доступу до Google Drive із визначенням геолокації доступу

Другий етап практичного дослідження передбачав перевірку журналу активності користувачів у межах Google Workspace. На зображенні видно доступ до audit-логу, де фіксуються всі сесії входу до облікового запису, включаючи:

- дату і час доступу;
- IP-адресу;
- країну або місто;

– тип пристрою та браузера.

Ця інформація дає змогу виявити аномальні підключення (наприклад, доступи з незвичних геолокацій), а також здійснювати проактивний моніторинг безпеки. Адміністратори можуть налаштувати автоматичне сповіщення у випадку підозрілої активності або несанкціонованого входу.

РОЗДІЛ 3 АНАЛІЗ КОМП'ЮТЕРНОЇ МЕРЕЖІ ТА ЗАХИСТУ ДАНИХ ПІДПРИЄМСТВА

3.1 Опис структури комп'ютерної мережі підприємства

Структура комп'ютерної мережі є одним із ключових елементів інформаційної інфраструктури будь-якого сучасного підприємства, оскільки вона забезпечує безперервність бізнес-процесів, оперативний обмін даними між підрозділами та підтримку взаємодії з зовнішніми контрагентами. У межах практичного аналізу було здійснено поетапне вивчення архітектури локальної мережі підприємства, зокрема конфігурації активного мережевого обладнання, принципів IP-адресації, топології з'єднань, а також розподілу вузлів за функціональним призначенням.

Особливу увагу приділено питанню логічного сегментування мережі, наявності резервних каналів зв'язку та інтеграції елементів безпеки на фізичному й мережевому рівнях. Такий підхід дозволяє не лише комплексно оцінити існуючу модель організації мережевої взаємодії, а й визначити критичні точки, які потенційно можуть стати об'єктами кіберзагроз або спричинити зниження ефективності обробки інформації в межах корпоративного середовища.

Комп'ютерна мережа підприємства демонструє ознаки ієрархічної побудови з частковими елементами сіткової топології, що дає змогу забезпечити підвищену відмовостійкість і гнучкість у процесі адміністрування. Робочі станції, розміщені в окремих підрозділах, підключаються до локальних комутаторів, які, своєю чергою, з'єднані з центральними вузлами, що відповідають за маршрутизацію трафіку та передачу даних до серверів. У структурі також передбачено наявність окремого сервера мережі, що відповідає за внутрішні служби доступу, файл-сервер для зберігання інформаційних ресурсів, а також шлюз до інших мереж, який функціонує як точка взаємодії з Інтернетом або суміжними сегментами.

Наявність спеціалізованого сервера доступу до мережі свідчить про запровадження політик централізованого управління і контролю користувацьких

сесій, що є важливою передумовою для подальшого впровадження комплексної системи захисту. Така архітектура дозволяє здійснювати гнучку маршрутизацію, балансування навантаження та забезпечення резервування критично важливих вузлів, що є особливо актуальним для підприємств із розгалуженою структурою або високим рівнем вимог до доступності IT-сервісів.

На рис. 3.1 представлено структурну схему комп'ютерної мережі підприємства, яка умовно відображає логічну топологію взаємодії ключових вузлів інформаційної інфраструктури. Як видно зі схеми, мережева архітектура побудована з використанням централізованої комутаційної структури, в якій активне мережеве обладнання (позначене як ВК – вузли комутації) виконує роль основи для об'єднання серверного сегменту, робочих станцій, шлюзів зовнішнього доступу та сегментів взаємодії з іншими мережами.

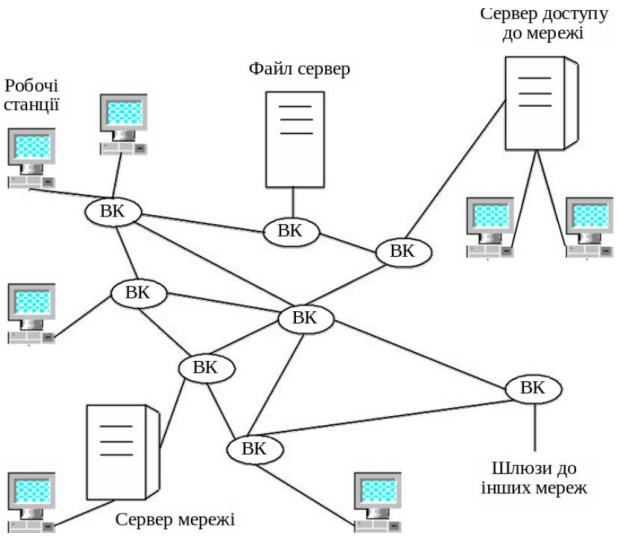


Рисунок 3.1 – Топологія комп'ютерної мережі підприємства

З метою повнішого розуміння логіки побудови мережевої інфраструктури підприємства, доцільним є деталізований аналіз активного та пасивного мережевого обладнання, яке формує фізичну основу взаємодії між вузлами. У таблиці 3.1 наведено узагальнену інформацію щодо основних мережевих пристроїв, що використовуються в структурі комп'ютерної мережі досліджуваного об'єкта, із зазначенням їх типу, моделі, кількості та фізичного розміщення в межах приміщення підприємства або серверної зони.

Таблиця 3.1 – Основні мережеві пристрої підприємства

№	Тип пристрою	Модель/марка	Кількість	Місце встановлення
1	Комутатор рівня 2	Cisco Catalyst 2960	6	Робочі зони, серверна
2	Основний маршрутизатор	MikroTik RB4011	1	Серверна кімната
3	Фаєрвол	FortiGate 60F	1	Між зовнішнім шлюзом і LAN
4	Wi-Fi точка доступу	Ubiquiti UniFi AP-AC-Pro	4	Ключові адміністративні зони
5	Сервер файлів	HP ProLiant DL380 Gen10	1	Серверна кімната
6	Сервер доступу до мережі	Dell PowerEdge R440	1	Серверна кімната
7	Шлюз міжмережевої взаємодії	Cisco ISR 4331	1	Вузол зовнішніх підключень

Аналізуючи дані таблиці 3.1, можна зробити висновок, що підприємство орієнтоване на побудову стабільної, масштабованої та безпечної мережі з використанням перевірених технічних рішень. Упровадження обладнання від провідних виробників (Cisco, Fortinet, HP, Dell) свідчить про прагнення до підвищеної надійності та сумісності компонентів. Присутність спеціалізованого фаєрвола на межі з зовнішніми мережами забезпечує базову лінію оборони від зовнішніх загроз, у той час як внутрішнє розмежування через комутатори й Wi-Fi-точки дає змогу ефективно управляти локальним трафіком і покривати потреби мобільних користувачів .

Окрім цього, очевидною є тенденція до централізації серверних ресурсів – як для зберігання даних, так і для управління доступом, що відкриває перспективи для подальшої віртуалізації інфраструктури або її часткового перенесення в хмарне середовище за умов забезпечення відповідного рівня захисту даних.

На основі структурної схеми мережі підприємства, зображеної на рис. 3.1, а також проведеного аудиту IT-інфраструктури, було здійснено кількісне узагальнення типів підключених пристроїв і користувацьких робочих місць.

Таблиця 3.2 – Кількість робочих місць, серверів, принтерів і точок доступу Wi-Fi на підприємстві

№	Тип пристрою / елемента інфраструктури	Кількість	Примітки
1	Робочі місця користувачів (ПК)	48	Основні офісні працівники в різних відділах
2	Ноутбуки (мобільні робочі місця)	15	Адміністративний персонал та виїзні фахівці
3	Сервери (файлові, доступу, мережі)	3	Централізовано розміщені в серверній кімнаті
4	Мережеві принтери	5	Інтегровані у внутрішню мережу з автоспільним доступом
5	Точки доступу Wi-Fi	4	Покриття для адміністративних та гостьових зон

Дана інформація є критично важливою не лише для оцінювання масштабів навантаження на мережеве середовище, а й для обгрунтування доцільності вибору окремих архітектурних рішень, зокрема – типу комутації, конфігурації шлюзів, кількості серверних інстанцій та зон покриття бездротового доступу. Як видно з табл. 3.2, навантаження на мережеву інфраструктуру є достатньо значним, що пояснює необхідність використання керованих комутаторів і сегментування трафіку для забезпечення стабільності при високій кількості одночасних підключень.

Крім того, помітною є тенденція до часткового переходу на мобільні формати роботи – на що вказує наявність ноутбуків і розвиненої Wi-Fi-мережі, що, своєю чергою, зумовлює потребу в удосконаленні політик доступу та впровадженні додаткових механізмів ідентифікації користувачів.

Значна частка стаціонарних робочих місць також вимагає централізованого управління ресурсами, резервного копіювання даних і адміністрування доступу, що безпосередньо впливає на проектування серверної інфраструктури. У цілому, кількісний розподіл пристроїв демонструє необхідність у чіткому плануванні та подальшій оптимізації мережевих процесів, особливо в контексті масштабування або переходу на гібридну модель роботи.

Одним із визначальних факторів стабільності функціонування корпоративної мережі є надійність зовнішнього каналу зв’язку з Інтернетом, оскільки саме через нього забезпечується доступ до хмарних сервісів,

корпоративних ресурсів, VPN-підключень для віддалених співробітників, а також виконуються комунікаційні завдання – електронна пошта, обмін документами, відеозв'язок тощо. У випадку досліджуваного підприємства підключення до Інтернету здійснюється через провайдера «Укртелеком», який надає послуги на основі оптоволоконної інфраструктури за технологією FTTB (Fiber to the Building).

Основний канал зв'язку реалізовано за допомогою високошвидкісного з'єднання, що підтримує симетричну швидкість передачі та прийому даних на рівні до 1 Гбіт/с, з гарантованим SLA на рівні 99,5% доступності. Додатково підприємство має резервне підключення до альтернативного провайдера – Vodafone Business, що функціонує через зашифрований VPN-канал із мобільною маршрутизацією, який активується автоматично у разі втрати основного каналу.

IP-адресація в мережі організована за змішаним принципом. Для зовнішнього доступу використовується статична публічна IP-адреса, що прив'язана до доменного імені компанії й дозволяє забезпечувати стабільний доступ до внутрішніх ресурсів ззовні (у разі потреби – через захищені порти). У локальному сегменті IP-адреси призначаються динамічно через DHCP-сервер, з попередньо зарезервованими діапазонами для критично важливих вузлів (серверів, мережевих принтерів, комутаторів).

З технічного боку реалізація багаторівневого доступу до зовнішніх ресурсів супроводжується налаштуванням фаєрвола FortiGate з вхідними й вихідними фільтрами, а також застосуванням NAT (Network Address Translation) для підвищення гнучкості маршрутизації. Такий підхід дозволяє поєднувати високий рівень безпеки з максимально можливою швидкістю обміну інформацією, що критично важливо для бізнес-процесів, які мають часову чутливість.

Варто окремо зазначити, що концепція віртуального сегментування суттєво знижує ризики несанкціонованого доступу, дозволяючи реалізувати принцип мінімальних привілеїв на мережевому рівні. Зокрема, усі запити з VLAN 50 до адрес корпоративного сегменту VLAN 10 блокуються фаєрволом за

замовчуванням, тоді як трафік із VLAN 10 має повноцінний доступ до ресурсів мережі та Інтернету відповідно до політик безпеки.

Крім ізоляції користувачів, важливою перевагою є можливість гнучко масштабувати мережу, додаючи нові підрозділи чи функціональні зони без необхідності суттєвих фізичних змін у структурі з'єднань. У разі розширення, достатньо створити додатковий VLAN та налаштувати правила маршрутизації між сегментами на рівні фаєрвола.

На рис. 3.2 візуалізовано логічну схему сегментування мережі підприємства із використанням технології VLAN, що є сучасним інструментом для побудови гнучкої, ізольованої й масштабованої інформаційної інфраструктури. У даному прикладі реалізовано два ключових віртуальних сегменти: VLAN 10 – призначений для підключення основного персоналу (статичні та бездротові робочі станції), та VLAN 50 – виділений гостьовий сегмент, який фізично ізольований від внутрішньої корпоративної мережі і забезпечує лише доступ до Інтернету.

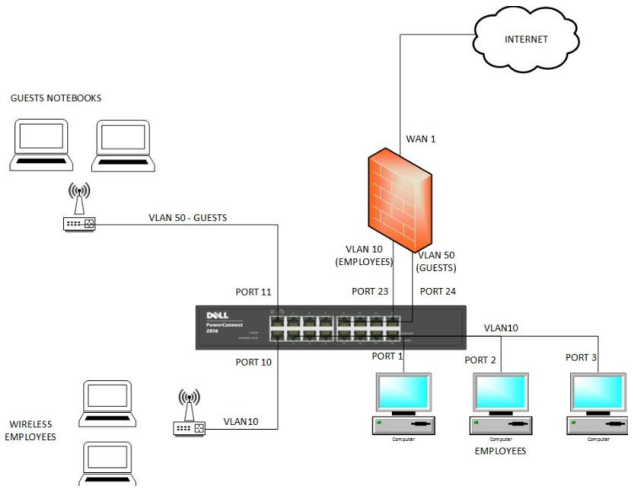


Рисунок 3.2 – Віртуальні сегменти мережі (VLAN), DMZ, гостьові зони

Центральним елементом архітектури виступає комутатор Dell PowerConnect 2816, що підтримує 802.1Q VLAN tagging і дозволяє ефективно розділяти трафік за портами. Порти 1–3 використовуються для проводового підключення штатних працівників до VLAN 10, порт 10 – для Wi-Fi точки доступу для мобільного персоналу, порт 11 – для гостьової бездротової мережі,

а порти 23–24 зарезервовані для взаємодії з фаєрволом і подальшого виходу в глобальну мережу через WAN-інтерфейс. Такий підхід до побудови логічної структури дозволяє не тільки підвищити рівень безпеки, а й значно спростити адміністрування доступів.

Функціонування корпоративної мережі підприємства неможливе без чіткого узгодження набору базових протоколів і мережевих служб, які забезпечують як обмін даними всередині локального середовища, так і вихід до зовнішніх ресурсів. У ході дослідження було ідентифіковано перелік протоколів, що активно використовуються в інфраструктурі досліджуваного підприємства, кожен із яких виконує специфічну функціональну роль у забезпеченні надійності, гнучкості та керованості інформаційного простору.

Однією з базових служб є DHCP (Dynamic Host Configuration Protocol), яка автоматизує процес призначення IP-адрес для кінцевих пристроїв. Вона забезпечує централізований контроль за IP-адресацією в рамках кожного VLAN-сегмента (зокрема VLAN 10 і VLAN 50), з попередньо визначеними діапазонами, виключеннями й фіксованими адресами для критичних вузлів (серверів, принтерів, Wi-Fi-точок). Відповідна служба розміщена на сервері доступу, а інтерфейс адміністрування дозволяє оперативно змінювати параметри з розмежуванням прав доступу.

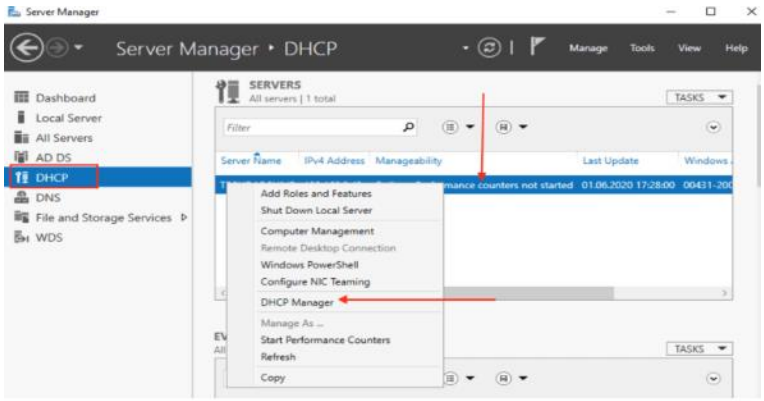


Рисунок 3.3 – Інтерфейс налаштування DHCP-серверу (Windows Server 2019)

Інтерфейс налаштування DHCP-серверу представлено на рис. 3.3, на якому можна побачити консоль керування DHCP, де видно структуру DHCP-сервера з розгорнутими розділами «Address Pool» та «Reservations». У розділі «Address Pool» відображається діапазон IP-адрес, призначених для автоматичного розподілу серед клієнтів мережі. Розділ «Reservations» містить список зарезервованих IP-адрес, які постійно призначаються конкретним пристроям на основі їх MAC-адрес. Це забезпечує стабільність мережевих підключень для критично важливих ресурсів, таких як сервери, принтери та мережеві пристрої.

Використання таких резервувань дозволяє уникнути конфліктів IP-адрес та забезпечує передбачуваність у мережевому середовищі, що є особливо важливим для підтримки безперебійної роботи корпоративної інфраструктури.

Крім того, у мережі функціонує DNS (Domain Name System), що забезпечує трансляцію доменних імен у відповідні IP-адреси в межах внутрішнього сегменту. Локальний DNS-сервер використовується для прискорення внутрішнього запиту до служб (файлового сховища, CRM, ERP), а також для кешування зовнішніх запитів з метою зменшення затримок під час роботи з хмарними сервісами.

Ще одним ключовим компонентом є NAT (Network Address Translation), який реалізовано на фаєрволі FortiGate. Завдяки NAT забезпечується перетворення внутрішніх приватних IP-адрес у зовнішню публічну адресу для виходу в Інтернет, що дозволяє приховати реальну структуру мережі та підвищити її захищеність. Усі правила NAT створені на основі принципу обмеження доступу до лише необхідних портів (зокрема HTTP/HTTPS, SMTP, VPN), з логуванням активності для подальшого аудиту.

На рис. 3.4 представлено інтерфейс налаштування політики NAT у фаєрволі FortiGate. У розділі “Policy & Objects” вибрано підрозділ “IPv4 Policy”, де створюється нова політика з вказанням вхідного та вихідного інтерфейсів, джерела та призначення трафіку, а також служб, до яких застосовується політика.

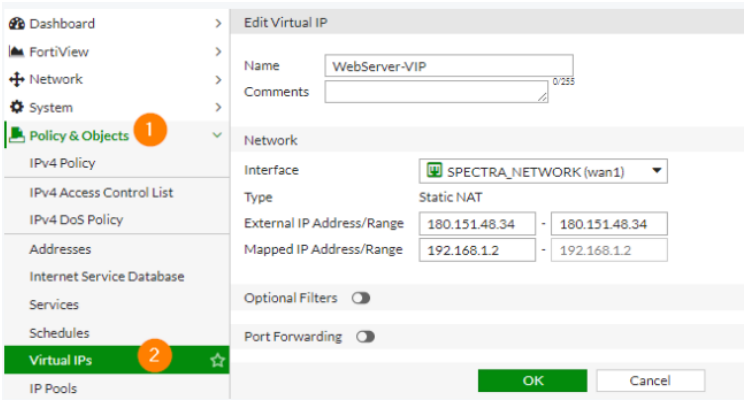


Рисунок 3.4 – Налаштування політик NAT на фаєрволі FortiGate

У секції «Firewall / Network Options» активовано опцію «NAT», що дозволяє здійснювати трансляцію мережевих адрес. Це забезпечує можливість внутрішнім користувачам отримувати доступ до зовнішніх ресурсів Інтернету, використовуючи публічну IP-адресу, призначену зовнішньому інтерфейсу фаєрвола.

Таке налаштування є типовим для організацій, які прагнуть забезпечити безпечний та контрольований доступ до Інтернету для своїх співробітників, зберігаючи при цьому внутрішню мережеву інфраструктуру ізольованою від зовнішніх загроз.

Для віддаленого доступу співробітників до внутрішніх ресурсів використовується VPN (Virtual Private Network) – зашифрований тунель, який базується на протоколі IPsec, із попередньо налаштованими профілями користувачів і автентифікацією за принципом двофакторного підтвердження. VPN-з’єднання дозволяє працівникам безпечно підключатися до серверів підприємства з віддалених локацій, не ризикуючи розкриттям даних у відкритому каналі.

З метою технічного обслуговування серверного парку та віддаленого адміністрування застосовується RDP (Remote Desktop Protocol) – з обмеженням доступу лише до внутрішнього сегмента мережі, із застосуванням політик обмеження IP-діапазонів та регламентованого часу підключення. Окремі сервери мають активовані журнали RDP-підключень, що уможливлює аудит дій адміністратора.

Отже, здійснений аналіз структури комп'ютерної мережі підприємства засвідчив, що її архітектура побудована на принципах логічного сегментування, централізованого керування та багаторівневого доступу. Поєднання статичних і динамічних підключень, використання VLAN-сегментів, наявність окремої гостьової зони, резервованих IP-адрес і сучасних мережевих протоколів свідчить про раціональний підхід до організації IT-інфраструктури. Така модель забезпечує високу масштабованість, відмовостійкість і передумови для впровадження більш складних політик інформаційної безпеки в наступних рівнях мережевої взаємодії.

3.2. Методи захисту даних, що використовуються на підприємстві

Захист інформаційних ресурсів у межах підприємницької діяльності вже давно вийшов за межі суто технічного завдання, перетворившись на невід'ємний елемент загальної системи корпоративного управління ризиками. В умовах постійного зростання кіберзагроз, підвищеної регуляторної відповідальності та збільшення обсягів конфіденційної інформації, яка обробляється в цифровому середовищі, особливого значення набуває впровадження багаторівневих методів захисту даних.

На підприємстві впроваджено багаторівневу систему антивірусного захисту, що поєднує корпоративні та вбудовані рішення. Основним інструментом є ESET Endpoint Security, який забезпечує комплексний захист робочих станцій і серверів. Його функціонал включає захист у реальному часі, антифішинг, брандмауер, контроль пристроїв та веб-фільтрацію. Програмне забезпечення для антивірусного захисту представлено в табл. 3.3.

Для додаткового захисту використовується Malwarebytes Premium, який спеціалізується на виявленні шкідливого програмного забезпечення, захисті від експлойтів та поведінковому аналізі. Цей інструмент встановлено на критично важливих системах, що обробляють конфіденційні дані.

Таблиця 3.3 – Програмне забезпечення для антивірусного захисту

№	Назва ПЗ	Тип	Основні функції	Охоплення пристроїв
1	ESET Endpoint Security	Корпоративний	Захист у реальному часі, антифішинг, брандмауер, контроль пристроїв, веб-фільтрація	100%
2	Microsoft Defender	Вбудований у Windows	Базовий захист у реальному часі, інтеграція з Windows Security Center	100%
3	Malwarebytes Premium	Додатковий	Виявлення шкідливого ПЗ, захист від експлойтів, поведінковий аналіз	30%

Всі пристрої мають активований Microsoft Defender, який забезпечує базовий рівень захисту та інтегрується з Windows Security Center для централізованого моніторингу. На рисунку 3.5 подано фрагмент вікна «Диспетчер задач» операційної системи Windows, який ілюструє перелік активних процесів, що функціонують у фоновому режимі на робочій станції користувача. Серед них помітні сервіси, пов’язані з Adobe, системним середовищем Windows та службою віддаленого доступу AnyDesk, що потенційно може бути використаною як інструмент адміністрування або канал підвищеного ризику при неналежній конфігурації.

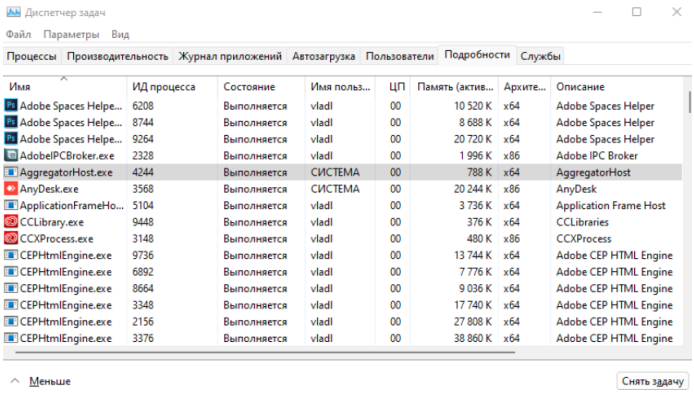


Рисунок 3.5 – Активні процеси антивірусного та захисного ПЗ у середовищі Windows

Однак специфічних процесів, які б прямо свідчили про активність ESET Endpoint Security, на зображенні не ідентифіковано – що, ймовірно, пояснюється

налаштуванням приховування служб або обмеженим рівнем прав користувача для перегляду системних служб.

Такий фрагмент може бути корисним як приклад індикаторного моніторингу активних завдань, особливо в контексті виявлення сторонніх утиліт або підозрілих компонентів, які потенційно несуть загрозу для цілісності даних або цільового втручання в інфраструктуру.

Системи міжмережевого екранування є одним із базових інструментів захисту корпоративної мережі, оскільки забезпечують фільтрацію трафіку, контроль з'єднань між внутрішніми та зовнішніми сегментами, а також виконання політик доступу до мережевих сервісів. На досліджуваному підприємстві застосовується гібридна модель фаєрволів, яка поєднує апаратне рішення на базі FortiGate 60F та вбудовані програмні засоби Windows Firewall на рівні окремих кінцевих пристроїв.

Апаратний фаєрвол FortiGate виконує роль основного шлюзу безпеки, розташованого між внутрішньою мережею та глобальним Інтернетом. Його конфігурація передбачає створення окремих політик для кожного сегмента VLAN (зокрема VLAN 10 – співробітники, VLAN 50 – гостьова зона) із вказанням дозволених протоколів, портів, джерел та цільових адрес. Додатково застосовуються механізми NAT, DPI (Deep Packet Inspection) та фільтрація за категоріями веб-сайтів, що дозволяє автоматично блокувати шкідливі або небажані ресурси.

На рівні кінцевих точок Windows Firewall використовується у стандартному режимі з додатковими користувацькими правилами – наприклад, блокування вхідних з'єднань для необладнаних робочих місць або дозвіл на підключення лише з певного IP-діапазону адміністративної мережі. Така подвійна модель дозволяє реалізувати зонування і послідовну перевірку трафіку як на рівні мережі, так і на рівні пристроїв.

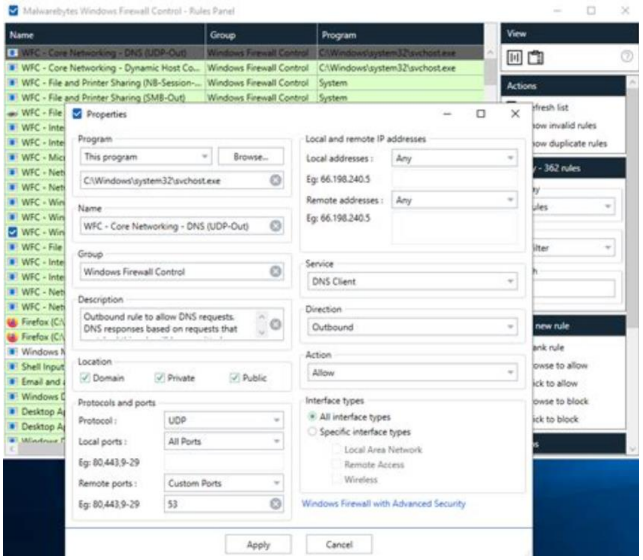


Рисунок 3.6 – Приклад правил фаєрвола у Windows

На рис. 3.6 зображено приклад налаштувань вхідних правил у середовищі Windows Firewall. У представленому фрагменті видно активовані політики для обробки вхідних з’єднань, які фільтруються відповідно до типу трафіку, назви застосунку або порту. Окремі правила мають вказану дію (дозволити / блокувати), а також статус активності – що дозволяє IT-відділу здійснювати моніторинг і адаптивне налаштування в реальному часі.

Комбінація апаратного фаєрвола з централізованим керуванням політиками доступу та програмного екрану на кінцевих точках створює багаторівневу модель мережевого захисту, яка значно знижує ризики як внутрішнього, так і зовнішнього несанкціонованого доступу до цифрових ресурсів підприємства.

Ефективна система аутентифікації та авторизації є не лише технічним інструментом, а й складовою культури інформаційної безпеки підприємства. В умовах, коли значна частина операцій виконується в цифровому середовищі, питання контролю доступу до ресурсів потребує ретельного і структурованого підходу. У досліджуваному підприємстві реалізовано комбіновану модель, яка поєднує централізоване управління через Active Directory, підтримку LDAP-протоколу для інтеграції з окремими сервісами, а також елементи двофакторної автентифікації (2FA) для критичних вузлів. В табл. 3.4 показано засоби аутентифікації та авторизації користувачів.

Таблиця 3.4 – Засоби аутентифікації та авторизації користувачів

№	Система / метод	Призначення	Сфера застосування
1	Active Directory (AD)	Централізоване управління обліковими записами, групами	Усі користувачі локальної мережі
2	LDAP	Протокол доступу до довідників користувачів	Інтеграція із CRM та зовнішніми порталами
3	2FA (OTP, Push)	Двофакторна автентифікація для адміністраторів і серверів	Сервери, VPN, адмін-доступ до файлових систем
4	Політики паролів	Примусове використання складних паролів, автооновлення	Усі облікові записи, згідно з політиками GPO

У межах реалізованої архітектури Active Directory використовується для централізованого адміністрування облікових записів, що дозволяє ефективно управляти правами доступу, контролювати групові політики (GPO) та впроваджувати єдині стандарти безпеки. Інтеграція з LDAP-сумісними сервісами дає змогу автоматизувати синхронізацію з внутрішніми порталами, CRM-системами, а також забезпечити розширену гнучкість у розмежуванні прав.

Важливим компонентом сучасної моделі захисту є використання 2FA – зокрема, одноразових кодів (OTP) або push-повідомлень через спеціальні додатки. Двофакторна автентифікація впроваджена для VPN-з’єднань, доступу до серверів та для користувачів із підвищеними правами, що знижує ймовірність компрометації облікового запису навіть у разі витоку пароля.

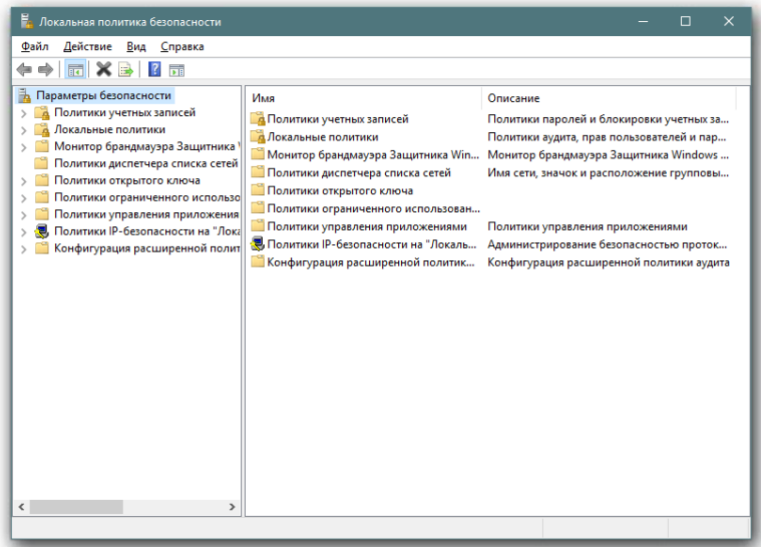


Рисунок 3.7 – Приклад політики безпеки користувачів у Windows Server (GPO)

На рис. 3.7 зображено приклад реалізації політики паролів у середовищі Windows Server за допомогою групової політики (Group Policy Object). Зокрема, визначено мінімальну довжину пароля, необхідність використання складних символів та періодичність зміни пароля. Такі налаштування встановлюються централізовано на рівні домену та забезпечують дотримання єдиних стандартів безпеки для всіх користувачів мережі.

Впровадження зазначених інструментів дозволяє підприємству дотримуватися принципу розмежування доступу, контролювати привілеї, зменшувати ризики зловживань і водночас – підвищувати загальну стійкість системи до зовнішніх і внутрішніх загроз.

У системі захисту інформаційної інфраструктури будь-якого підприємства ключову роль відіграють механізми аутентифікації та авторизації, що безпосередньо впливають на рівень контрольованості доступу до критичних ресурсів. У рамках даного дослідження було проаналізовано підходи, що застосовуються на підприємстві для ідентифікації користувачів, визначення рівня їхніх прав та запобігання несанкціонованому доступу як зсередини, так і ззовні локальної мережі.

Система управління обліковими записами реалізована на базі Active Directory (AD), що дозволяє централізовано адмініструвати доступ до домену, файлових систем, мережевих принтерів, поштових сервісів та інших інтегрованих ресурсів. Доповненням до AD є LDAP-протокол, який використовується для синхронізації з внутрішніми сервісами, зокрема CRM та базами персоналу. Водночас для підвищення стійкості до компрометації облікових даних, на підприємстві впроваджено двофакторну автентифікацію (2FA) для окремих категорій користувачів – насамперед, адміністраторів, бухгалтерії та IT-відділу.

Реалізація політики на рівні групових політик (GPO) дозволяє примусово застосовувати єдині вимоги до паролів: мінімальна довжина – 10 символів, обов’язкове використання цифр, літер різного регістру та спеціальних символів, а також обмеження на повторне використання попередніх паролів. Визначено

термін обов’язкової зміни – кожні 60 днів, з автоматичним повідомленням за 7 днів до завершення строку дії.

Таблиця 3.5 – Системи аутентифікації та авторизації, що застосовуються на підприємстві

№	Система / метод	Призначення	Область застосування
1	Active Directory (AD)	Централізоване керування обліковими записами, політиками	Вся доменна мережа
2	LDAP	Синхронізація даних користувачів із внутрішніми сервісами	CRM, HR-система, доступ до документації
3	2FA (двофакторна)	Захист критичних систем через OTP або мобільні токени	Сервери, VPN, віддалений доступ
4	Парольні політики	Мінімальна довжина, складність, періодичність зміни	Усі облікові записи у домені (через GPO)

На рисунку 3.8 зображено фрагмент інтерфейсу локальної політики безпеки, який дозволяє системному адміністратору визначити параметри облікових записів користувачів. Зокрема, видно налаштування для політики паролів – мінімальна довжина, строк дії, вимоги до складності – а також розділ політики блокування облікового запису, що активується при перевищенні заданої кількості невдалих спроб входу.

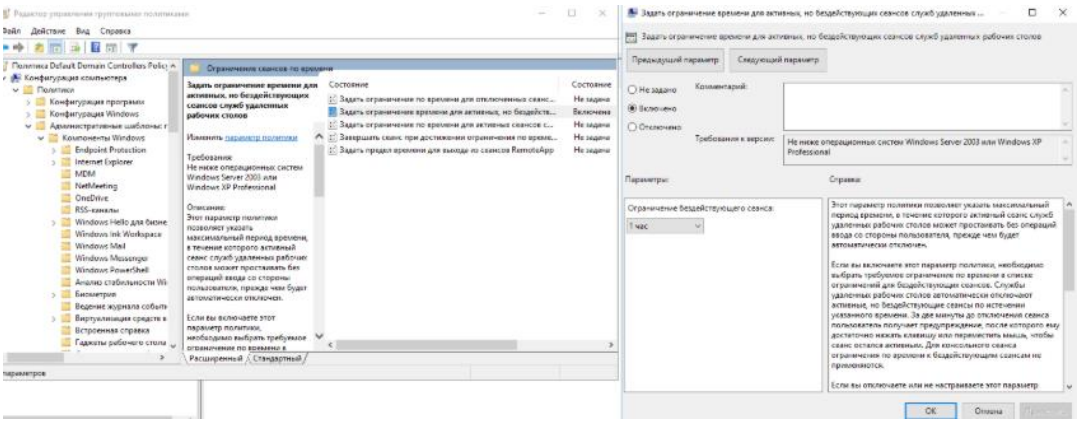


Рисунок 3.8 – Інтерфейс налаштування політики безпеки користувачів у Windows Server (GPO)

Комплексний підхід, що базується на поєднанні технічних інструментів, централізованого адміністрування й політик корпоративної безпеки, дозволяє значно знизити вірогідність несанкціонованого доступу до внутрішніх ресурсів підприємства. Водночас система залишається гнучкою до змін структури

персоналу, організаційних реорганізацій або масштабування мережі, зберігаючи керованість і відповідність сучасним вимогам інформаційної безпеки.

Система резервного копіювання є одним із ключових елементів забезпечення безперервності бізнес-процесів і захисту критично важливої інформації від втрат унаслідок технічних збоїв, атак зловмисників або людського фактору. У ході аналізу було встановлено, що на досліджуваному підприємстві функціонує багаторівнева стратегія створення резервних копій, що поєднує локальне зберігання на окремих фізичних носіях та віддалене хмарне копіювання з використанням спеціалізованого програмного забезпечення.

Таблиця 3.6 – Характеристика системи резервного копіювання даних на підприємстві

№	Параметр	Значення
1	Програмне забезпечення	Acronis Cyber Protect, Veeam Backup & Replication
2	Метод копіювання	Гібридний: локальні NAS-сховища + хмара (Google Cloud)
3	Частота резервування	Щоденне – критичні сервери, щотижневе – робочі станції
4	Тип бекапу	Диференціальний з періодичним повним копіюванням
5	Період зберігання	30 днів (робочі), 90 днів (сервери)
6	Повідомлення / звіти	Автоматичні email-нотифікації + звіти в адміністративну консоль

На практиці найбільш критичні дані – такі як бухгалтерські архіви, CRM-база клієнтів, внутрішні документообіги – резервуються щоденно з вечірнім розкладом. Копії зберігаються як на локальному сервері NAS із захищеним доступом, так і на віддаленому сервері в хмарному середовищі, що дозволяє гарантувати збереження навіть у разі фізичної втрати обладнання. Програмне забезпечення Acronis використовується для централізованого керування політиками резервування, тоді як Veeam інтегровано з віртуалізованим середовищем для копіювання вмісту серверів у режимі «гарячого стану».

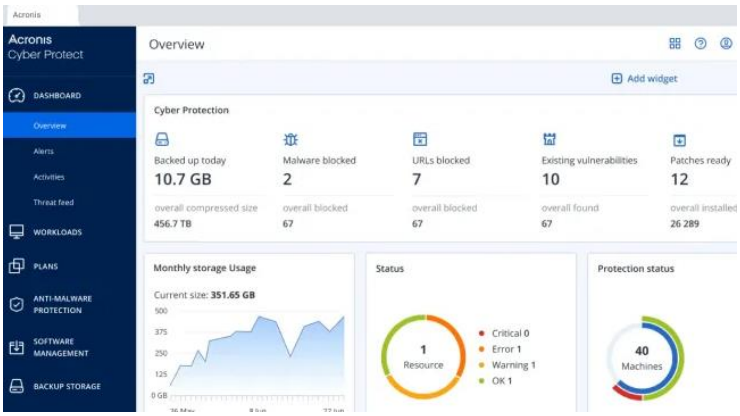


Рисунок 3.9 – Скріншот звіту про стан резервного копіювання (Acronis Cyber Protect)

На рисунку 3.9 представлено типовий звіт з адміністративної панелі Acronis Cyber Protect, який відображає статус останніх резервних копій, включаючи дату, тривалість процесу, обсяг даних та підсумковий результат (успішно / з помилками). Така візуалізація дозволяє ІТ-відділу оперативно контролювати стан резервування, своєчасно виявляти критичні збої та, у разі потреби, ініціювати відновлення з обраної точки.

Використання гібридного підходу до резервного копіювання, із залученням як локальних, так і хмарних компонентів, значно підвищує надійність системи збереження корпоративних даних і створює основу для швидкого реагування у випадку інформаційних інцидентів або аварійних ситуацій.

Отже, аналіз наявних методів захисту даних на підприємстві засвідчив високий рівень технологічної зрілості впроваджених рішень, які охоплюють як мережевий, так і прикладний рівень безпеки. Комбінація антивірусного ПЗ корпоративного класу, використання фаєрволів різної природи, централізованих систем аутентифікації з підтримкою двофакторного доступу, а також чітко регламентованої системи резервного копіювання створює комплексне середовище протидії основним кіберзагрозам. Така модель не лише відповідає сучасним вимогам до захисту інформаційних ресурсів, а й забезпечує сталу роботу критичних бізнес-процесів навіть в умовах потенційних інцидентів інформаційної безпеки.

3.3 Аналіз загроз та вразливостей комп’ютерної мережі

Оцінювання актуальних загроз і виявлення вразливостей у комп’ютерній мережі підприємства є критично важливим етапом формування ефективної стратегії кіберзахисту. У сучасному інформаційному середовищі, яке характеризується високою динамікою ризиків і зростанням кількості цілеспрямованих атак, навіть незначна прорахована вразливість може призвести до масштабних наслідків – від витоку конфіденційних даних до повної зупинки бізнес-процесів.

У цьому підпункті здійснено системний аналіз технічного стану мережевої інфраструктури підприємства з акцентом на типові вектори загроз, рівень захищеності окремих компонентів, наявність неактуалізованого програмного забезпечення та інші критичні чинники, що можуть бути використані потенційним зловмисником для реалізації атаки.

У межах комплексної перевірки інформаційної безпеки досліджуваного підприємства було проведено інвентаризацію ключових елементів мережевої інфраструктури з метою виявлення їхньої технічної вразливості. Особливу увагу приділено пристроям, які забезпечують критичні функції – зокрема, маршрутизаторам, комутаторам, файловим серверам, а також кінцевим точкам доступу користувачів. Для аналізу поточного стану безпеки застосовувався інструментарій автоматизованого сканування – Nessus Essentials – який дозволив здійснити оцінку оновлень ОС, виявити незахищені відкриті порти, застарілі версії служб, а також потенційні конфігураційні помилки.

Як видно з таблиці 3.7, більшість критичних вразливостей пов’язані з відсутністю регулярного оновлення операційних систем або прошивок, а також із залишенням активними застарілих протоколів і портів, що вже не рекомендовані до використання (наприклад, Telnet). Особливої уваги потребують мережеві пристрої, яким не було оновлено прошивку протягом тривалого часу, – оскільки саме вони формують основу всієї внутрішньої

маршрутизації та передавання трафіку, потенційно створюючи умови для вертикального розвитку атаки.

Таблиця 3.7 – Перелік пристроїв з виявленими критичними вразливостями

№	Пристрій / сегмент	Операційна система / ПЗ	Тип вразливості	Рівень ризику	Коментар
1	Файловий сервер (192.168.1.10)	Windows Server 2012 R2	Відсутність оновлень безпеки KB5012670	Високий	Останнє оновлення понад 90 днів тому
2	Комутатор D-Link DES-1210	Firmware 3.10.002	Відкритий Telnet-порт	Високий	Необхідно вимкнути Telnet
3	Робоча станція (відділ кадрів)	Windows 10 Pro (1909)	Застаріла версія ОС	Середній	Не підтримується з січня 2023 року
4	Wi-Fi точка UniFi AP	Firmware 4.0.69	Недійсний сертифікат SSL	Високий	Може бути використано для MITM-атак
5	Сервер CRM (192.168.1.17)	Ubuntu Server 18.04	Вразливість в Apache 2.4.29	Високий	CVE-2021-41773

На рис. 3.10 представлено фрагмент типового звіту після сканування внутрішньої мережі підприємства за допомогою інструменту Nessus. У таблиці результатів відображено список пристроїв, IP-адрес, тип вразливості, опис і присвоєний рівень загрози. Крім того, система надає рекомендації щодо усунення проблеми, що суттєво полегшує подальше впровадження заходів реагування.

Рисунок 3.10 – Сканування мережі на вразливості засобом Nessus

Інвентаризація вразливих елементів дозволяє сформувати об’єктивну картину стану інформаційної безпеки в межах локального середовища й закладає основу для пріоритизації оновлень, закриття зайвих служб і формування адаптивної системи моніторингу.

У рамках комплексного аудиту безпеки досліджуваної мережевої інфраструктури було проведено базове тестування на проникнення (penetration testing), що дало змогу змоделювати реальні сценарії можливих атак і оцінити рівень стійкості системи до спроб несанкціонованого доступу. Тестування виконувалося за методологією "чорної скриньки" (black-box) з обмеженим доступом до внутрішньої інформації, що дозволило об'єктивно імітувати дії умовного зловмисника без прав адміністратора.

У ході симуляції були реалізовані декілька ключових сценаріїв:

1. Сканування портів і служб – за допомогою утиліт `Nmap` та `Unicornscan` вдалося виявити активні сервіси на портах 21 (FTP), 80 (HTTP), 443 (HTTPS), 445 (SMB) та 3389 (RDP), частина з яких мала налаштування за замовчуванням.

2. Brute-force атака на RDP – через сервіс 3389 (віддалений робочий стіл) було змодельовано спробу підбору облікових даних із використанням відкритих словників (інструмент `Hydra`). Після кількох спроб система зафіксувала підозрілу активність і автоматично заблокувала IP-адресу джерела.

3. Експлуатація відомої вразливості в Apache показано на рис.3.11 – уразливий веб-сервер Apache 2.4.29 на одній із віртуальних машин був схильний до впливу вразливості CVE-2021-41773, яка дозволяє обхід шляху доступу (`path traversal`). Після успішної симуляції атаки вдалося отримати доступ до файлів за межами кореневого каталогу.

```
[*] Target detected: Apache/2.4.29 (Ubuntu)
[+] Vulnerable to CVE-2021-41773 - directory traversal confirmed
[+] Accessing /etc/passwd ...
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
...
```

Рисунок 3.11 – Приклад експлуатації відомої вразливості в Apache

Підсумковий звіт показав, що попри загальну стабільність інфраструктури, в системі залишаються технічні «точки входу», які можуть бути використані зловмисниками у разі недостатньої уваги до регулярного оновлення компонентів ПЗ, перегляду налаштувань служб за замовчуванням і відсутності багаторівневого моніторингу. Особливо критичним виявився доступ до вразливого веб-сервера, що функціонував без обмежень у доступі ззовні – це може бути легко виправлено шляхом зміни конфігурації та оновлення версії програмного забезпечення.

Результати тестування на проникнення дозволили не лише виявити конкретні вразливості, а й продемонструвати важливість впровадження постійного процесу перевірки стійкості системи, який має супроводжуватися як технічними, так і організаційними змінами у підходах до інформаційної безпеки.

У процесі функціонування інформаційної системи підприємства неминуче виникає певний рівень ризику, пов’язаний із як зовнішніми, так і внутрішніми загрозами, що можуть спричинити порушення конфіденційності, цілісності або доступності даних. Незалежно від типу бізнесу чи масштабу організації, спектр загроз залишається універсальним, хоча рівень їх критичності варіюється залежно від обсягу оброблюваної інформації, стану інфраструктури та підготовленості персоналу. У межах даного підпункту проведено систематизацію найбільш імовірних загроз для досліджуваного підприємства, із виокремленням їхніх потенційних наслідків та частоти виявлення.

Таблиця 3.8 – Типові загрози для інформаційної системи підприємства

№	Тип загрози	Характер впливу	Ймовірність	Потенційні наслідки
1	Фішинг	Отримання доступу до облікових даних користувачів	Висока	Компрометація облікових записів, витік даних
2	DDoS-атаки	Перевантаження каналів, недоступність сервісів	Середня	Перерва в обслуговуванні клієнтів
3	Шкідливе ПЗ (malware)	Пошкодження даних, несанкціонований контроль	Середня	Втрата інформації, фінансові збитки
4	Витік конфіденційних даних	Несанкціонований експорт або копіювання даних	Середня	Порушення регламентів, штрафи, репутаційні втрати
5	Внутрішні порушення	Помилки або зловживання з боку співробітників	Низька	Викривлення звітності, втручання в IT-системи

Аналіз наявних загроз свідчить, що найбільш поширеною формою атаки залишається фішинг, який здійснюється через електронну пошту або підроблені веб-сайти, з використанням соціальної інженерії для викрадення паролів. Цей тип загрози часто не потребує складних технічних інструментів і націлений безпосередньо на користувача, що робить його особливо небезпечним у середовищі з низьким рівнем кібергігієни.

DDoS-атаки не фіксувалися у критичних масштабах, однак упродовж останнього року було зафіксовано кілька випадків аномальної активності, які можна трактувати як спроби перевантаження вхідного трафіку. Шкідливе програмне забезпечення найчастіше проникає у внутрішню мережу через заражені вкладення або зовнішні носії, тому питання обмеження доступу до USB-портів залишається актуальним.

Рис. 3.12 демонструє кількісний розподіл основних типів інцидентів, які були виявлені службою інформаційної безпеки протягом останнього року. Як видно з графіка, найвищий пік зафіксовано за фішинговими атаками, що відповідає глобальним тенденціям, які свідчать про зростання соціально орієнтованих загроз на фоні посиленої автоматизації технічного захисту. Частка інфікувань шкідливим ПЗ переважно стосувалася робочих станцій співробітників відділу кадрів та бухгалтерії.

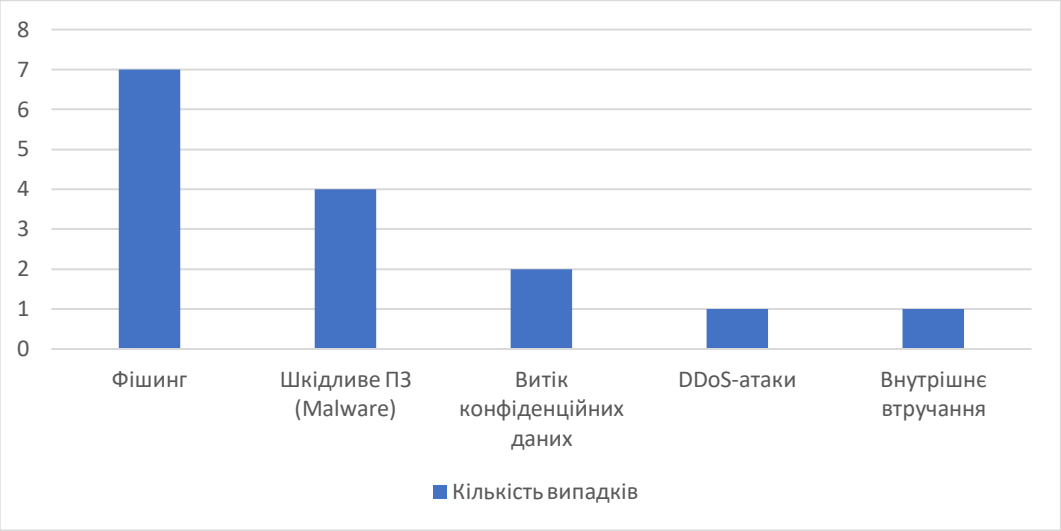


Рисунок 3.12 – Динаміка зареєстрованих інцидентів інформаційної безпеки (останні 12 місяців)

Систематизація загроз та реєстрація інцидентів дозволяє не лише виявляти поточні слабкі місця системи захисту, а й формувати на їх основі обґрунтовані пріоритети щодо вдосконалення політик безпеки, проведення навчань для персоналу та впровадження додаткових технічних бар'єрів.

Для цілісного оцінювання рівня кібербезпеки підприємства доцільним є застосування методу SWOT-аналізу, який дозволяє не лише виокремити внутрішні сильні й слабкі сторони наявної системи захисту, а й врахувати зовнішні чинники, що можуть сприяти або, навпаки, зашкодити її подальшому розвитку. Такий підхід є ефективним у стратегічному плануванні, зокрема при прийнятті рішень щодо інвестування у вдосконалення IT-інфраструктури або впровадження нових захисних технологій.

Як видно з наведеного аналізу у таблиці А.8 додатка А наявна система кіберзахисту демонструє достатньо розвинену інфраструктуру у частині контролю доступу, сегментації мережі, політик паролів і резервування. Водночас низка слабких сторін – передусім пов'язаних з людським фактором, обмеженою автоматизацією аналізу подій безпеки та нерівномірним рівнем захисту різних вузлів – потребують адресного реагування. Зовнішні загрози, зокрема еволюція шкідливого ПЗ і фішингових методик, підсилюють необхідність проактивного підходу до управління кіберризиками.

Отже, проведений аналіз дозволив комплексно охарактеризувати стан інформаційної безпеки комп’ютерної мережі підприємства крізь призму її вразливостей, наявних загроз та типових сценаріїв атак. Ідентифіковано критичні вузли інфраструктури, що залишаються потенційно вразливими через застарілі прошивки, відкриті порти або нестачу оновлень.

Результати тестування на проникнення підтвердили реальність ризиків, пов’язаних як із технічними недоліками, так і з людським фактором. Водночас динаміка зафіксованих інцидентів демонструє, що найбільш імовірними залишаються фішингові атаки, інфікування шкідливим ПЗ та витоки даних. SWOT-аналіз засвідчив наявність фундаментальних технічних переваг у системі захисту, але також виявив критичні зони розвитку, зокрема в частині автоматизації виявлення загроз і підвищення компетентності персоналу. Сукупність цих факторів окреслює вектори подальшого вдосконалення системи кібербезпеки підприємства.

3.4 Оцінка ефективності використаних методів захисту

Оцінювання ефективності впроваджених заходів захисту є ключовим етапом у циклі забезпечення інформаційної безпеки підприємства, адже дозволяє не лише зафіксувати наявність технічних засобів захисту, а й з’ясувати, наскільки вони відповідають реальним загрозам, специфіці внутрішньої інфраструктури та очікуваному рівню функціональної стійкості. У цьому підпункті зроблено спробу системно співвіднести наявні технічні рішення (антивірусний захист, фаєрволи, механізми аутентифікації, резервне копіювання тощо) із результатами аналізу інцидентів, виявлених вразливостей та сценаріїв атак, змодельованих у рамках тестування. Такий підхід дозволяє виявити неочевидні диспропорції між потенціалом системи захисту та фактичним рівнем її адаптивності до сучасного спектра кіберзагроз.

У межах об’єктивної оцінки ефективності впроваджених засобів захисту особливу цінність становить порівняльний аналіз базових показників

інформаційної безпеки підприємства до і після модернізації інфраструктури. Такий підхід дозволяє не лише констатувати факт наявності технічних змін, а й оцінити їхній практичний вплив на частоту інцидентів, швидкість реагування та загальні витрати на підтримку IT-безпеки. Аналіз охоплює період у 12 місяців – по шість місяців до і після оновлення, що включало розширення 2FA, впровадження Acronis Cyber Protect та централізацію моніторингу подій безпеки.

Як видно з табл. А.9 додатка А, модернізація системи кібербезпеки продемонструвала високу ефективність у зниженні інцидентів майже за всіма основними типами загроз. Найбільш відчутним став ефект у сфері зменшення часу реагування – завдяки впровадженню централізованого моніторингу та автоматизованих сповіщень. Хоча витрати на IT-безпеку зросли, проте це зростання є економічно обґрунтованим з огляду на масштаб зниження ризиків і зменшення непрямих втрат (наприклад, простоїв або витоку даних).

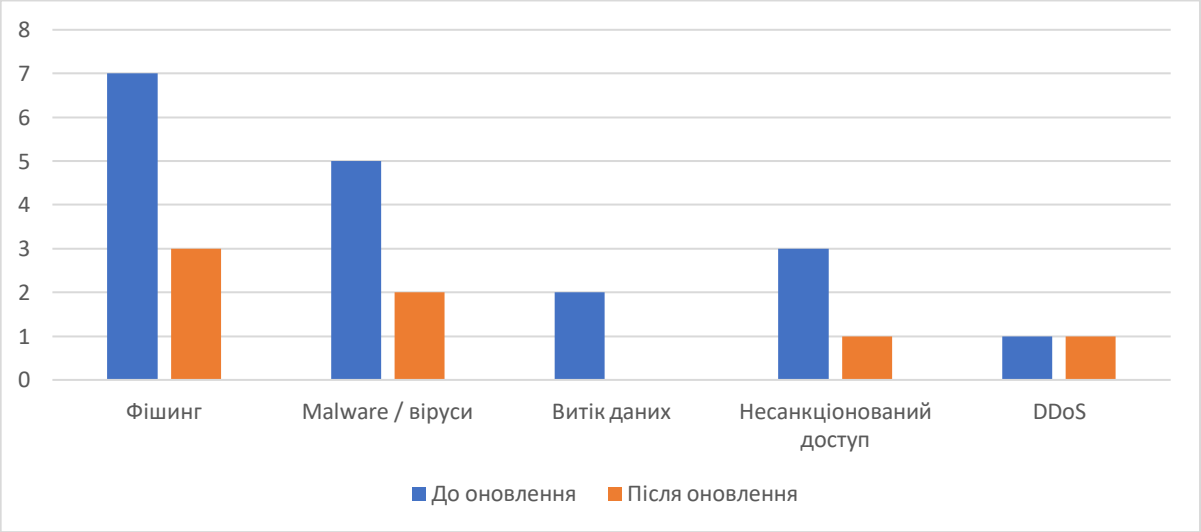


Рисунок 3.13 – Зміна кількості атак до та після оновлення системи захисту

Рис. 3.13 наочно демонструє тенденцію до суттєвого зниження кількості атак після впровадження оновленої інфраструктури захисту. Показники, пов’язані з фішинговими інцидентами та проникненням шкідливого ПЗ, знизилися практично вдвічі, що свідчить про дієвість удосконалених фільтрів та поведінкової аналітики. Показник витоку даних дорівнює нулю, що є прямим свідченням ефективності політик обмеження доступу та резервного копіювання.

У сучасних умовах зростання кіберризиків та ускладнення регуляторного середовища питання відповідності міжнародним стандартам інформаційної безпеки набуває не лише формального, а й стратегічного значення для підприємства. Відповідність вимогам стандартів, таких як ISO/IEC 27001, GDPR чи локальних нормативно-правових актів, свідчить про наявність системного підходу до управління ризиками, а також про відповідальність організації перед партнерами та клієнтами.

Як свідчить проведений аналіз у таблиці А.10 додатка А, система інформаційної безпеки на підприємстві має певні ознаки відповідності ключовим принципам ISO/IEC 27001, зокрема в частині доступу до ресурсів, резервного копіювання, управління обліковими записами та оцінки ризиків. Водночас у частині GDPR виявлено низку критичних невідповідностей – зокрема відсутність механізму повідомлення про інциденти витоку даних та нерозроблену політику шифрування персональної інформації. Це свідчить про необхідність не лише технічної модернізації, а й впровадження внутрішніх політик, що відповідають вимогам регламентів захисту персональних даних.

У межах щорічної перевірки було проведено внутрішній аудит стану інформаційної безпеки підприємства. Перевірка охоплювала як технічну частину (налаштування серверів, резервного копіювання, доступу до мережевих ресурсів), так і адміністративні процедури, пов’язані з політиками безпеки. Оцінювання проводилося на основі внутрішніх регламентів і базових вимог ISO/IEC 27001.

Під час аудиту виявлено кілька ключових моментів, які потребують доопрацювання:

– деякі робочі станції не оновлені, особливо в бухгалтерії та архівному відділі – це підвищує ризики для системи в цілому.

– Не всі архіви шифруються, хоча зберігають важливі файли. У випадку втрати чи доступу до них сторонніх, це може стати проблемою.

– Використання 2FA обмежене, хоча в IT-відділі реалізовано повністю, в інших підрозділах (наприклад, у фінансах) ця функція ще не підключена.

– Відсутній єдиний порядок дій при інцидентах. У разі витоку чи підозрілої активності співробітники діють «на власний розсуд», що ризиковано.

– Немає централізованого журналювання подій безпеки – журнали зберігаються локально на пристроях, а не збираються в одне місце.

На підставі цих спостережень аудитори сформували рекомендації:

– оновити всі робочі станції до підтримуваної версії ОС;

– впровадити обов’язкове шифрування для всіх архівних копій;

– поширити двофакторну автентифікацію на всі користувацькі облікові записи з доступом до чутливих даних;

– затвердити інструкцію дій у разі ІБ-інциденту;

– розглянути можливість впровадження базової системи логування (наприклад, через Wazuh або інші open source-рішення).

У підсумку, внутрішній аудит виявив як позитивні моменти (наявність політик, загальний контроль доступу, робоча система резервного копіювання), так і слабкі місця, що потенційно можуть призвести до уразливості. Робота в цьому напрямі триває, але вже зараз зрозуміло, куди потрібно рухатись і які саме кроки дадуть найвідчутніший ефект для посилення інформаційної безпеки.

З урахуванням результатів аудиту, виявлених вразливостей та загальної динаміки інцидентів інформаційної безпеки, було сформульовано низку пропозицій, які мають на меті підвищення ефективності захисту IT-інфраструктури підприємства. Насамперед доцільно здійснити логічну сегментацію мережі із впровадженням VLAN, що дозволить обмежити розповсюдження трафіку між різними підрозділами та ізолювати критичні ресурси (зокрема сервери CRM, бухгалтерські системи та архіви даних) у відокремлених зонах з обмеженим доступом. Такий підхід забезпечує локалізацію потенційних інцидентів та полегшує моніторинг активності всередині мережі.

Особливу увагу необхідно приділити розширенню використання багатофакторної автентифікації. На момент аналізу ця технологія була впроваджена лише частково, здебільшого для облікових записів адміністраторів.

У зв’язку з цим рекомендовано забезпечити покриття 2FA на всі облікові записи, які мають доступ до критичних бізнес-сервісів, включаючи внутрішню пошту, фінансові програми та хмарні платформи.

Варто переглянути підходи до архітектури доступу, орієнтуючись на принципи Zero Trust, які базуються не на довірі до внутрішнього середовища, а на постійній перевірці кожної дії користувача або пристрою незалежно від його розташування. Це передбачає введення обмежень на рівні доступу до ресурсів, базованих на ролях, контексті сесії та актуальному стані пристрою, з якого здійснюється запит.

Окремою складовою покращення має стати впровадження централізованої системи журналювання та моніторингу подій безпеки, бажано у форматі легкої SIEM-системи з відкритим кодом (наприклад, на базі Wazuh). Це дозволить не лише автоматизувати збирання логів, а й аналізувати потенційні загрози в реальному часі, спрощуючи реагування на інциденти.

Важливим кроком також є уніфікація та централізація процесу оновлення програмного забезпечення, особливо для користувацьких робочих станцій, які наразі демонструють нерівномірний рівень оновлень. Централізоване керування оновленнями через MDM-системи або внутрішні репозиторії дозволить зменшити кількість вразливостей, пов’язаних із застарілими версіями ПЗ.

Паралельно з технічними заходами слід реалізувати навчальні ініціативи для персоналу. Пропонується запровадити короткі практичні тренінги з елементами симуляцій (наприклад, фішингових листів), аби сформувати в працівників стійкі навички реагування та розпізнавання найпоширеніших соціотехнічних атак.

Запропоновані заходи є взаємодоповнюваними та охоплюють як архітектурні, так і поведінкові аспекти інформаційної безпеки. Їх реалізація дозволить суттєво знизити рівень ризику та підвищити загальну стійкість підприємства до сучасних кіберзагроз без потреби в радикальному оновленні інфраструктури.

РОЗДІЛ 4 ШЛЯХИ ВДОСКОНАЛЕННЯ СИСТЕМИ ЗАХИСТУ ДАНИХ

4.1 Модернізація апаратного забезпечення

Оцінка ефективності функціонування будь-якої системи захисту даних неминуче пов’язана з технічним станом апаратної частини мережевої інфраструктури. У сучасних умовах, коли інтенсивність обміну даними та вимоги до обчислювальних ресурсів постійно зростають, недостатня продуктивність або морально застаріле обладнання стають не лише фактором уповільнення процесів, а й безпосередньою загрозою інформаційній безпеці. У цьому підпункті розглянуто стан поточного апаратного забезпечення підприємства, визначено вузькі місця та сформульовано практичні рекомендації щодо його оновлення з урахуванням потреб безперервності, масштабованості та зниження ризику відмови критичних компонентів.

З метою визначення реального технічного потенціалу IT-інфраструктури підприємства було проведено повноцінний аудит апаратного забезпечення з урахуванням кількох ключових параметрів: технічного стану, року експлуатації, виробничого навантаження, частоти збоїв, а також рівня критичності кожного пристрою в контексті безперервності бізнес-процесів. Аналіз охопив серверне обладнання, робочі станції, мережеві пристрої та допоміжні засоби зберігання даних.

Загальна картина у табл.А.11 додатка А демонструє, що близько 40–50% активних пристроїв функціонують у режимі ресурсного виснаження або експлуатуються понад рекомендований життєвий цикл виробника. Особливу стурбованість викликає серверна інфраструктура, яка, попри стабільну роботу, не забезпечує достатнього запасу продуктивності та резервування для зростаючих обсягів даних і віртуалізованих навантажень.

На основі отриманих даних доцільно сформувати поетапний план технічної модернізації з пріоритетним оновленням серверів та мережевих вузлів, які безпосередньо впливають на безпеку, швидкість обробки критичних даних і

підтримку сучасних технологій (включаючи 2FA, резервне копіювання, шифрування та Zero Trust-моделі).

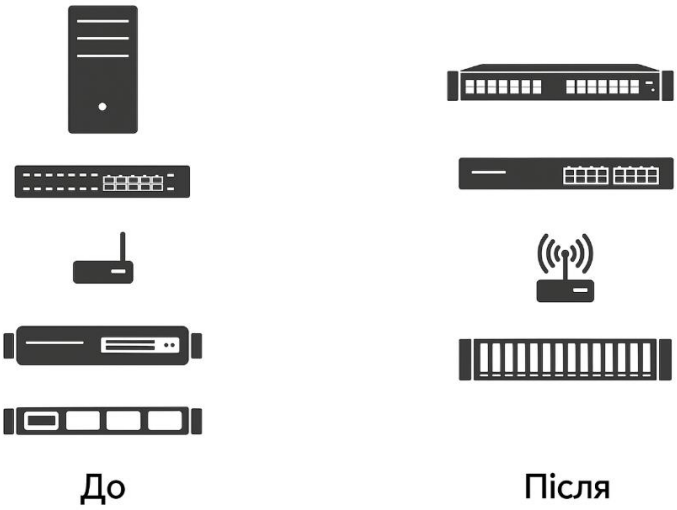
Аналіз фактичного стану апаратної частини інформаційної системи підприємства виявив низку пристроїв, технічні характеристики яких більше не відповідають поточним вимогам до продуктивності, енергоефективності, підтримки безпечних протоколів та масштабованості.

У таблиці А.12 додатка А запропоновано конкретні моделі для оновлення ключових елементів інфраструктури з урахуванням критичності, сумісності та перспектив розширення. Вибір апаратних рішень здійснювався з акцентом на довготривалу підтримку, продуктивність у віртуалізованому середовищі, сумісність із сучасними стандартами шифрування та підтримку актуальних версій системного ПЗ.

Запропоновані моделі забезпечують підвищення загальної продуктивності системи щонайменше на 40–60% при збереженні або навіть зниженні енергоспоживання на одиницю обчислювального ресурсу. Наприклад, заміна серверної платформи на сучасну лінійку з підтримкою віртуалізації й розширеною ECC-пам’яттю дозволить ефективніше розподіляти ресурси між ізольованими сервісами (CRM, бухгалтерія, поштові сервіси), не створюючи «точок перевантаження» у години пік.

Окремо варто наголосити на доцільності переходу на маршрутизатори з вбудованою системою глибокого аналізу трафіку (DPI) та апаратним шифруванням VPN-з’єднань – це дозволить підвищити якість взаємодії з віддаленими офісами та мінімізувати ризики перехоплення даних у процесі передавання.

Модернізація Wi-Fi-інфраструктури через впровадження точок доступу нового покоління (Wi-Fi 6, WPA3) дозволить зменшити навантаження на канал, підвищити стійкість до атак на бездротову мережу та забезпечити стабільне покриття у приміщеннях з великою кількістю користувачів.



Рисунка 4.1 – Схема фізичної інфраструктури серверної кімнати (до/після)

На рис. 4.1 наведено порівняльну схему фізичної організації серверної кімнати до та після впровадження заходів модернізації. У верхній частині ілюстрації представлено стан інфраструктури на момент початку аудиту: система складалася переважно з обладнання попереднього покоління, розміщеного без уніфікованого кабельного менеджменту, з частковим дублюванням функцій між окремими вузлами та без чіткого зонування за функціональним призначенням (зокрема, сервери баз даних, резервного копіювання, вебсервіси розміщувалися спільно без фізичного або логічного відокремлення).

Нижня частина рисунка демонструє стан після реалізації технічного оновлення, у ході якого здійснено впорядкування простору, впроваджено вертикальну стійку з серверними вузлами нового покоління (у т.ч. платформи під віртуалізацію), впроваджено керований комутатор з підтримкою VLAN, резервне живлення (UPS) із моніторингом навантаження, а також ізольовану зону для NAS-сховища. Сегментація на рівні фізичної структури супроводжується кращою вентиляцією, зменшенням перехресного навантаження та підвищеною стійкістю до збоїв завдяки резервуванню ключових компонентів.

Загалом, після модернізації серверна кімната не лише набула функціональної впорядкованості, а також стала й основою для подальшого впровадження логічної мережевої сегментації, а також розширення засобів контролю за доступом та моніторингом критичних вузлів у реальному часі.

У межах техніко-функціонального аналізу запропонованих заходів модернізації було проведено прогнозування очікуваних змін у продуктивності та надійності інформаційної інфраструктури після впровадження нового обладнання. Оцінка здійснювалася з урахуванням практичного впливу на ключові параметри: швидкодію серверів, пропускну здатність каналів, відмовостійкість та загальне скорочення часу простою систем. Окремо проаналізовано вплив оновлення на стабільність роботи критичних служб – таких як файлові системи, віртуальні середовища та VPN-з'єднання.

Згідно з розрахунками у табл. А.13 додатка А, у результаті реалізації запропонованого оновлення очікується інтегральне підвищення продуктивності системи щонайменше на 50–60%, що безпосередньо вплине на швидкість обробки користувацьких запитів, стабільність віртуальних середовищ і доступність сервісів у пікові години. Окремої уваги заслуговує очікуване зменшення часу відновлення після інцидентів: завдяки сучасному NAS та автоматизації відновлення цей показник скорочується вдвічі, що є критично важливим у контексті безперервності бізнес-процесів.

Сумарно запропоновані кроки дозволяють не лише оновити технічну основу системи захисту даних, але й створити резерв потужностей для подальшого масштабування та впровадження сучасних стандартів кібербезпеки.

4.2 Використання сучасних технологій кібербезпеки

У процесі аналізу поточного стану інформаційної безпеки підприємства було сформовано набір технологічних рішень, що відповідають сучасним викликам у сфері кіберзахисту. Враховуючи виявлені слабкі місця, а також потребу в автоматизації виявлення загроз, захисті кінцевих точок, контролі

доступу та централізованому моніторингу, було запропоновано впровадження низки технологій, які довели свою ефективність у корпоративному середовищі малого та середнього бізнесу.

Запропоновані технології у табл. А.14 додатка А не є взаємовиключними – навпаки, вони формують комплексну багаторівневу архітектуру захисту, що поєднує захист периметру, поведінковий моніторинг, контроль користувацьких дій і збереження журналів для юридичної та технічної верифікації. Особливої уваги заслуговує інтеграція SIEM та EDR – ці системи в тандемі дозволяють виявляти як миттєві загрози, так і латентні атаки, що можуть залишатися невидимими для класичних фаєрволів чи антивірусів.

Урахуванням специфіки підприємства, обсягів оброблюваних даних і наявного бюджету, більшість із зазначених технологій можна впровадити поступово, починаючи з безкоштовних або умовно безкоштовних версій (наприклад, Wazuh, OpenDLP, FreeRADIUS з підтримкою 2FA). Такий підхід дозволяє сформувати надійний каркас безпеки без одномоментних витрат і з поступовим нарощуванням функціональності відповідно до потреб.

Проаналізовані дані у табл. А.15 додатка А демонструють чітке відставання наявної системи від сучасного рівня кіберзахисту – не лише на рівні технічної архітектури, а й за принципами її побудови. Наприклад, у випадку антивірусного ПЗ наразі не реалізовано жодної поведінкової моделі детекції, що суттєво знижує шанси на вчасне виявлення шкідника, який не має відомого сигнатурного профілю. Те саме стосується резервного копіювання – ручне збереження копій без плану відновлення суперечить навіть базовим вимогам до безперервності діяльності.

Усі рекомендовані альтернативи підбиралися з урахуванням можливості поступового впровадження без повної реконструкції інфраструктури. Це дозволяє зберегти існуючу архітектуру як тимчасову основу, водночас закладаючи підґрунтя для поетапного переходу до більш зрілої, захищеної та адаптивної моделі кібербезпеки, здатної реагувати не лише на відомі, а й на невідомі загрози.

Рисунок 4.2 – Модель впровадження Zero Trust у корпоративну мережу

Запровадження принципів Zero Trust у корпоративному середовищі передбачає докорінну зміну підходів до ідентифікації, авторизації та контролю доступу всередині мережі. Як видно на рис. 4.2, основною тезою моделі є відмова від апріорної довіри до будь-якого користувача або пристрою – незалежно від того, знаходиться він у внутрішньому чи зовнішньому периметрі. Відповідно, кожен запит до ресурсів має бути верифікований через багаторівневу систему автентифікації, а доступ – надано виключно на основі чітко визначених політик, прив'язаних до ролі, контексту та поведінки.

У схемі логічно розмежовані три ключові рівні: користувачі та пристрої, доступ через інтернет, а також корпоративна мережа з зоною потенційного компрометування. Усі запити фільтруються через центральний вузол безпеки, де відбувається автентифікація, застосування політик доступу, а також постійний моніторинг із логуванням активності. Система побудована так, що навіть у разі проникнення зловмисника в мережу, його можливості залишаються мінімальними через ізоляцію, обмеження прав доступу та негайне виявлення аномалій.

У процесі оцінювання доцільності впровадження новітніх технологій кібербезпеки було здійснено прогнозний аналіз змін рівня ризику та частоти інцидентів, що спостерігаються в межах поточної інфраструктури.

Методологічною основою стали результати попередніх аудитів, звіти служби IT-підтримки та аналітика журналів безпеки. Для кожної з запропонованих технологій визначено очікувані кількісні ефекти, що виражаються у зменшенні ризику компрометації, кількості інцидентів та операційних втрат, пов'язаних із відновленням нормального функціонування після порушення [30].

Очікуваний ефект упровадження вказаних технологій підтверджує доцільність системного переходу до моделі проактивного захисту, орієнтованої не лише на стримування вже відомих загроз, також і на раннє виявлення аномалій, ізоляцію джерела атаки та запобігання розповсюдженню шкідливих впливів у межах мережі. Як показано в табл. А.16, зниження ризиків у ключових векторах досягає від 40 до 80%, при цьому кількість зареєстрованих інцидентів скорочується щонайменше втричі, що прямо впливає на стійкість бізнес-процесів.

З позицій операційної ефективності та стабільності IT-середовища впровадження сучасних технологій кібербезпеки забезпечує відчутне зменшення навантаження на технічну підтримку, прискорює час реагування на інциденти та знижує загальну вартість відновлення після атак. Наприклад, після інтеграції EDR-системи очікується автоматичне припинення підозрілих процесів без участі адміністратора, що суттєво зменшує вікно вразливості.

Так само SIEM-система дозволяє перейти від ручного перегляду локальних логів до корельованої оцінки подій у реальному часі. Це забезпечує швидше виявлення складних атак, таких як вертикальне підвищення привілеїв, сканування внутрішньої мережі або підготовка до lateral movement.

Упровадження MFA вже само по собі дозволяє уникнути значної частки фішингових інцидентів, які раніше проходили непомітно через соціальну інженерію. Водночас DNS-фільтрація діє превентивно – вона зменшує кількість випадків переходу на шкідливі ресурси, не даючи атаці шансу на реалізацію.

Отже, впровадження новітніх технологій безпеки не лише знижує рівень ризику, а й сприяє автоматизації, стандартизації та масштабованості системи

захисту, що є необхідним етапом зрілості IT-інфраструктури сучасного підприємства.

4.3 Поліпшення політики інформаційної безпеки підприємства

У рамках внутрішнього аудиту було проаналізовано наявні нормативні документи підприємства, що регламентують питання інформаційної безпеки, на предмет їх відповідності ключовим вимогам міжнародних стандартів – ISO/IEC 27001:2022, NIST SP 800-53 Rev. 5 та положенням Загального регламенту про захист даних (GDPR). Аналіз охоплював не лише формальну наявність відповідних політик, але й глибину їх опрацювання, актуальність, відповідність реальним процесам, а також практику впровадження на рівні організаційної культури.

Як показав аудит, окремі аспекти політики інформаційної безпеки або відсутні повністю, або реалізовані частково, без деталізації механізмів реалізації, відповідальності або процедур контролю. Це створює потенційно небезпечні зони регуляторного вакууму, які вразливі як до внутрішніх, так і до зовнішніх загроз.

Проведений аналіз засвідчив, що хоча базові політики – такі як загальна інформаційна політика підприємства чи внутрішні інструкції з кібергігієни – формально існують, їхній зміст не охоплює низку важливих елементів, передбачених міжнародними стандартами. Найбільш критичними є відсутність документації щодо реагування на інциденти та неконтрольоване використання особистих пристроїв у робочих цілях без сегментації мережі. Виявлені прогалини у політиках інформаційної безпеки (за ISO/IEC 27001, NIST, GDPR) показано в табл. А.17.

Особливої уваги потребують питання, пов’язані з обробкою персональних даних відповідно до вимог GDPR. Попри те, що підприємство не є великим оператором персональних даних, навіть обмежене оброблення імен, ідентифікаторів доступу, медичних чи фінансових документів потребує чітких процедур надання згоди, обмеження доступу та реалізації прав суб’єктів.

Перегляд і оновлення існуючих політик є не лише рекомендацією, а безпосередньою потребою, що дозволить не лише знизити ризики порушень, але й забезпечити юридичну захищеність підприємства у випадку перевірок, інцидентів або запитів від державних або міжнародних партнерів.

У результаті комплексної перевірки локальних політик інформаційної безпеки було ідентифіковано не лише низку відсутніх документів, але й ситуації, коли чинні положення не відповідають поточному технічному стану інфраструктури або не враховують зміну характеру загроз. У зв'язку з цим сформульовано пакет практичних пропозицій щодо їх актуалізації, доповнення та адаптації відповідно до вимог стандартів ISO/IEC 27001:2022, NIST 800-53, а також рекомендацій ENISA та OWASP. Окрема увага приділена врегулюванню використання особистих пристроїв, організації процесу багатофакторної автентифікації та процедур реагування на інциденти, які на момент аудиту були неформалізованими.

Усі запропоновані зміни, з табл. А.18 додатка А, мають не декларативний, а операційний характер, і передбачають конкретні технологічні або організаційні рішення, які можуть бути реалізовані поетапно. Найпріоритетнішими є впровадження інструкції реагування на інциденти та політики MFA, оскільки саме ці напрями найтісніше пов'язані з динамікою актуальних загроз (зокрема фішингу, несанкціонованого доступу та втрати контролю над активами).

Запровадження змін до нормативної документації, яке підкріплено не лише формальними вимогами стандартів, а й внутрішнім аналізом інцидентів і типових сценаріїв, дозволяє створити цілісну, несуперечливу і гнучку політику інформаційної безпеки, адаптовану до реальних умов функціонування підприємства.

Реформування нормативного блоку інформаційної безпеки є надзвичайно важливим не лише в контексті відповідності міжнародним стандартам, а й як передумова побудови цілісної та відповідальної культури захисту даних. Для ефективної реалізації оновлень був сформований покроковий план, який включає перелік конкретних політик, відповідальних за їх опрацювання осіб або

підрозділів, орієнтовні терміни та очікувані результати. Такий підхід дозволяє уникнути ситуацій формального переписування документів «для звітності» й фокусує увагу на досягненні конкретних практичних ефектів – зниженні ризиків, підвищенні прозорості, автоматизації процесів та відповідальності персоналу.

Оновлення політик інформаційної безпеки, показаних в табл.А.19 в перспективі впливає на кілька критично важливих компонентів організаційної стійкості:

По-перше, це підвищення персональної відповідальності користувачів. Завдяки оновленим інструкціям, прописаним алгоритмам дій та прив'язці політик до електронних систем авторизації й обліку, кожен працівник чітко розуміє, за що він відповідає, який рівень доступу має, та що буде у разі порушення процедур.

По-друге, зменшується кількість неформалізованих рішень і дій, що раніше мали місце через відсутність регламентів. Приклади – самовільне копіювання службової інформації на флешки, віддалена робота без VPN або використання особистих гаджетів без захисту. Впровадження політик BYOD, контролю USB та логування дій дозволяє змінити це середовище.

По-третє, нові документи створюють прозорість у процесах управління безпекою: усі ролі та процеси фіксуються, їх можна перевірити, змінити або адаптувати до нових умов. Це важливо не лише для внутрішнього контролю, а й для зовнішнього аудиту, сертифікації або юридичного захисту у разі розслідувань.

Отже, формалізація політик – це інструмент практичного управління ризиками, що дає змогу перейти від реактивного до проактивного формату захисту інформаційного середовища підприємства.

4.4 Впровадження резервного копіювання та відновлення даних

Резервне копіювання є критично важливою складовою політики забезпечення безперервності бізнесу, однак ефективність цього процесу

безпосередньо залежить від його системності, технічної реалізації та наявності відповідального супроводу. У рамках внутрішнього аудиту було проаналізовано стан реалізації резервного копіювання на підприємстві за ключовими параметрами: наявність процедури, тип бекапу (повне, інкрементне, диференційне), частота створення копій, середовище зберігання, рівень автоматизації, тестування відновлення, а також призначення відповідальних осіб. Оцінювання проводилося по основних IT-системах, що обробляють критичні для підприємства дані.

На основі таблиці А.20 можна зробити висновок, що система резервного копіювання носить фрагментарний і нефіксований характер. Лише окремі компоненти інфраструктури (зокрема файловий сервер і сайт) мають налаштоване автоматичне копіювання з використанням сучасних інструментів, тоді як частина критичних даних (наприклад, HR-документи або кеш CRM) не охоплені захистом узагалі. В окремих випадках резервне копіювання здійснюється вручну, без політики шифрування або перевірки цілісності, що суперечить не лише ISO/IEC 27001 (A.12.3), а й базовим принципам забезпечення цифрової безперервності.

У більшості випадків відсутнє тестування відновлення даних, що знижує реальну ефективність існуючих копій у випадку критичного інциденту. Також є технічні обмеження – окремі зовнішні диски перебувають у стані деградації, а обсяг NAS-сховища вже досягає граничних меж.

Загалом, існує об’єктивна потреба в уніфікації підходу до резервного копіювання, розробці єдиної політики з визначенням форматів, інтервалів, способів шифрування, каналів зберігання та відповідальних осіб, що і буде реалізовано у наступному підпункті.

Враховуючи результати проведеного аналізу поточного стану резервного копіювання, а також специфіку критичних інформаційних активів підприємства, було розроблено уніфіковану стратегію, яка передбачає реалізацію гібридної моделі з комбінуванням локальних та хмарних сховищ, оптимізацію типів копіювання залежно від частоти змін даних, впровадження автоматизації

процесів та щомісячного тестування відновлення. У запропонованій стратегії враховано як обмеження доступних ресурсів, так і вимоги щодо RPO (Recovery Point Objective) та RTO (Recovery Time Objective) для кожної категорії систем.

Упровадження зазначеної стратегії дозволить не лише підвищити рівень відмовостійкості, а й сформувати чітку документовану політику резервного копіювання, яка враховує критичність кожної підсистеми, обмеження доступу до копій, потребу у шифруванні та багатоканальності сховищ. Зокрема, поєднання локального зберігання з віддаленими хмарними платформами дозволяє дотримуватись принципу «3-2-1» (три копії, два носії, одна за межами підприємства). Запропонована стратегія резервного копіювання інформаційних ресурсів показана в табл. А.21

Також передбачено періодичне тестування відновлення, що суттєво знижує ризик "хибного захисту" – коли бекап існує, але відновлення виявляється неможливим через пошкоджені файли, несумісні формати або відсутність системи автоматизації.

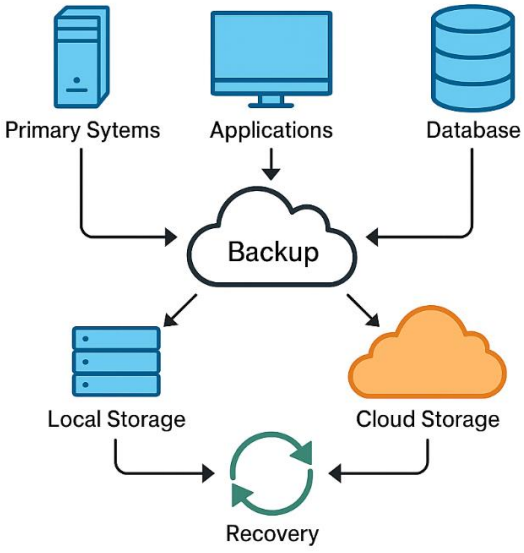


Рисунок 4.3 – Архітектура нової системи резервного копіювання та відновлення

Оновлена архітектура системи резервного копіювання, подана на рис. 4.3, побудована за принципом гібридної моделі, яка поєднує локальні та хмарні сховища, централізовану систему керування резервуванням та автоматизовану

процедуру відновлення даних. У центрі рішення – логічно ізольований вузол Backup, який отримує дані безпосередньо з трьох основних джерел: серверів додатків, баз даних та критичних систем підприємства. Усі канали побудовані з використанням шифрування (TLS), що гарантує цілісність переданих даних.

Процес резервування розділено на два незалежні напрямки: збереження копій у локальному сховищі (NAS / RAID-масив) для швидкого відновлення та паралельне копіювання в хмару (наприклад, AWS, Azure, Backblaze) для сценаріїв катастрофостійкості. Таким чином, реалізовано принцип 3-2-1: щонайменше три копії даних, на двох різних носіях, з яких одна знаходиться поза межами підприємства.

У підсумку, впровадження структурованої, багатоетапної системи резервного копіювання й відновлення даних істотно підвищує цифрову стійкість підприємства та мінімізує ризики втрати критичної інформації. Запропонована гібридна модель – з чітким розмежуванням джерел, каналів зберігання та відповідальних осіб – дозволяє поєднати швидкість локального відновлення з надійністю хмарної катастрофостійкості. Формалізація політик, автоматизація процесів і регулярне тестування копій створюють підґрунтя для ефективної реалізації принципів безперервності бізнесу (BCP) на практиці.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було комплексно реалізовано поставлені завдання, що дозволило не лише узагальнити теоретичні підходи до побудови комп'ютерних мереж та їх захисту, а й поглибити практичне розуміння взаємозв'язку між архітектурою мережевої інфраструктури та рівнем інформаційної безпеки.

На першому етапі дослідження було систематизовано теоретичні засади функціонування комп'ютерних мереж, зокрема розглянуто їх класифікацію, логічні й фізичні топології, принципи маршрутизації, сегментації та підходи до побудови надійних систем доступу. Окрему увагу приділено базовим моделям захисту мережі (Defense in Depth, Zero Trust), а також вимогам міжнародних стандартів безпеки ISO/IEC 27001 та NIST.

На основі аналізу актуального стану кіберзагроз було здійснено їх детальну класифікацію з урахуванням векторів атаки, мотивацій зловмисників та типів уразливостей. До найбільш імовірних загроз для мережевого середовища підприємства віднесено фішинг, атаки типу DDoS, несанкціонований доступ до систем через вразливі протоколи, а також загрози, пов'язані з людським фактором та використанням незахищених персональних пристроїв.

Значна увага була зосереджена на порівняльному аналізі програмного забезпечення для забезпечення інформаційної безпеки, серед якого проаналізовано антивірусні системи, фаєрволи, SIEM-платформи, засоби резервного копіювання, багатофакторної автентифікації та виявлення поведінкових аномалій. На прикладі впровадження таких рішень, як Bitdefender GravityZone, FortiGate, Acronis Cyber Protect і Wazuh, було показано можливість формування багаторівневого захисного контуру.

Практичний блок роботи базувався на дослідженні реальної структури комп'ютерної мережі конкретного підприємства. Було виконано моделювання логічної топології, схематичне відображення сегментації трафіку, опис віртуальних мереж VLAN, серверної частини, маршрутизаторів і точок доступу.

Виявлено низку проблем: морально застаріле обладнання, обмеженість у розгортанні сучасних протоколів, недостатній рівень логування подій та відсутність стандартизованих політик доступу.

За результатами аналізу мережевої інфраструктури та сканування вразливостей (використано інструменти Nessus та OpenVAS) було виявлено критичні слабкі місця – неоновлені прошивки комутаторів, відкриті порти без захисту, використання застарілих версій ОС, а також людський фактор як один з основних векторів загроз. Оцінювання ефективності наявних засобів захисту показало їх обмежену здатність до виявлення складних атак, недостатню інтегрованість і слабку масштабованість.

На завершальному етапі сформульовано комплекс практичних рекомендацій щодо модернізації системи захисту даних підприємства. Вони включають поетапне оновлення апаратної інфраструктури, впровадження політики MFA, побудову резервної системи з використанням хмарних сховищ, централізоване управління логами, а також поступовий перехід до архітектури Zero Trust. Запропоновано оновлення внутрішніх політик з урахуванням вимог ISO/IEC 27001 і GDPR, що дозволить не лише підвищити рівень технічного захисту, а й забезпечити організаційну зрілість в управлінні інформаційною безпекою.

Отже, результати дослідження свідчать про те, що цілі роботи досягнуто повною мірою. Проведений аналіз має не лише академічну, а й практичну цінність для підприємств, які перебувають на етапі цифрової трансформації та стикаються з новими викликами у сфері кіберзахисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Довгань О., Литвинова Л., Дорогих С. Кібербезпека № 1/2019. Київ: НДІ інформатики і права НАПрН України, 2019. 364 с.
2. Довгань О., Литвинова Л., Дорогих С. Кібербезпека № 8/2019. Київ: НДІ інформатики і права НАПрН України, 2019. 318 с.
3. Журавчак А., Піскозуб А. Аналіз методів машинного навчання для автоматизації тестування на проникнення // Кібербезпека: освіта, наука, техніка. 2025. Т. 3, № 27. С. 54–62.
4. Забезпечення кібербезпеки та захисту даних. Дія.Бізнес. URL: https://business.diia.gov.ua/consultations/zabezpechennia_kiberbezpeky_ta_zakhystu_danykh (дата звернення: 21.04.2025).
5. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI // Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 21.04.2025).
6. Закон України «Про захист персональних даних». Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 20.04.2025).
7. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII // Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 30.04.2025).
8. Ільєнко А., Телющенко В., Дубчак О. Сучасні кіберзагрози критичної інфраструктури України та світу // Кібербезпека: освіта, наука, техніка. – 2025. Т. 3, № 27. С. 150–164.
9. Кібербезпека в Україні: нормативна база, коментарі та роз'яснення. Київ: ЮрКнига, 2023. 412 с.
10. Кібербезпека як важлива складова всієї системи захисту держави. Міністерство оборони України. URL: https://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html (дата звернення: 21.04.2025).

11. Кібербезпека. Міністерство охорони здоров'я України. URL: https://moz.gov.ua/uk/kiberbezpeka (дата звернення: 30.04.2025).
12. Кібербезпека: як захистити себе у цифрову епоху. Міністерство внутрішніх справ України. URL: https://health.mvs.gov.ua/uk/chernihiv/novini/kiberbezpeka_iak_zaxistiti_sebe_u_cifrovu_epoxu (дата звернення: 07.05.2025).
13. Когут Ю. Кібербезпека та ризики цифрової трансформації компаній. Київ: Сідкон, 2021. 224 с.
14. Лісовська Ю. Кібербезпека. Ризики та заходи. Київ: Кондор, 2022. 320 с.
15. Нові правила захисту персональних даних в соціальних мережах та електронній пошті. Національна платформа з протидії кіберзлочинності. URL: https://stopfraud.gov.ua/video/novi-pravyla-zahystu-personalnyh-danyh-v-sotsialnyh-merezhah-ta-elektronnij-poshti-i816 (дата звернення: 21.05.2025).
16. Політика управління інцидентами кібербезпеки в інформаційній системі. Державна служба статистики України. URL: https://stat.gov.ua/sites/default/files/2025-01/Polituka_181.pdf (дата звернення: 03.05.2025).
17. Солодовник О. Кібербезпека України: досягнення і перспективи її забезпечення // ResearchGate. 2023. URL: https://www.researchgate.net/publication/375642132_KIBERBEZPEKA_UKRAINI_DOSAGNENNA_I_PERSPEKTIVI_II_ZABEZPECENNA (дата звернення: 07.05.2025).
18. Стратегія кібербезпеки України (2021–2025 роки). Рада національної безпеки і оборони України. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення: 03.05.2025).
19. Стратегія кібербезпеки України на 2021–2025 роки // Рада національної безпеки і оборони України. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення: 05.05.2025).

20. Тема 6.1. Основи кібербезпеки. Міністерство охорони здоров'я України. URL: https://moz.gov.ua/uk/osnovi-kiberbezpeki-2 (дата звернення: 05.05.2025).
21. Цехмейстер Р., Платоненко А., Ворохоб М. та ін. Дослідження методів забезпечення інформаційної безпеки у віртуальному середовищі // Кібербезпека: освіта, наука, техніка. 2025. Т. 3, № 27. С. 63–71.
22. Що таке кібербезпека для бізнесу? Дія.Бізнес. URL: https://business.diia.gov.ua/entrepreneur-handbook/item/scho_take_kiberbezpeka_dlya_biznesu (дата звернення: 10.05.2025).
23. Як захистити свої персональні дані від кіберзлочинців. Кіберполіція України. URL: https://cyberpolice.gov.ua/article/yak-zaxystyty-svoyi-personalni-dani-vid-kiberzlochyncziv-dyvitsya-chergovu-seriyu-proyektu-kiberbezpekaua-7914/ (дата звернення: 18.05.2025).
24. Acronis Cyber Protect – AI-Powered Integration of Data Protection and Cybersecurity. Acronis. URL: https://www.acronis.com/en-us/products/cyber-protect/ (date of access: 13.05.2025).
25. Aljohani T.M. Cyberattacks on Energy Infrastructures: Modern War Weapons // arXiv. 2022. URL: https://arxiv.org/abs/2208.14225 (дата звернення: 12.05.2025).
26. Cambridge University Press. Ukraine, Cyberattacks, and the Lessons for International Law // American Journal of International Law. 2022. URL: https://www.cambridge.org/core/journals/american-journal-of-international-law/article/ukraine-cyberattacks-and-the-lessons-for-international-law/69B36016B06998BCE1EC67C757CDF34D (дата звернення: 12.05.2025).
27. Carlos O.S. Using Cyber Threat Intelligence to Support Adversary Understanding Applied to the Russia-Ukraine Conflict // arXiv. 2022. URL: https://arxiv.org/abs/2205.03469 (дата звернення: 12.05.2025).

28. Center for European Policy Analysis (CEPA). Ukraine Teaches Europe Cyber Lessons. 2025. URL: https://cepa.org/article/ukraine-teaches-europe-cyber-lessons/ (дата звернення: 21.05.2025).
29. Cybersecurity & Infrastructure Security Agency (CISA). U.S. Department of Homeland Security. URL: https://www.cisa.gov/ (дата звернення: 21.05.2025).
30. Cybersecurity Act. European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881 (дата звернення: 21.05.2025).
31. Cybersecurity and Data Protection. World Economic Forum. URL: https://www.weforum.org/topics/cybersecurity-and-data-protection (дата звернення: 14.05.2025).
32. Cybersecurity Best Practices. European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu/topics/csirt-cert-services/good-practices (дата звернення: 21.05.2025).
33. Cybersecurity Framework. National Institute of Standards and Technology. URL: https://www.nist.gov/cyberframework (дата звернення: 21.05.2025).
34. Cybersecurity Guidelines. European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu/publications/guidelines (дата звернення: 23.05.2025).
35. Cybersecurity in the Digital Age. Harvard Business Review. URL: https://hbr.org/2019/05/cybersecurity-in-the-digital-age (дата звернення: 21.05.2025).
36. Cybersecurity Strategy of the European Union. European Commission. URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy (дата звернення: 21.05.2025).
37. Cybersecurity Threat Landscape. European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu/topics/csirt-cert-services/incident-handling/cyber-threat-landscape (дата звернення: 21.05.2025).
38. Cybersecurity Trends 2025. Gartner. URL: https://www.gartner.com/en/articles/cybersecurity-trends-2025 (дата звернення: 16.05.2025).

39. Cybersecurity Ventures. Cybersecurity Market Report. URL: https://cybersecurityventures.com/cybersecurity-market-report/ (дата звернення: 15.05.2025).
40. Dashboard | ESET PROTECT 10.1. ESET Online Help. URL: https://help.eset.com/protect_admin/10.1/en-US/dashboard.html (date of access: 12.05.2025).
41. Eichensehr K.E. Ukraine, Cyberattacks, and the Lessons for International Law // American Journal of International Law. 2022. Vol. 116, Issue 4. P. 708–727.
42. General Data Protection Regulation (GDPR). European Union. URL: https://gdpr.eu/ (дата звернення: 14.05.2025).
43. Greenberg A. Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. New York: Doubleday, 2019. 368 p.
44. How to create and delete a DHCP reservation in Windows Server. TechDirectArchive. URL: https://techdirectarchive.com/2020/06/01/how-to-make-dhcp-reservation-in-windows-server-2019/ (date of access: 24.05.2025).
45. Impact of State and State Sponsored Actors on the Cyber Environment and the Future of Critical Infrastructure. arXiv. URL: https://arxiv.org/abs/2212.08036 (дата звернення: 14.05.2025).
46. ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization. URL: https://www.iso.org/standard/54534.html (дата звернення: 17.05.2025).
47. ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems Requirements. URL: https://www.iso.org/standard/54534.html (дата звернення: 21.05.2025).
48. ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection – Information security controls. International Organization for Standardization. URL: https://www.iso.org/standard/75652.html (дата звернення: 21.05.2025).
49. Mitnick K. The Art of Invisibility. New York: Little, Brown Book Group, 2017. 320 p.

50. Mitnick K., Simon W.L. The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers. Indianapolis: Wiley, 2005. 270 p.
51. Modern Quantum Technologies of Information Security. arXiv. URL: https://arxiv.org/abs/1005.5553 (дата звернення: 15.05.2025).
52. National Cyber Security Centre (NCSC-NL). Four Cyber Security Lessons from One Year of War in Ukraine. 2023. URL: https://english.ncsc.nl/binaries/ncsc-en/documenten/publications/2023/3/14-3/four-cyber-security-lessons-from-one-year-of-war-in-ukraine/230313_oekraine_document_NCSC_ENG.pdf (дата звернення: 14.05.2025).
53. Nessus Vulnerability Scanner: Network Security Solution. Tenable®. URL: https://www.tenable.com/products/nessus (date of access: 15.05.2025).
54. NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (дата звернення: 17.05.2025).
55. NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations. URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final (дата звернення: 17.05.2025).
56. One to One Static NAT Configuration in FortiGate – ITAdminGuide.com. ITAdminGuide.com – Configuration guides for IT Administrators. URL: https://itadminguide.com/one-one-static-nat-configuration-fortigate/ (date of access: 17.05.2025).
57. Password Policy - Windows 10. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/password-policy (date of access: 17.05.2025).
58. Perlroth N. This Is How They Tell Me the World Ends: The Cyberweapons Arms Race. New York: Bloomsbury Publishing, 2021. 528 p.

59. Shapiro S. Fancy Bear Goes Phishing: The Dark History of the Information Age, in Five Extraordinary Hacks. New York: Farrar, Straus and Giroux, 2023. 384 p.
60. The Importance of Cybersecurity. Forbes. URL: https://www.forbes.com/sites/forbestechcouncil/2020/10/20/the-importance-of-cybersecurity/?sh=3f2c5d3e7b3e (дата звернення: 17.05.2025).
61. UCSC News. Ukraine Blackouts Caused by Malware Attacks Warn Against Evolving Cybersecurity Threats to the Physical World. – 2024. – URL: https://news.ucsc.edu/2024/05/ukraine-cybersecurity/ (дата звернення: 17.05.2025).
62. Vu A.V., Thomas D.R., Collier B. та ін. Getting Bored of Cyberwar: Exploring the Role of Low-level Cybercrime Actors in the Russia-Ukraine Conflict // arXiv. 2022. URL: https://arxiv.org/abs/2208.10629 (дата звернення: 20.05.2025).
63. Watters P. Cybercrime and Cybersecurity. London: Taylor & Francis, 2019. 350 p.
64. Wired. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. 2018. URL: https://www.wired.com/story/notpetya-cyberattack- (дата звернення: 21.05.2025)

ДОДАТОК А – ТАБЛИЦІ

Додаток А.1 – Порівняння типів мережевих топологій

№	Тип топології	Опис	Переваги	Недоліки	Сфера застосування
1	Шина (Bus)	Усі пристрої з’єднані одним кабелем, по якому передаються дані	Простота реалізації, низька вартість	Обмеження по довжині кабелю, складність у виявленні помилок	Невеликі локальні мережі, застарілі офісні рішення
2	Зірка (Star)	Пристрої підключені до центрального вузла (комутатора або хаба)	Висока надійність, зручність управління	Залежність від центрального вузла, більше кабелів	Офіси, школи, підприємства
3	Кільце (Ring)	Кожен пристрій має два з’єднання – з попереднім і наступним	Відсутність колізій, передбачуваність трафіку	Зупинка роботи через відмову одного вузла	Системи з критичними вимогами до порядку обміну
4	Дерево (Tree)	Ієрархічна структура, поєднання кількох топологій зірки	Масштабованість, централізоване адміністрування	Складність розгортання, часткова залежність від вузлів вищого рівня	Великі корпоративні мережі
5	Сітка (Mesh)	Кожен вузол з’єднаний з кількома іншими, що формує кілька маршрутів	Надійність, стійкість до збоїв, гнучкість	Висока вартість, складність керування	Військові мережі, центри обробки даних, системи моніторингу

Додаток А.2 – Порівняння архітектур комп’ютерних мереж за способом управління

№	Тип мережі	Опис	Приклад взаємодії	Переваги	Недоліки
1	Централізована	Один головний сервер або вузол управляє всіма процесами в мережі	Терміни подаються через центральний сервер	Повний контроль, централізоване зберігання даних	Висока залежність від одного вузла; вразливість до збоїв
2	Децентралізована	Кілька рівноправних вузлів, що можуть приймати рішення автономно	Регіональні сервери в банківській мережі	Баланс навантаження, гнучкість, підвищена стійкість	Ускладнене адміністрування, потенційні конфлікти між вузлами
3	Одноранго ва (P2P)	Усі пристрої рівноправні, виконують як функції клієнтів, так і серверів	Обмін файлами між ПК у локальній мережі	Простота впровадження, відсутність потреби у сервері	Обмежений контроль, низький рівень безпеки, складність масштабування
4	Клієнт-серверна	Один або кілька серверів обслуговують запити клієнтів	Сервер надає базу даних клієнтам	Централізоване керування, ефективне адміністрування	Потреба у високопродуктивному сервері, дорожче впровадження

Додаток А.3 – Класифікація загроз інформаційній безпеці в комп’ютерних мережах

№	Категорія загроз	Опис	Типові приклади	Наслідки
1	Внутрішні	Походять від користувачів або співробітників системи, які мають доступ до інформації	Несанкціоноване копіювання файлів, витік даних через USB-накопичувачі, зловмисні дії персоналу	Компрометація конфіденційної інформації, порушення політик доступу
2	Зовнішні	Надходять із зовнішнього середовища, включаючи кібератаки від третіх осіб	DDoS-атаки, фішингові розсилки, несанкціоноване сканування портів	Порушення доступності сервісів, втручання в мережевий трафік
3	Програмні	Виникають через помилки в ПЗ або шкідливе програмне забезпечення	Віруси, трояни, експлойти, недокументовані функції	Пошкодження даних, втрати доступу, проникнення в систему
4	Фізичні	Пов’язані з фізичним впливом на компоненти мережі або серверів	Відмова електроживлення, пожежа, крадіжка серверного обладнання	Знищення або втрата носіїв інформації, зупинка мережі

Додаток А.4 – Характеристика поширених атак на комп’ютерні мережі

№	Тип атаки	Суть атаки	Мета зловмисника	Типові наслідки	Характер загрози
1	2	3	4	5	6
1	DoS / DDoS	Перевантаження сервера або мережі надмірною кількістю запитів	Порушення доступності	Зупинка сервісів, фінансові втрати, зниження довіри	Зовнішня, технічна
2	Фішинг	Обман користувача для викрадення конфіденційних даних	Отримання логінів, паролів, фінансової інформації	Несанкціонований доступ до облікових записів, шахрайство	Соціоінженерна, зовнішня
3	Man-in-the-middle (MITM)	Перехоплення й модифікація трафіку між двома сторонами	Отримання конфіденційних даних, маніпуляція інформацією	Компрометація даних, втручання в комунікацію	Зовнішня, активна
4	Sniffing	Пасивне прослуховування незашифрованого трафіку в мережі	Перехоплення паролів, особистих повідомлень	Витік критичних даних, несанкціонований моніторинг	Пасивна, зовнішня

Додаток А.5 – Порівняння ключових положень стандартів ISO/IEC 27001, NIST SP 800-53, GDPR

№	Критерій	ISO/IEC 27001	NIST SP 800-53	GDPR
1	Призначення	Система управління інформаційною безпекою	Каталог технічних і адміністративних контролів	Регулювання обробки персональних даних
2	Тип документа	Міжнародний стандарт	Методологічне керівництво	Нормативно-правовий акт ЄС
3	Охоплення	Усі типи організацій	Державні і приватні IT-системи, переважно у США	Організації, що обробляють персональні дані громадян ЄС
4	Орієнтація	Управління ризиками, політики, аудит	Практичні технічні заходи, конфігурація систем	Права суб'єктів даних, згода, прозорість
5	Контрольні механізми	114 заходів безпеки у 14 доменах	Понад 900 контролів у 20+ категоріях	Прямі вимоги до згоди, мінімізації даних, сповіщень
6	Аудит / сертифікація	Можлива сертифікація організації	Не передбачає сертифікації, орієнтований на імплементацію	Нагляд з боку регуляторів, штрафи до 20 млн євро
7	Актуальність	Глобальне визнання	Обов'язковий у США для державних структур	Обов'язковий для компаній, що працюють з ЄС

Додаток А.6 – Порівняльна характеристика антивірусних рішень

№	Антивірус	Рівень виявлення	Навантаження на систему	Частота оновлень	Інтеграція з ОС
1	ESET	99,3 %	Низьке	Щогодини	Висока (автооновлення, служби безпеки)
2	Avast	97,8 %	Середнє	До 4 разів на день	Середня (деякі конфлікти з Windows Firewall)
3	Kaspersky	99,7 %	Високе	Щогодини	Висока (глибока інтеграція з системними процесами)
4	Bitdefender	99,6 %	Середнє	Кожні 1–2 години	Висока (адаптивна поведінка в системі)
5	Microsoft Defender	98,5 %	Низьке	Автоматичне (через Windows Update)	Повна інтеграція з ОС Windows

Додаток А.7 – Порівняння політик безпеки хмарних сервісів

№	Сервіс	Шифрування	Резервне копіювання	DLP	MFA
1	Google Workspace	TLS/SSL, AES-256 для зберігання	Автоматичне, з контрольними версіями	Так, на рівні Drive, Gmail	Так (SMS, додатки, ключі безпеки)
2	Microsoft 365	TLS/SSL, BitLocker, AES	Автоматичне, версійність у OneDrive	Так, з політиками в Microsoft Purview	Так (Authenticator, SMS, FIDO2)
3	Amazon AWS	AES-256, KMS, шифрування S3	Багаторівневе (Snapshot, Glacier)	Так, через Amazon Macie та IAM	Так (MFA, апаратні токени, SMS)
4	Dropbox Business	TLS/SSL, AES-256	Автоматичне, до 180 днів історії	Частково (через логіку спільного доступу)	Так (через мобільний додаток або SMS)

Додаток А.8 – SWOT-аналіз поточної системи кібербезпеки підприємства

№	Сильні сторони (S)	Слабкі сторони (W)
1	Централізована система автентифікації через Active Directory	Відсутність повноцінної SIEM-системи моніторингу інцидентів
2	Реалізований контроль доступу з багаторівневими політиками	Недостатній рівень обізнаності працівників у сфері кібергігієни
3	Регулярне резервне копіювання з використанням хмарного зберігання	Часткова застарілість серверного програмного забезпечення
4	Наявність фаєрвола корпоративного рівня (FortiGate)	Обмежене покриття 2FA для користувачів із середніми правами доступу
	Можливості (O)	Загрози (T)
1	Впровадження повноцінної SIEM-системи (наприклад, Zabbix + Wazuh)	Актуалізація глобальних фішингових кампаній, спрямованих на людський фактор
2	Перехід на сучасні версії ОС із розширеним захистом ядра	Поширення zero-day вразливостей у використаному програмному стеку
3	Розширення 2FA на всі ключові сервіси та сегменти	Фізичний доступ сторонніх осіб у недостатньо контрольованих зонах
4	Навчання персоналу з елементами симульованих атак (red teaming)	Потенційні атаки на інфраструктуру через вразливі IoT-пристрої

Додаток А.9 – Порівняльна характеристика показників інформаційної безпеки до та після модернізації

№	Показник	До впровадження (період I)	Після впровадження (період II)	Динаміка / Ефект
1	Загальна кількість інцидентів	18	7	↓ на 61%
2	Середній час реагування (хвилин)	95	38	↓ на 60%
3	Кількість інцидентів через фішинг	7	3	↓ на 57%
4	Випадки витоку даних	2	0	↓ до 0
5	Частка систем з 2FA (%)	35%	82%	↑ на 47 п.п.
6	Витрати на безпеку (грн/міс.)	18 500	24 700	↑ на 33%, із компенсаторним ефектом

Додаток А.10 – Оцінка відповідності елементів системи захисту вимогам міжнародних стандартів

№	Критерій відповідності	ISO/IEC 27001	GDPR	Коментар
1	Управління обліковими записами користувачів	Так	Так	Через централізовану систему AD з обмеженнями доступу
2	Шифрування персональних та службових даних	Ні	Ні	Дані зберігаються без шифрування на рівні файлових систем
3	Аудит і журналювання подій	Так	Частково	Локальний аудит є, але відсутній централізований SIEM
4	Політики резервного копіювання	Так	Так	Регламентований графік копіювання, у т.ч. хмарного
5	Реалізація права на забуття / видалення даних	Ні	Частково	Механізм частково реалізований лише на CRM-рівні
6	Повідомлення про витік персональних даних	Ні	Ні	Не прописана процедура реагування згідно з GDPR
7	Двофакторна автентифікація (2FA)	Частково	Так	Реалізовано частково для критичних сервісів
8	Ризик-орієнтоване управління інформаційними активами	Так	–	Ведеться облік критичних IT-ресурсів, оцінка ризиків

Додаток А.11 – Аудит наявного апаратного забезпечення підприємства

№	Тип обладнання	Модель / виробник	Рік введення в експлуатацію	Поточний технічний стан	Критичність для бізнесу	Коментар / проблеми, що фіксувалися
1	Сервер файлового сховища	HPE ProLiant DL380 Gen9	2017	Працездатний, але зношений HDD	Висока	Часті повідомлення S.M.A.R.T. про деградацію RAID-масиву
2	Комутатор рівня доступу	Cisco Catalyst 2960	2015	Застарілий, підтримує лише 100 Мбіт/с	Середня	Обмежує пропускну здатність між сегментами VLAN
3	Робоча станція бухгалтера	Dell OptiPlex 3050	2018	Повільна робота при запуску важких Excel-файлів	Висока	Обмежена оперативна пам’ять, відсутній SSD-диск
4	Wi-Fi точка доступу	TP-Link EAP225	2019	Робочий стан, стабільна передача	Низька	Не підтримує новітні стандарти шифрування WPA3
5	Сервер віртуалізації	Dell PowerEdge R720	2016	Працює з навантаженням понад 80% CPU	Висока	Висока температура процесорів, відсутність підтримки сучасних hypervisor
6	NAS для резервного копіювання	Synology DS918+	2018	Стан добрий, часткова деградація одного HDD	Середня	Необхідна заміна одного диску, обмежений обсяг для зростання
7	Маршрутизатор основного каналу	MikroTik RB3011UiAS-RM	2017	Працездатний, але морально застарілий	Висока	Немає апаратного прискорення VPN, що впливає на швидкість
8	Мережевий принтер	HP LaserJet Pro M404dn	2020	Без зауважень	Низька	Використовується нерегулярно, переважно внутрішньо

Додаток А.12 – Рекомендовані заходи щодо оновлення апаратного забезпечення

№	Поточний пристрій	Рекомендована модель / рішення	Причини модернізації
1	HPE ProLiant DL380 Gen9 (2017)	HPE ProLiant DL380 Gen11 / AMD EPYC	Високе навантаження, критична роль у зберіганні даних, підтримка DDR5, PCIe Gen5
2	Cisco Catalyst 2960 (100 Мбіт/с)	Cisco Catalyst C9200L	Недостатня пропускна здатність, відсутність підтримки 1/10 Гбіт, обмеження VLAN
3	Dell OptiPlex 3050 (2018)	HP ProDesk 600 G6 + SSD 1TB	Повільна обробка об’ємних документів, дефіцит оперативної пам’яті, HDD без TRIM
4	TP-Link EAP225	Ubiquiti UniFi 6 Lite	Відсутність підтримки WPA3, обмежена кількість одночасних з’єднань
5	Dell PowerEdge R720	Dell PowerEdge R650 / VMware Ready	Потреба в сучасному hypervisor, надмірне тепловиділення, високе енергоспоживання
6	Synology DS918+ (NAS)	QNAP TS-873A / RAID-Z	Обмежена масштабованість, низький поріг відновлення, часткова деградація RAID
7	MikroTik RB3011UiAS-RM	FortiGate 60F або MikroTik CCR1009	Відсутність апаратного VPN-шифрування, низький рівень DPI, неможливість масштабування
8	HP LaserJet Pro M404dn	Заміна не потрібна	Стабільна робота, відповідність навантаженню

Додаток А.13 – Очікуваний приріст продуктивності та надійності після оновлення обладнання

№	Компонент	Поточний стан (до)	Очікувані покращення (після)	Приріст (%) / ефект
1	Сервер файлового сховища	Повільна обробка запитів, зношений RAID, HDD	SSD-RAID з контролером нового покоління, підтримка PCIe Gen5	↑ продуктивність читання/запису до 70%
2	Сервер віртуалізації	Часті перевантаження, 80–90% CPU-навантаження	Новий CPU, збільшена RAM, підтримка гіпервізора ESXi 8.0	↓ середнє навантаження на 40–50%
3	Комутатор доступу	100 Мбіт, нестабільна передача VLAN	Підтримка 1/10 Гбіт, керованість, розмежування трафіку	↑ пропускна здатність у 10 разів
4	Робочі станції	Повільний запуск, HDD, 4 ГБ ОЗП	Перехід на SSD, 16 ГБ ОЗП, Windows 11 Pro	↓ час запуску додатків у 2–3 рази
5	Точка доступу Wi-Fi	Підключення не більше 30 користувачів, WPA2	Wi-Fi 6, WPA3, 75+ пристроїв, QoS	↑ стабільність з’єднання, мінус лагів
6	NAS (резервне копіювання)	Обмежений обсяг, деградація RAID	Модульна система, масштабування до 100 ТБ, підтримка Btrfs	↑ час відновлення ↓ на 60%, резерв ↑
7	VPN/маршрутизатор	Низька пропускна здатність, без апаратного шифрування	Апаратне шифрування IPsec, DPI, централізований контроль доступу	↑ швидкість VPN у 3–4 рази
8	Рівень резервування живлення	Один UPS, без мережевого моніторингу	Два незалежних UPS, SNMP-моніторинг, автоматичне вимкнення	↑ надійність електроживлення

Додаток А.14 – Перелік рекомендованих технологій для підвищення рівня кібербезпеки

№	Технологія	Призначення	Приклад ПЗ / платформи	Очікуваний ефект / переваги
1	EDR (Endpoint Detection and Response)	Моніторинг поведінки кінцевих точок, виявлення загроз на рівні ОС	CrowdStrike Falcon, Bitdefender GravityZone	Виявлення складних атак, контроль процесів, миттєва ізоляція
2	Zero Trust	Верифікація кожного запиту незалежно від місця або ролі	Zscaler, Cisco Zero Trust	Мінімізація ризику lateral movement, повна перевірка сесій
3	MFA (Multi-Factor Authentication)	Багатофакторна автентифікація для доступу до систем	Google Authenticator, Duo Security	Захист облікових записів, зниження успішності фішингу
4	UTM (Unified Threat Management)	Комплексна система захисту периметру мережі	FortiGate, Sophos XG Firewall	Захист на одному рівні: фаєрвол, IPS, антивірус, фільтри URL
5	SIEM (Security Information and Event Management)	Централізований збір і аналіз логів подій	Wazuh, Splunk, IBM QRadar	Реальне виявлення аномалій, історичний аналіз інцидентів
6	DLP (Data Loss Prevention)	Захист від витоку чутливої інформації	Symantec DLP, Safetica	Блокування відправки файлів за межі системи, контроль USB
7	DNS-фільтрація	Блокування доступу до шкідливих або фішингових ресурсів	Cisco Umbrella, NextDNS	Попередження фішингу, зниження навантаження на антивірус
8	SOC-інтеграція	Створення базової системи оперативного реагування	Wazuh + ELK Stack	Керований моніторинг, єдина точка контролю безпеки

Додаток А.15 – Порівняння існуючих засобів безпеки з сучасними альтернативами

№	Категорія	Використовується наразі	Сучасна альтернатива	Коментар / Очікуваний ефект
1	Антивірусний захист	Avast Business (free)	Bitdefender GravityZone / ESET Protect	Відсутність EDR, низький рівень реакції на скрипти
2	Фаєрвол	Windows Firewall + MikroTik	FortiGate 60F або Sophos XGS	Відсутність DPI, немає IPS, ручне конфігурування
3	VPN	PPTP через MikroTik	IPsec/OpenVPN із 2FA, WireGuard	Низька криптостійкість, відсутність журналювання
4	Аутентифікація	Паролі + GPO	MFA з OTP або push-нотифікаціями	Вразливість до фішингу, немає step-up аутентифікації
5	Система резервного копіювання	Ручне копіювання на USB / NAS	Acronis Cyber Protect / Veeam Backup	Немає автоматизації, немає інкрементного резерву
6	Моніторинг подій	Локальні журнали Windows	Wazuh + ELK Stack (SIEM)	Події не централізуються, немає правил кореляції
7	Захист електронної пошти	Вбудований фільтр MS Outlook	Mimecast, Zimbra Security, Proofpoint	Високий рівень фішингу, відсутність SPF/DKIM/DMARC
8	Контроль доступу до даних	Структурні права NTFS	DLP + класифікація інформації (Safetica)	Користувачі мають зайві повноваження, немає аудитів
9	Веб-фільтрація	Відсутня	Cisco Umbrella / NextDNS	Не блокується шкідливий контент, немає логування

Додаток А.16 – Очікувані результати впровадження сучасних технологій кібербезпеки

№	Технологія	Рівень ризику (до)	Рівень ризику (після)	Кількість інцидентів / 12 міс. (до)	Після впровадження	Очікуваний ефект / зміни
1	EDR	Високий	Низький	6	1	Ізоляція процесів, поведінкове блокування, автоаналіз
2	MFA	Середній	Низький	5 (злам акаунтів)	1	Блокування несанкціонованого доступу, зниження фішингу
3	SIEM	Високий	Середній	12 (втрачено через непомічені події)	3	Централізація логів, раннє виявлення загроз
4	Zero Trust	Середній	Низький	4	1	Ізоляція користувачів, зменшення lateral movement
5	DNS-фільтрація	Високий	Низький	8 (перехід на фішингові сайти)	1	Превентивне блокування доступу до небезпечних доменів
6	DLP	Середній	Низький	3 (витік файлів через пошту / флешки)	0	Контроль каналів передачі, попередження витоків
7	UTM	Високий	Середній	7	2	Фільтрація трафіку, виявлення підозрілих сесій

Додаток А.17 – Виявлені прогалини у політиках інформаційної безпеки (за ISO/IEC 27001, NIST, GDPR)

№	Напрям / вимога	Стан реалізації на підприємстві	Відповідний стандарт	Коментар щодо прогалин і потенційних ризиків
1	2	3	4	5
1	Політика управління доступом	Частково	ISO/IEC 27001 (A.9), NIST AC-1	Немає єдиного документа, немає атрибутивної сегментації, 2FA часткова
2	Політика резервного копіювання	Формально наявна, не оновлюється	ISO A.12.3, NIST CP-9	Відсутній план відновлення, не тестуються копії, не регламентований термін зберігання
3	Політика реагування на інциденти	Відсутня	ISO A.16.1, NIST IR-1	Жодної задокументованої процедури реагування або журналювання
4	Політика щодо роботи з персональними даними	Частково	GDPR Art. 5, 32	Відсутні чіткі правила обробки, немає права на "забуття", не фіксуються згоди
5	Політика безпеки BYOD	Відсутня	ISO A.6.2.1, NIST AC-19	Співробітники використовують особисті пристрої без сегментованого доступу
6	Політика оновлення ПЗ	Частково	NIST SI-2, ISO A.12.6	Патчі встановлюються вручну, відсутній централізований контроль
7	Політика збереження логів	Частково (локальні журнали)	NIST AU-11, ISO A.12.4	Відсутня SIEM-система, логування неповне, зберігається менше 30 днів
8	Політика розмежування обов’язків	Відсутня	ISO A.6.1.2	Немає ролей для «перехресної перевірки», адміністратори мають повний доступ

Додаток А.18 – Пропозиції щодо вдосконалення політик інформаційної безпеки

№	Напрям / документ	Пропоновані зміни або нова політика	Обґрунтування / очікуваний ефект	Відповідальний підрозділ
1	Політика багатофакторної автентифікації (MFA)	Запровадити нову політику щодо обов'язкового MFA для всіх адміністраторів, а також працівників, які працюють із персональними/фінансовими даними	Зниження ймовірності компрометації облікових записів через фішинг або витік паролів	ІТ-відділ
2	Інструкція реагування на інциденти	Розробити детальну покрокову інструкцію щодо дій у разі виявлення порушення ІБ, з призначенням відповідальних і термінами реакції	Підвищення швидкості реагування, уникнення паніки, юридична фіксація дій	ІБ-відділ / комплаєнс
3	Політика використання USB-накопичувачів	Обмежити використання зовнішніх накопичувачів до whitelist-переліку пристроїв, заборонити автостарт	Зменшення ризику зараження систем шкідливим ПЗ, контроль витоку даних	ІТ-відділ / служба безпеки
4	Політика обробки персональних даних	Оновити процедури надання згоди, зберігання, доступу, реалізації права на видалення даних	Відповідність вимогам GDPR, зменшення юридичних ризиків	Юридичний відділ
5	Політика роботи з BYOD (Bring Your Own Device)	Ввести вимогу реєстрації особистих пристроїв, застосування окремої VLAN для гостьового доступу	Мінімізація ризиків втручання з несанкціонованих пристроїв	ІТ-відділ / служба безпеки
6	Політика оновлення ПЗ	Впровадити процедуру централізованого управління оновленнями через WSUS або MDM	Зниження кількості вразливостей, зменшення ручної роботи	Системний адміністратор
7	Політика щодо контролю доступу	Уточнити матрицю доступу до даних за ролями, періодично переглядати актуальність прав	Забезпечення принципу найменших привілеїв, уникнення "мертвих" акаунтів	ІБ-відділ / кадровий відділ
8	Політика збереження логів	Визначити перелік критичних подій, які обов'язково підлягають логуванню та зберігаються не менше 180 днів	Покращення трасування інцидентів, можливість розслідувань	ІТ-відділ / аналітики ІБ

Додаток А.19 – План оновлення політик інформаційної безпеки

№	Політика / документ	Відповідальний	Етап реалізації	Термін виконання	Очікуваний результат
1	2	3	4	5	6
1	Політика MFA	IT-директор	Розробка, тестування, впровадження	квітень–травень	Всі адміністратори та ключові працівники з MFA
2	Інструкція реагування на інциденти	ІБ-аналітик	Аналіз інцидентів, створення сценаріїв	травень	Стандартизовані дії персоналу при атаках
3	Політика резервного копіювання	Системний адм.	Оновлення плану, документування процедур	червень	Автоматизований контроль бекапів, періодичне тестування
4	Політика роботи з персональними даними	Юридичний відділ	Перегляд процедур відповідно до GDPR	червень–липень	Впровадження права на «забуття», фіксація згод
5	Політика доступу та ролей (RBAC)	Кадрова служба + IT	Визначення критичних ролей, матриця доступу	липень	Принцип мінімальних прав, автоматичний контроль доступу
6	Політика BYOD	IT-відділ	Сегментація Wi-Fi, whitelist пристроїв	серпень	Ізоляція гостьового трафіку, захист від несанкц. пристроїв
7	Політика оновлення ПЗ	DevOps / IT	Впровадження централізованого оновлення	серпень	Єдиний підхід до патчів, зниження вразливостей
8	Політика збереження логів та моніторингу	ІБ-відділ	Створення правил, запуск SIEM-системи	вересень	Централізований аудит, розслідування інцидентів

Додаток А.20 – Оцінка поточного стану резервного копіювання по IT-системах підприємства

№	Система / дані	Наявність копії	Тип бекапу	Частота	Місце зберігання	Автоматизація	Відповідальний / підрозділ	Проблеми / ризики
1	Бухгалтерська система (M.E.Doc, 1C)	Так	Повне + інкрементне	Щодня	NAS локальний + USB	Частково	Системний адміністратор	Відсутність шифрування, не перевіряється відновлення
2	Пошта (корпоративний сервер IMAP)	Так	Повне (архів .pst)	Щотижня	NAS (одна копія)	Ручне	IT-фахівець	Старий формат копій, ручна ініціація
3	CRM (хмарна, локальний кеш)	Ні	–	–	–	–	Відсутній	Дані кешу не бекапляться взагалі
4	Сервер файлів	Так	Повне	Щодня (вночі)	NAS + зовнішній HDD	Автоматично	Служба адміністрування	HDD на межі ємності, один диск має помилки SMART
5	HR-документи (локальні ПК)	Частково	Ручне копіювання	Нерегулярно	USB, Google Drive	Ні	Працівники відділу кадрів	Невідомо, що саме копіюється, ризик витоку
6	Бекап сервера віртуалізації	Так	Повне	1 раз / тиждень	Розділ RAID6	Так	DevOps / системний адміністратор	Відсутність позасайтової копії, нема DRP
7	Сайт / вебсервер	Так	Повне	Щодня	Хмара (AWS snapshot)	Так	Підрядник з технічного супроводу	Журнал не ведеться, немає сповіщення про помилки

Додаток А.21 – Запропонована стратегія резервного копіювання інформаційних ресурсів

№	Категорія даних / система	Тип копіювання	Локальне зберігання	Хмарне зберігання	Частота / розклад	Примітки щодо автоматизації та відновлення
1	Бухгалтерські системи (1С, M.E.Doc)	Повне щотижневе + інкрементне щоденне	NAS RAID10, окрема ізольована мережа	Acronis Cloud EU Server	Інкремент – щодня, повне – субота 01:00	Повна автоматизація, тест відновлення щомісяця
2	Сервер файлів	Інкрементне щоденне + версійність	QNAP NAS (бекап в репозиторій)	Amazon S3 (архівне зберігання)	Щодня о 03:00	Версійність + дедуплікація, відновлення через веб-інтерфейс
3	CRM (хмарна)	Експорт даних у форматі CSV + API snapshot	Зберігання на окремому SFTP	Google Cloud Bucket	Раз на 48 годин	Автоматизоване через скрипт API-запиту
4	Корпоративна пошта (IMAP, MS365)	Повне архівування поштових скриньок	Локальний сервер архіву (Vault)	Azure Backup for Exchange	Щосуботи о 02:00	Шифрування AES256, вибіркове відновлення листування
5	Сайт та база даних (MySQL, CMS)	Повне знімкове копіювання (snapshot)	Локальний RAID6, ізоляція по VLAN	AWS snapshot S3 zone	Щодня о 05:00	Автоматизоване, обмежено доступ через VPN
6	HR-документи	Повне + інкрементне в реальному часі	Сервіс Synology Active Backup	OneDrive for Business	Синхронізація – кожні 30 хвилин	Контроль версій, заборона локального копіювання
7	Сервер віртуалізації (Hyper-V)	Повна копія + export VM	Локальний Veeam-репозиторій	Backblaze B2	Повна копія щотижня, дельта – щодня	Інтеграція із Windows Server Backup