МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ

КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

на тему:

ОПТИМІЗАЦІЯ СИСТЕМИ ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

Виконав: студент групи 1КІ-23
зі спеціальності
123 – «Комп'ютерна інженерія»
Артьом ШМАРАЄВ
Науковий керівник:
к.т.н Роксолана БРЕУС
(науковий ступінь, вчене звання,
прізвище та ініціали)

Черкаси, 2025

АНОТАЦІЯ

У кваліфікаційній роботі представлено комплексне дослідження з оптимізації систем захисту комп’ютерної мережі підприємства. Робота спрямована на вирішення актуальної проблеми підвищення стійкості корпоративної мережевої інфраструктури до сучасних кіберзагроз, включаючи фішингові атаки, експлойти, DDoS, несанкціонований доступ та витоки даних.

Аналіз існуючої мережі охоплює фізичну та логічну архітектуру, DMZ-сегменти, VLAN, а також оцінку ризиків і вразливостей. Було виявлено критичні недоліки: незашифровані протоколи (HTTP, FTP), відкриті порти, застаріле програмне забезпечення, неналежне управління доступом.

У роботі запропоновано технічні та організаційні заходи: впровадження багатофакторної аутентифікації (MFA), рольової моделі доступу (RBAC), оптимізація міжмережевого екрану, сегментація трафіку та використання сучасних VPN-протоколів (IPSec, SSL). Для виявлення загроз рекомендовано впровадити SIEM-платформи, системи IDS/IPS, а також поведінковий аналіз (UEBA) із використанням машинного навчання.

Особлива увага приділена політикам безпеки, аудитам доступу, навчанню персоналу та впровадженню стратегій резервного копіювання на основі принципу «3-2-1». Практичні результати демонструють можливість значного зниження ризиків компрометації та підвищення готовності підприємства до реагування на інциденти.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, МЕРЕЖЕВА ІНФРАСТРУКТУРА, ФАЙРВОЛ, VPN, MFA, SIEM, IDS/IPS, АУДИТ ДОСТУПУ, РОЛЬОВА МОДЕЛЬ, РЕЗЕРВНЕ КОПІЮВАННЯ.

ABSTRACT

The qualification work presents a comprehensive study on optimising enterprise computer network security systems. The work is aimed at solving the urgent problem of increasing the resilience of corporate network infrastructure to modern cyber threats, including phishing attacks, exploits, DDoS, unauthorised access and data leaks.

The analysis of the existing network covers physical and logical architecture, DMZ segments, VLANs, as well as risk and vulnerability assessment. Critical deficiencies were identified: unencrypted protocols (HTTP, FTP), open ports, outdated software, and inadequate access control.

The paper proposes technical and organisational measures: implementation of multi-factor authentication (MFA), role-based access control (RBAC), firewall optimisation, traffic segmentation, and the use of modern VPN protocols (IPSec, SSL). To detect threats, it is recommended to implement SIEM platforms, IDS/IPS systems, and behavioural analysis (UEBA) using machine learning.

Particular attention is paid to security policies, access audits, staff training, and the implementation of backup strategies based on the 3-2-1 principle. Practical results demonstrate the possibility of significant reduction of compromise risks and increase of enterprise readiness to respond to incidents.

Keywords: INFORMATION SECURITY, NETWORK INFRASTRUCTURE, FIREWALL, VPN, MFA, SIEM, IDS/IPS, ACCESS AUDIT, ROLE MODEL, BACKUP.

ЗМІСТ

ВСТУП

У сучасному світі інформаційні технології стали невід'ємною частиною діяльності підприємств, урядових установ, наукових центрів та побутового життя. Комп'ютерні мережі відіграють ключову роль у забезпеченні швидкого обміну інформацією, доступу до ресурсів та підтримки безперервної роботи критичних систем. Однак із розширенням цифрового простору зростають і загрози, пов'язані з кібербезпекою.

Швидке збільшення обсягів даних, поширення хмарних технологій та інтеграція IoT-рішень створюють нові виклики для захисту інформації. Дані переміщуються між різними системами та фізичними локаціями, що розширює можливості для несанкціонованого доступу або атак. Зловмисники застосовують дедалі складніші методи, включаючи фішингові кампанії, шкідливе програмне забезпечення, експлойти уразливостей та атаки на мережеву інфраструктуру.

У цьому контексті забезпечення безпеки комп'ютерних мереж стає пріоритетним завданням. Захисні механізми повинні не лише запобігати проникненню зловмисників, а й забезпечувати виявлення та оперативне реагування на загрози. Ефективна система захисту охоплює широкий спектр технологій, серед яких міжмережеві екрани (фаєрволи), системи виявлення вторгнень (IDS/IPS), криптографічні алгоритми для захисту даних та політики контролю доступу.

Одним із ключових заходів є впровадження багатофакторної автентифікації, яка значно ускладнює несанкціонований доступ, оскільки вимагає підтвердження особи за кількома критеріями (пароль, біометричні дані, одноразовий код). Важливу роль також відіграє управління правами доступу: користувачі повинні мати лише ті привілеї, які їм необхідні для виконання своїх функцій. Моніторинг активності мережі та користувачів, використання SIEM-систем для кореляції

подій та аналізу аномалій дозволяють вчасно виявляти потенційні загрози та запобігати масштабним інцидентам.

Актуальність дослідження зумовлена необхідністю підвищення рівня безпеки корпоративних мереж, забезпечення захисту даних та протидії сучасним кіберзагрозам. Недостатнє використання превентивних заходів, відсутність механізмів детекції та нерегулярне оновлення систем можуть спричинити критичні наслідки для бізнесу.

Метою роботи є комплексне дослідження загроз інформаційної безпеки та розробка методів удосконалення системи захисту комп'ютерної мережі.

Завдання дослідження включають:

- Аналіз сучасних загроз інформаційній безпеці та їхніх векторів атаки.
- Дослідження методів та засобів захисту корпоративних мереж, включаючи міжмережеві екрани, IDS/IPS та SIEM-рішення.
- Оцінку поточних недоліків у політиках доступу, контролі користувачів та шифруванні даних.
- Розробку рекомендацій щодо оптимізації архітектури мережевої безпеки.

Метод дослідження. Робота базується на аналізі наукових праць, технічної документації та практичних випадків кіберзагроз. Використовується метод моделювання ризиків, порівняльний аналіз ефективності захисних механізмів та статистичний підхід до оцінки вразливостей.

Об'єкт дослідження – методи та засоби забезпечення інформаційної безпеки комп'ютерних мереж.

Предметом дослідження є структурні, функціональні та технічні особливості механізмів захисту мережевої інфраструктури, включаючи міжмережеві екрани, системи виявлення вторгнень, криптографічні алгоритми та контроль доступу.

Практичне значення. Запропоновані підходи до захисту комп’ютерної мережі можуть бути використані в корпоративних середовищах для підвищення рівня безпеки, впровадження адаптивних механізмів реагування та мінімізації ризиків витоку даних.

У межах роботи досліджено сучасні методи та засоби забезпечення інформаційної безпеки комп’ютерних мереж, проведено класифікацію загроз за їхнім походженням та впливом, здійснено аналіз ключових механізмів захисту, включаючи міжмережеві екрани, системи виявлення вторгнень та криптографічні засоби. Виявлено поточні недоліки у політиках доступу, контролі користувачів та управлінні ризиками, а також визначено перспективні напрямки вдосконалення мережевої безпеки, орієнтовані на інтеграцію адаптивних та інтелектуальних технологій захисту.

РОЗДІЛ 1 ОСОБЛИВОСТІ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ

1.1 Сутність інформаційної безпеки та сучасні загрози в комп'ютерних мережах

Інформаційна безпека є однією з ключових складових сталого функціонування підприємств, установ та організацій у цифрову епоху. В умовах глобальної інформатизації забезпечення конфіденційності, цілісності та доступності інформації стає критично важливим чинником для збереження конкурентоспроможності та репутації суб'єкта господарювання [1].

Відповідно до міжнародного стандарту ISO/IEC 27000:2018, інформаційна безпека трактується як збереження конфіденційності, цілісності та доступності інформації, а також, за потреби, й інших її характеристик, таких як автентичність, відповідальність, заперечуваність та надійність. Іншими словами, інформаційна безпека передбачає реалізацію політик, процедур та технічних засобів, які дають змогу запобігти несанкціонованому доступу, зміні або втраті інформації [2].

До базових принципів інформаційної безпеки належать:

– конфіденційність (Confidentiality) – забезпечення того, що інформація доступна лише уповноваженим особам;

– цілісність (Integrity) – збереження точності й повноти інформації та методів її обробки;

– доступність (Availability) – гарантування своєчасного і безперешкодного доступу до інформації користувачам, які мають на це право.

Ці три складові формують так звану CIA-тріаду, яка є фундаментом будь-якої системи інформаційної безпеки. Модель CIA-тріади в інформаційній безпеці показано на рис. 1.1.

У сучасному бізнес-середовищі, де переважна більшість операцій здійснюється в цифровій формі, роль інформаційної безпеки не обмежується лише

технічними заходами. Вона охоплює широкий спектр управлінських, організаційних і правових заходів, що включають політики доступу до ресурсів, аудит, контроль змін, резервне копіювання, навчання персоналу тощо [3].

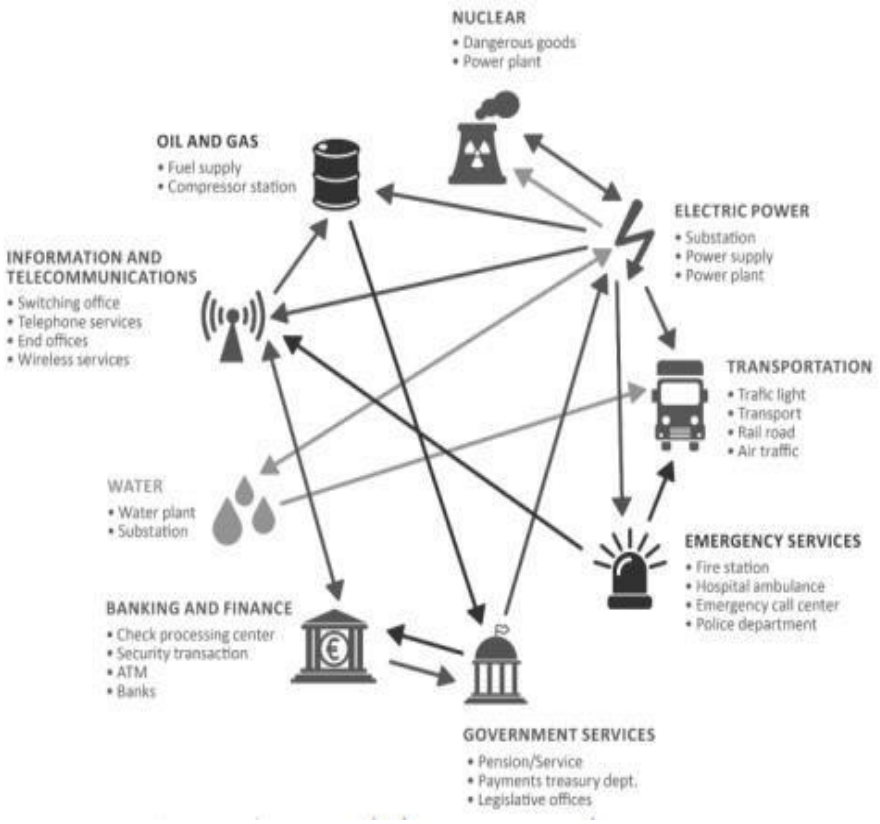

Рисунок 1.1 – Модель CIA-тріади в інформаційній безпеці

Інформаційна безпека є не лише технічним, а й стратегічним елементом корпоративного управління, що сприяє досягненню сталого розвитку підприємства, зниженню фінансових ризиків та зміцненню довіри з боку клієнтів і партнерів.

У контексті побудови ефективної системи захисту комп’ютерної мережі особливого значення набуває розуміння характеру загроз, з якими вона може зіткнутися. Загрози інформаційної безпеки – це потенційні або реальні дії, події чи процеси, які можуть завдати шкоди інформації, її носіям або системам, що забезпечують обробку, зберігання та передавання даних [4].

Існує кілька класифікаційних підходів до поділу загроз. Найбільш поширеною є класифікація за природою походження, що передбачає поділ на такі основні групи:

– техногенні загрози – пов’язані з несправністю або виходом з ладу технічних засобів, енергопостачання, комунікацій тощо;

– технічні загрози – результат експлуатації вразливостей у програмному або апаратному забезпеченні (наприклад, шкідливе ПЗ, логічні бомби) [5];

– організаційні загрози – зумовлені відсутністю або недотриманням регламентів, інструкцій, політик безпеки;

– людські загрози – навмисні або ненавмисні дії персоналу, користувачів або третіх осіб (наприклад, соціальна інженерія, помилки при роботі з даними).

Інший важливий критерій класифікації – вектор загрози, тобто її джерело щодо системи:

– внутрішні загрози – походять від співробітників організації або користувачів, які мають доступ до мережі;

– зовнішні загрози – ініційовані ззовні (наприклад, хакерські атаки, спроби несанкціонованого доступу з інтернету).

Класифікація загроз мережам за походженням і впливом відображена в табл. 1.1.

Таблиця 1.1 – Класифікація загроз мережам за походженням і впливом

№ з/п	Тип загроз	Джерело виникнення	Приклади	Можливі наслідки
1.	Техногенні	Інфраструктурні збої	Відмова електропостачання, пожежа	Знищення носіїв даних, збій систем
2.	Технічні	Програмне/апаратне СЗ	Віруси, трояни, уразливості ОС	Витік, модифікація, втрата даних
3.	Організаційні	Неврегульовані процеси	Відсутність політик, аудитів	Несанкціонований доступ, інциденти
4.	Людські	Користувачі/персонал	Фішинг, помилкове введення даних	Компрометація системи, порушення
5.	Внутрішні	Співробітники, ІТфахівці	Зловживання правами доступу	Витік конфіденційної інформації
6.	Зовнішні	Хакери, конкуренти	DDoS, злом паролів, сніфінг	Параліч мережі, крадіжка даних

Зазначена класифікація є основою для побудови стратегії управління ризиками, яка, своєю чергою, визначає пріоритети захисту й ефективність впроваджених заходів безпеки. Важливо враховувати, що загрози часто виникають у комбінації: наприклад, технічна вразливість може бути використана зовнішнім суб’єктом, а організаційна слабкість – стати підґрунтям для внутрішнього порушення.

У сучасному інформаційному просторі загрози, що спрямовані на комп’ютерні мережі, відзначаються не лише високою частотою, а й зростаючою складністю реалізації. Характерною особливістю новітніх атак є їх мультивекторність, а також здатність адаптуватися до специфіки мережевої інфраструктури цільового об’єкта.

До найбільш поширених типів атак, які фіксуються в корпоративних мережах, належать [6]:

– фішинг (phishing) – вид соціальної інженерії, спрямований на введення користувача в оману з метою отримання конфіденційних даних (логінів, паролів, банківської інформації);

– DDoS-атаки (Distributed Denial of Service) – навмисне перевантаження інформаційної системи великою кількістю запитів з різних джерел з метою виведення її з ладу;

– шкідливе програмне забезпечення (malware) – віруси, трояни, вимагачі (ransomware), які здатні порушити цілісність або доступність даних;

– експлойти (exploits) – програми або скрипти, що використовують вразливості в ПЗ для несанкціонованого доступу до системи;

– атакуючі боти (botnets) – мережі заражених пристроїв, які використовуються для координації масових атак, зокрема DDoS або розсилання спаму [7].

Актуальність загроз підтверджується численними резонансними кіберінцидентами, що мали місце в останні роки. Наприклад, у 2021 році міжнародна корпорація Colonial Pipeline зазнала атаки з використанням програмвимагачів, унаслідок чого на декілька днів було паралізовано постачання пального у східній частині США. Інший приклад – поширення вимогливого ПЗ Petya/NotPetya у 2017 році, яке завдало значної шкоди компаніям в Україні та по всьому світу, блокуючи роботу систем на основі Windows.

Особливе занепокоєння викликають DDoS-атаки, які часто використовуються як засіб конкурентної боротьби або кібершантажу. Їхня ефективність зумовлена простотою реалізації (через ботнети) та відносно низькими витратами на запуск [8]. Схема дії типової DDoS-атаки на підприємство представлено на ис.1.2.

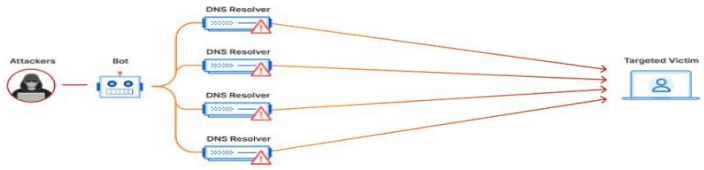

Рисунок 1.2 – Типова DDoS-атака на підприємство: схема дії

У контексті інформаційної безпеки сучасного підприємства важливо не лише ідентифікувати потенційні вектори атак, а й вчасно виявляти підозрілу активність та реалізовувати механізми нейтралізації загроз. Ефективна реакція на інциденти залежить від інтеграції превентивних, детекційних та відновлювальних заходів у єдину систему захисту [9].

Отже, інформаційна безпека є фундаментом функціонування будь-якої сучасної комп'ютерної мережі. Основу ІБ становить принципова триєдність конфіденційності, цілісності та доступності інформації. У свою чергу, загрози мережевій безпеці мають різноманітну природу – від людського фактора до складних зовнішніх атак, таких як DDoS чи використання експлойтів. Їхнє своєчасне виявлення, розуміння механізмів реалізації та класифікація за типами дають змогу сформувати цілісну картину ризиків і створити ефективну стратегію захисту інформаційного середовища підприємства.

1.2 Класифікація методів та засобів захисту мережевої інфраструктури

Превентивні заходи є першою лінією оборони в забезпеченні інформаційної безпеки комп'ютерних мереж підприємства. Їх основне завдання – запобігання несанкціонованому доступу, втраті або компрометації інформації ще до того, як загроза встигне реалізуватися. До основних превентивних методів належать механізми аутентифікації, авторизації, шифрування даних, а також застосування захищених протоколів і віртуальних приватних мереж [10].

Аутентифікація – це процес перевірки достовірності користувача або пристрою, що здійснює спробу доступу до інформаційної системи. Сучасні підприємства використовують багатофакторну аутентифікацію (MFA), яка поєднує кілька елементів: знання (пароль), володіння (смарт-карта, мобільний пристрій), притаманність (біометричні дані).

Авторизація – процес надання прав доступу до ресурсів після успішної аутентифікації. Політики авторизації встановлюють, які дії може виконувати користувач у межах системи, що запобігає зловживанню повноваженнями.

Шифрування є ключовим інструментом забезпечення конфіденційності даних як при зберіганні, так і при передаванні. Воно перетворює дані у вигляд, незрозумілий стороннім особам, без наявності відповідного ключа. У корпоративному середовищі застосовуються як симетричні (AES), так і асиметричні (RSA, ECC) алгоритми шифрування [11].

Особливу роль у захисті комунікацій відіграє впровадження віртуальних приватних мереж (VPN). VPN створює зашифрований тунель між пристроєм користувача та внутрішньою мережею підприємства, запобігаючи перехопленню даних під час їх передавання через публічні мережі.

До інших важливих інструментів належать:

– SSL/TLS (Secure Sockets Layer / Transport Layer Security) – криптографічні протоколи, які забезпечують шифрування інтернет-трафіку, зокрема в браузерах;

– PKI (Public Key Infrastructure) – інфраструктура відкритих ключів, що забезпечує управління цифровими сертифікатами, необхідними для безпечного обміну інформацією;

– Захищені протоколи передачі – такі як HTTPS (HyperText Transfer Protocol Secure), SFTP (Secure File Transfer Protocol), SMTPS тощо, які гарантують безпечне передавання даних.

Превентивні методи інформаційної безпеки відіграють фундаментальну роль у захисті сучасних інформаційних систем, оскільки їх застосування дозволяє створити багаторівневий бар'єр проти потенційних кіберзагроз ще на початкових стадіях атаки. Ці методи включають широкий спектр технологічних та організаційних заходів, таких як налаштування брандмауерів, системи контролю

доступу, шифрування даних, регулярне оновлення програмного забезпечення, впровадження політик безпеки та навчання персоналу основам кібербезпеки.

Використання превентивних підходів значною мірою знижує ймовірність успішної компрометації системи, адже створює перешкоди для зловмисників на етапі спроби вторгнення, коли система ще не зазнала безпосередньої шкоди. Крім того, впровадження превентивних методів є обов'язковою вимогою для відповідності міжнародним стандартам інформаційної безпеки, таким як ISO 27001, NIST Cybersecurity Framework, та іншим галузевим регуляторним документам, що визначають мінімальні вимоги до захисту інформаційних активів організацій.

Проте реалії сучасного кіберпростору демонструють, що навіть найдосконаліші превентивні заходи не можуть гарантувати стовідсотковий захист від усіх видів кіберзагроз, оскільки зловмисники постійно розробляють нові методи атак, використовують раніше невідомі вразливості нульового дня та застосовують складні техніки соціальної інженерії. У цьому контексті критично важливою складовою комплексної системи інформаційної безпеки стає реактивний компонент, що включає системи виявлення вторгнень, моніторинг безпеки в реальному часі та процедури швидкого реагування на інциденти.

Своєчасне виявлення аномальної активності та підозрілих дій у мережі дозволяє службам безпеки швидко ідентифікувати факт атаки та ініціювати відповідні контрзаходи, що має вирішальне значення для мінімізації потенційних наслідків кіберінциденту.

Швидке реагування на виявлені загрози включає ізоляцію скомпрометованих систем, блокування підозрілого трафіку, активацію резервних копій даних та координацію дій між різними підрозділами організації, що дозволяє обмежити зону ураження атаки та запобігти її поширенню на критично важливі системи. Така комбінована стратегія превентивних та реактивних заходів забезпечує збереження контролю над інформаційною системою навіть у випадку

часткового прориву захисту, що є ключовим фактором для підтримання безперервності бізнес-процесів та збереження довіри клієнтів і партнерів до організації. Схема роботи IDS та IPS у корпоративній мережі показано на рис.1.3.

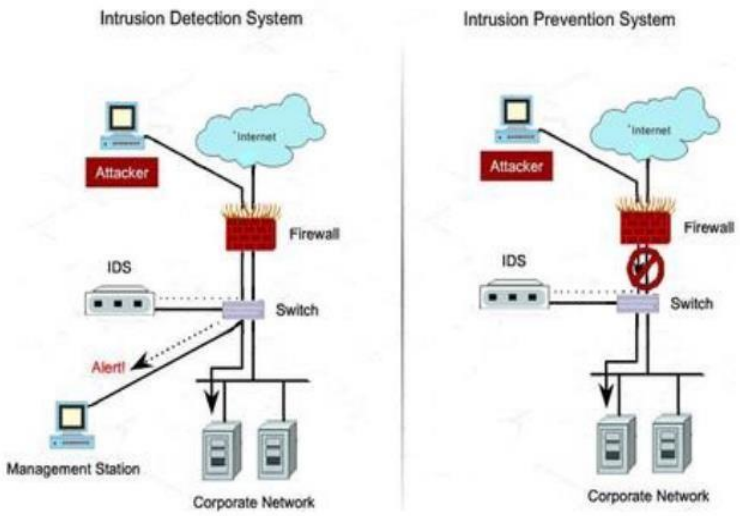

Рисунок 1.3 – Схема роботи IDS та IPS у корпоративній мережі

Серед основних технологій для таких завдань варто виділити системи IDS (Intrusion Detection System) та IPS (Intrusion Prevention System). IDS виконує функції виявлення підозрілої активності, не втручаючись у сам процес передачі даних, тоді як IPS діє активно – блокує загрозу ще до того, як вона зможе завдати шкоди [13]. У корпоративних мережах ці системи зазвичай розгортаються на межі між зовнішнім трафіком і внутрішньою мережею, фільтруючи дані в реальному часі.

SIEM (Security Information and Event Management) представляє собою один з найбільш критично важливих компонентів сучасної архітектури кібербезпеки, який функціонує як центральна нервова система для моніторингу та управління інформаційною безпекою в масштабах всієї організації. Ця комплексна технологічна платформа поєднує в собі дві ключові функціональності: управління інформацією про безпеку (Security Information Management) та управління

подіями безпеки (Security Event Management), що дозволяє створити єдиний централізований центр операцій безпеки з можливістю отримання повного уявлення про стан захищеності всієї інформаційної інфраструктури.

Основною перевагою SIEM-систем є їх здатність до централізованого збору величезних обсягів даних з найрізноманітніших джерел інформації, включаючи мережеве обладнання, сервери, робочі станції, системи контролю доступу, антивірусні програми, брандмауери, системи запобігання вторгненням, бази даних, веб-сервери, хмарні сервіси та навіть фізичні системи безпеки, що забезпечує формування комплексного та цілісного погляду на всі процеси, які відбуваються в інформаційному середовищі організації.

Процес збору даних в SIEM-системах здійснюється через різноманітні методи інтеграції, включаючи використання агентів, встановлених на цільових системах, технології syslog для передачі журналів подій, SNMP-протоколи для моніторингу мережевого обладнання, API-інтерфейси для взаємодії з хмарними сервісами та спеціалізовані коннектори для інтеграції з конкретними додатками та системами.

Зібрані дані проходять процес нормалізації та стандартизації, що дозволяє привести інформацію з різних джерел до єдиного формату, придатного для подальшого аналізу та кореляції. Ключовою особливістю SIEM-платформ є їх здатність до аналізу подій у реальному часі, що означає можливість обробки та інтерпретації інформації про безпеку одразу після її надходження, без значних затримок, які могли б критично вплинути на ефективність виявлення та реагування на загрози.

Аналітичні можливості SIEM-систем базуються на використанні складних алгоритмів корреляції подій, які дозволяють виявляти зв'язки між, здавалося б, незалежними подіями з різних джерел та ідентифікувати складні багатоетапні атаки, які могли б залишитися непоміченими при аналізі окремих компонентів системи. Система автоматичних правил і політик безпеки, вбудована в SIEM-

платформи, забезпечує можливість миттєвого реагування на виявлені аномалії, порушення встановлених політик безпеки або підозрілі паттерни активності.

Дані правила можуть бути як стандартними, розробленими на основі відомих сигнатур атак і найкращих практик кібербезпеки, так і кастомізованими відповідно до специфічних вимог і особливостей конкретної організації. При спрацьовуванні правил система автоматично генерує сповіщення різних рівнів критичності, які можуть надсилатися відповідальному персоналу через електронну пошту, SMS, push-уведомлення або інтегровані системи управління інцидентами.

Сучасні SIEM-рішення також інтегрують технології штучного інтелекту та машинного навчання, що дозволяє системі не лише виявляти відомі типи загроз, але й ідентифікувати раніше невідомі аномалії та потенційні загрози на основі аналізу поведінкових паттернів та статистичних відхилень від нормальної активності. Це особливо важливо в контексті протидії розвинутим постійним загрозам (Advanced Persistent Threats), які характеризуються тривалим перебуванням у системі та використанням складних технік приховування своєї присутності. Завдяки можливостям візуалізації та створення детальних звітів, SIEM-системи забезпечують не лише оперативне реагування на інциденти, але й стратегічний аналіз трендів безпеки, що дозволяє організаціям вдосконалювати свої захисні стратегії та демонструвати відповідність регуляторним вимогам у сфері кібербезпеки.

Не менш важливим є постійний моніторинг і логування подій. Збереження записів про активність користувачів, доступ до ресурсів, зміни в системах тощо дозволяє не тільки швидко виявити інцидент, а й розслідувати його причини. Такий підхід забезпечує повноцінну картину стану інформаційної безпеки на підприємстві.

Отже, виявлення загроз і реагування є критично важливим компонентом багаторівневої моделі захисту, що забезпечує оперативну відповідь на атаки та дозволяє захистити мережу навіть у разі прориву первинної лінії оборони [14].

Забезпечення інформаційної безпеки не обмежується виключно програмними чи мережевими засобами. Важливу роль у комплексному захисті комп'ютерних мереж відіграють інженерно-технічні та адміністративні заходи, які створюють додаткові рівні безпеки на фізичному та організаційному рівнях.

Серед інженерно-технічних засобів насамперед варто відзначити контроль фізичного доступу до IT-інфраструктури. До цього належать системи відеоспостереження, електронні замки, турнікети, охоронні сигналізації. Вони запобігають несанкціонованому доступу до серверних приміщень, робочих станцій або мережевого обладнання, що має критичне значення для функціонування підприємства.

Не менш важливою є адміністративна складова захисту, яка включає розробку внутрішніх політик безпеки, регламентів доступу, правил поводження з конфіденційною інформацією. Одним із ключових напрямів є підвищення обізнаності персоналу через регулярне навчання, інструктажі та моделювання типових інцидентів (наприклад, фішингових атак) [15].

Резервне копіювання та комплексні плани відновлення даних являють собою один з найбільш фундаментальних та критично важливих компонентів стратегії забезпечення безперервності бізнесу та кібербезпеки, оскільки вони функціонують як остання лінія захисту проти катастрофічних сценаріїв втрати інформації та служать гарантією можливості відновлення нормального функціонування організації навіть за найнесприятливіших обставин.

Сучасні системи резервного копіювання далеко виходять за межі простого створення копій файлів і представляють собою складні технологічні екосистеми, які включають автоматизовані процедури створення резервних копій на різних рівнях інфраструктури, від окремих файлів та баз даних до повних образів

віртуальних машин та фізичних серверів, що забезпечує можливість відновлення як окремих документів, так і цілих інформаційних систем у їх повному обсязі.

Стратегія резервного копіювання базується на принципі багаторівневого захисту, який передбачає створення декількох незалежних копій критично важливих даних з розміщенням їх у різних локаціях та на різних типах носіїв інформації, що значно знижує ймовірність одночасної втрати всіх резервних копій внаслідок локальних катастроф, технічних збоїв або цілеспрямованих атак.

Популярна концепція «3-2-1» передбачає наявність щонайменше трьох копій важливих даних, збережених на двох різних типах носіїв, з обов'язковим розміщенням однієї копії в географічно віддаленому місці, що може включати хмарні сховища, віддалені дата-центри або фізично ізольовані системи зберігання. Сучасні технології дозволяють реалізувати як традиційні методи резервного копіювання на магнітні стрічки та зовнішні жорсткі диски, так і передові рішення, включаючи хмарне резервне копіювання, синхронну та асинхронну реплікацію даних, snapshot-технології та інкрементальне копіювання, яке дозволяє зберігати лише зміни, внесені з моменту останнього резервного копіювання.

Плани відновлення даних та аварійного відновлення (Disaster Recovery Plans) представляють собою детально розроблені документи, які визначають послідовність дій, відповідальних осіб, часові рамки та технічні процедури, необхідні для швидкого та ефективного відновлення нормального функціонування інформаційних систем після інциденту. Ці плани включають детальну інвентаризацію всіх критично важливих систем та даних з присвоєнням їм пріоритетів відновлення, визначення максимально допустимого часу простою (Recovery Time Objective – RTO) та максимально допустимих втрат даних (Recovery Point Objective – RPO) для кожної системи, що дозволяє оптимізувати розподіл ресурсів та зусиль під час процесу відновлення.

Важливою складовою планів відновлення є регулярне тестування процедур відновлення через проведення навчальних тренувань та симуляцій різних

сценаріїв катастроф, що дозволяє виявити потенційні проблеми та недоліки в планах до настання реальної критичної ситуації.

У контексті сучасних кіберзагроз особливої актуальності набуває захист резервних копій від ransomware-атак та інших видів шкідливого програмного забезпечення, яке спеціально розроблене для знищення або шифрування резервних копій з метою ускладнення процесу відновлення та примушення жертв до сплати викупу. Для протидії таким загрозам використовуються технології незмінних резервних копій (immutable backups), які неможливо змінити або видалити протягом визначеного періоду часу, air-gapped рішення, які передбачають фізичну ізоляцію резервних копій від основної мережі, та принцип «нульової довіри» до резервних систем, який вимагає додаткової автентифікації та авторизації для доступу до резервних копій.

Практичний досвід численних організацій, які зіткнулися з серйозними кіберінцидентами, природними катастрофами або технічними збоями, переконливо демонструє, що наявність добре організованої та регулярно тестованої системи резервного копіювання може скоротити час відновлення нормального функціонування з тижнів або місяців до годин або днів, що критично важливо для збереження операційної ефективності та конкурентоспроможності організації.

Фінансові переваги інвестицій у надійні системи резервного копіювання стають особливо очевидними при порівнянні витрат на впровадження та підтримання таких систем з потенційними втратами від простою бізнес-процесів, відновлення втрачених даних, сплати штрафів за порушення вимог щодо захисту персональних даних, компенсацій клієнтам та партнерам, а також довгострокових репутаційних збитків, які можуть негативно впливати на довіру клієнтів та ринкову позицію компанії протягом багатьох років після інциденту.

Статистичні дані показують, що організації з ефективними системами резервного копіювання та планами відновлення зазвичай відновлюють свою

діяльність у 3-5 разів швидше та несуть у 2-10 разів менші фінансові втрати порівняно з компаніями, які не мали адекватних систем захисту даних, що робить інвестиції в резервне копіювання одним з найбільш економічно ефективних заходів забезпечення кібербезпеки та безперервності бізнесу.

Загалом, інженерно-технічні та адміністративні засоби створюють стійке середовище безпеки, яке доповнює програмні й мережеві компоненти, формуючи цілісну систему протидії загрозам [16]. Порівняльна характеристика засобів захисту мереж показано утабл.1.2.

Таблиця 1.2 – Порівняльна характеристика засобів захисту мереж

№ з/п	Засіб захисту	Рівень впливу	Основне призначення	Приклади реалізації
1.	Відеоспостереже ння, замки, турнікети	Фізичний	Захист від несанкціонованого доступу	Камери, зчитувачі карт, біометрія
2.	Політики безпеки, навчання персоналу	Організацій ний	Запобігання помилкам та зловживанням	Регламент, тренінги, інструкції
3.	Резервне копіювання та відновлення	Технічний/ відновлювал ьний	Забезпечення збереження та відновлення даних	Щоденний backup, DRP-план (Disaster Recovery Plan)

Отже, превентивні, виявляючі та адміністративно-технічні засоби захисту утворюють багаторівневу систему безпеки комп’ютерних мереж, де кожен елемент виконує взаємодоповнюючу функцію. Від ефективної аутентифікації та шифрування – до виявлення загроз у реальному часі та контролю фізичного доступу – усі ці складові забезпечують цілісність, безперервність і надійність інформаційної інфраструктури підприємства.

1.3 Нормативно-правова база та стандарти інформаційної безпеки

Законодавче регулювання є фундаментом побудови ефективної системи інформаційної безпеки на рівні держави, установ і підприємств. В Україні сформована базова нормативно-правова база, яка визначає правові засади захисту інформації, встановлює вимоги до технічних і організаційних заходів, а також розмежовує повноваження відповідальних органів [17].

Ключовими законодавчими актами в цій сфері є Закон України «Про інформацію» та Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». Перший визначає загальні принципи інформаційних правовідносин, форми доступу до інформації, вимоги до її захисту та класифікації. Другий встановлює правові й організаційні засади захисту інформації в інформаційно-телекомунікаційних системах, включно з державними стандартами, сертифікацією технічних засобів і порядком створення комплексних систем захисту.

Кабінетом Міністрів України затверджено низку постанов і розпоряджень, що деталізують застосування законодавства в сфері ІБ. Особливої уваги заслуговують нормативи технічного та криптографічного захисту інформації, які мають бути дотримані організаціями, що обробляють інформацію з обмеженим доступом [18].

Важливе місце в системі регулювання займають державні стандарти України (ДСТУ), які відповідають міжнародним вимогам та охоплюють як загальні вимоги до інформаційної безпеки (наприклад, ДСТУ ISO/IEC 27001), так і специфічні аспекти (захист персональних даних, електронний документообіг, шифрування тощо).

Серед органів, відповідальних за реалізацію політики у сфері кібербезпеки, слід виділити Адміністрацію Державної служби спеціального зв’язку та захисту інформації України (Держспецзв’язку), яка здійснює технічний нагляд,

сертифікацію, контроль за дотриманням стандартів і нормативів. Важливу координаційну функцію також виконує Національний координаційний центр кібербезпеки (НКЦК) при Раді національної безпеки і оборони України, який формує стратегію та оперативно реагує на загрози національного рівня. Законодавче поле інформаційної безпеки в Україні представляє собою комплексну та багаторівневу систему нормативно-правових актів, яка формує цілісну правову основу для регулювання всіх аспектів захисту інформації та кібербезпеки в державі, охоплюючи як фундаментальні конституційні принципи права на інформацію та її захист, так і деталізовані технічні вимоги до конкретних категорій інформаційних систем та технологій. Ця нормативна база включає закони України «Про інформацію», «Про захист персональних даних», «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-телекомунікаційних системах», численні підзаконні акти, технічні регламенти, національні стандарти та галузеві нормативи, які в сукупності створюють всеохоплюючу систему правового регулювання, що визначає права та обов'язки громадян, організацій та державних органів у сфері інформаційної безпеки. Законодавство встановлює загальні принципи регулювання, такі як забезпечення балансу між доступністю інформації та її захистом, пропорційність заходів безпеки рівню загроз, відповідальність за порушення вимог інформаційної безпеки, прозорість процедур обробки персональних даних та обов'язковість дотримання міжнародних стандартів у сфері кібербезпеки.

Конкретні вимоги до організацій, визначені українським законодавством, охоплюють широкий спектр зобов'язань, включаючи необхідність розробки та впровадження політик інформаційної безпеки, проведення регулярних аудитів безпеки, забезпечення відповідного рівня технічного та криптографічного захисту інформації, навчання персоналу основам кібербезпеки, повідомлення про кіберінциденти до відповідних державних органів у встановлені терміни, ведення документації з питань інформаційної безпеки та забезпечення можливості

проведення перевірок з боку контролюючих органів. Особливі вимоги встановлені для операторів критичної інфраструктури, провайдерів телекомунікаційних послуг, фінансових установ, органів державної влади та місцевого самоврядування, освітніх та медичних закладів, які мають дотримуватися підвищених стандартів захисту інформації та регулярно звітувати про стан кібербезпеки у своїх організаціях.

Технічні засоби захисту інформації підлягають обов'язковій сертифікації відповідно до національних стандартів, що гарантує їх відповідність встановленим вимогам безпеки та ефективність у протидії актуальним кіберзагрозам. Законодавство визначає категорії технічних засобів, які підлягають сертифікації, процедури проведення сертифікаційних випробувань, вимоги до акредитованих лабораторій та органів сертифікації, а також механізми контролю за дотриманням вимог сертифікованими засобами протягом усього їх життєвого циклу. Відповідальні суб'єкти у сфері інформаційної безпеки включають

Службу безпеки України, Державну службу спеціального зв'язку та захисту інформації, Національну поліцію, кіберполіцію, галузеві регулятори та інші державні органи, кожен з яких має специфічні повноваження та відповідальність за забезпечення кібербезпеки у відповідних сферах діяльності, що створює систему розподіленої відповідальності та взаємодії між різними рівнями державного управління.

Впровадження міжнародних стандартів інформаційної безпеки в Україні відбувається в контексті європейської інтеграції та глобалізації інформаційного простору, що робить адаптацію світових найкращих практик не просто рекомендацією, а життєвою необхідністю для забезпечення конкурентоспроможності української економіки та ефективної участі країни у міжнародних економічних та політичних процесах.

Міжнародні стандарти, такі як ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework, COBIT, ITIL та інші визнані методології, надають

організаціям структуровані підходи до управління інформаційною безпекою, які базуються на десятиліттях практичного досвіду та наукових досліджень у галузі кібербезпеки. Ці стандарти функціонують як універсальний інструмент гармонізації процесів захисту інформації, забезпечуючи можливість створення єдиних підходів до оцінки ризиків, впровадження контрольних заходів, моніторингу ефективності систем безпеки та безперервного вдосконалення захисних механізмів незалежно від розміру організації, галузевої специфіки або географічного розташування.

Особливою перевагою міжнародних стандартів є їх здатність забезпечувати взаємну сумісність та довіру між організаціями з різних країн та юрисдикцій, що критично важливо для міжнародної торгівлі, транскордонного обміну даними та співпраці у сфері кібербезпеки. Впровадження цих стандартів дозволяє українським організаціям демонструвати свою відповідність світовим вимогам безпеки, що відкриває доступ до міжнародних ринків, спрощує процедури аудиту та сертифікації для іноземних партнерів, підвищує довіру інвесторів та клієнтів, а також забезпечує основу для ефективної міжнародної співпраці у протидії кіберзагрозам.

Стандарти також сприяють створенню прозорої та підзвітної системи управління ризиками, яка дозволяє керівництву організацій приймати обґрунтовані рішення щодо інвестицій у кібербезпеку, ефективно розподіляти ресурси між різними напрямками захисту та демонструвати стейкхолдерам свою відповідальність у питаннях захисту інформації, що особливо важливо в умовах зростаючих регуляторних вимог та підвищеної уваги суспільства до питань приватності та кібербезпеки.

Найбільш визнаним у світі є стандарт ISO/IEC 27001, який визначає вимоги до створення, впровадження, експлуатації, моніторингу, перегляду, підтримки та вдосконалення системи управління інформаційною безпекою (СУІБ). Основу стандарту становить підхід, орієнтований на оцінку ризиків та їх мінімізацію

через впровадження політик, контролів і процедур. Документ містить вимоги до контекста організації, лідерства, планування, підтримки, функціонування, оцінки результативності та вдосконалення [20].

Американською альтернативою ISO є NIST Cybersecurity Framework, розроблений Національним інститутом стандартів і технологій США. Цей фреймворк орієнтований на практичну реалізацію заходів безпеки і містить п’ять основних функцій: ідентифікація активів і ризиків, захист систем, виявлення інцидентів, реагування на порушення та відновлення після атак. Його гнучкість та адаптивність дозволяє впроваджувати його як у малому бізнесі, так і в критично важливих інфраструктурах.

До інших поширених міжнародних підходів належать:

- COBIT (Control Objectives for Information and Related Technologies) – модель корпоративного управління IT-процесами;
- ITIL (Information Technology Infrastructure Library) – бібліотека найкращих практик з управління IT-послугами;
- CIS Controls – набір базових і пріоритетних технічних заходів безпеки, рекомендований Центром інтернет-безпеки (CIS).

Міжнародні стандарти створюють універсальну основу для впровадження інформаційної безпеки на стратегічному, тактичному та операційному рівнях, забезпечуючи організаціям не лише відповідність вимогам регуляторів, а й підвищення довіри з боку клієнтів, партнерів і ринку загалом.

Впровадження міжнародних стандартів інформаційної безпеки, зокрема ISO/IEC 27001, є важливим кроком для підприємств, які прагнуть систематизувати управління ризиками, підвищити довіру клієнтів і забезпечити стабільність бізнес-процесів в умовах зростаючої кіберзагроз. Цей процес є складним, багатоступеневим і потребує залучення не лише технічних фахівців, а й менеджменту вищого рівня [21]. Порівняльна характеристика ISO/IEC 27001 та NIST Cybersecurity Framework відображено в табл.1.3.

Таблиця 1.3 – Порівняльна характеристика ISO/IEC 27001 та NIST Cybersecurity Framework

№ з/п	Критерій	ISO/IEC 27001	NIST Cybersecurity Framework
1.	Походження	Міжнародна організація зі стандартизації	Національний інститут стандартів США (NIST)
2.	Основна мета	Побудова СУІБ	Практичне управління кіберризиками
3.	Структура	10 розділів + Додаток А (контроли безпеки)	5 функцій, 23 категорії, 108 підкатегорій
4.	Підхід	Формальний, орієнтований на сертифікацію	Гнучкий, адаптивний
5.	Сертифікація	Можлива офіційна сертифікація	Сертифікація не передбачена
6.	Аудиторська оцінка	Обов’язкова для відповідності стандарту	Не обов’язкова, проте рекомендована
7.	Використання	Переважно в Європі, міжнародних компаніях	Переважно в США, у приватному секторі

Першим етапом є оцінка поточного стану безпеки та виявлення ризиків. На цьому етапі підприємство ідентифікує інформаційні активи, аналізує загрози й вразливості, а також визначає ймовірність та наслідки реалізації тих чи інших ризиків. Результатом є матриця ризиків, яка слугує базою для прийняття рішень щодо впровадження необхідних заходів захисту [22].

Наступним кроком є розробка політик інформаційної безпеки та створення документації, яка регулює правила доступу, обробки, зберігання й передачі даних. Ці документи мають бути узгоджені з загальною стратегією підприємства та відповідати вимогам стандарту ISO 27001.

На третьому етапі відбувається впровадження організаційних і технічних заходів, передбачених політиками: це може включати впровадження систем контролю доступу, шифрування, резервного копіювання, а також навчання персоналу [23].

Переваги сертифікації ISO/IEC 27001 для бізнесу є очевидними:

- підвищення довіри клієнтів, партнерів і регуляторів;
- зниження ризиків інформаційних інцидентів та пов’язаних з ними фінансових втрат;
- забезпечення відповідності законодавчим вимогам, зокрема у сфері захисту персональних даних;
- створення конкурентної переваги на ринку, особливо в сегментах, де безпека інформації є критично важливою (банківська справа, телеком, IT-аутсорсинг).

Отже, впровадження стандарту ISO/IEC 27001 – це не лише вимога часу, а й стратегічний інструмент побудови довготривалої, стійкої та надійної системи управління інформаційною безпекою на підприємстві.

РОЗДІЛ 2 АНАЛІЗ ІСНУЮЧОЇ СИСТЕМИ ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

2.1 Опис мережевої інфраструктури та інформаційних активів підприємства

Для оцінки ефективності системи захисту комп'ютерної мережі важливо мати чітке уявлення про її структуру, складові елементи та взаємозв'язки. У цьому підпункті здійснено детальний аналіз фізичної та логічної архітектури мережі, а також складено реєстр основного обладнання та інформаційних активів підприємства [24].

Рисунок 2.1 – Схема фізичної мережі підприємства (локальна мережа, серверна, доступ до інтернету)

Рисунок 2.1. демонструє фізичну структуру мережі підприємства, побудовану за класичною схемою з чітким розмежуванням на зовнішній і внутрішній сегменти. Центральним елементом є маршрутизатор, що забезпечує

з’єднання з глобальною мережею Інтернет. Він підключений до комутатора, який виконує функцію розподілу трафіку між внутрішніми підсистемами [25].

Комутатор з’єднує три основні блоки: локальну мережу, що включає робочі станції користувачів; серверну частину, де розміщені файлові сервери, поштові та бази даних; а також демілітаризовану зону (DMZ) – сегмент, призначений для розміщення публічних ресурсів (веб-серверів, поштових шлюзів), доступ до яких здійснюється ззовні. Така структура дозволяє фізично відокремити критичні ресурси від потенційно вразливих елементів і спростити контроль над потоками даних [26].

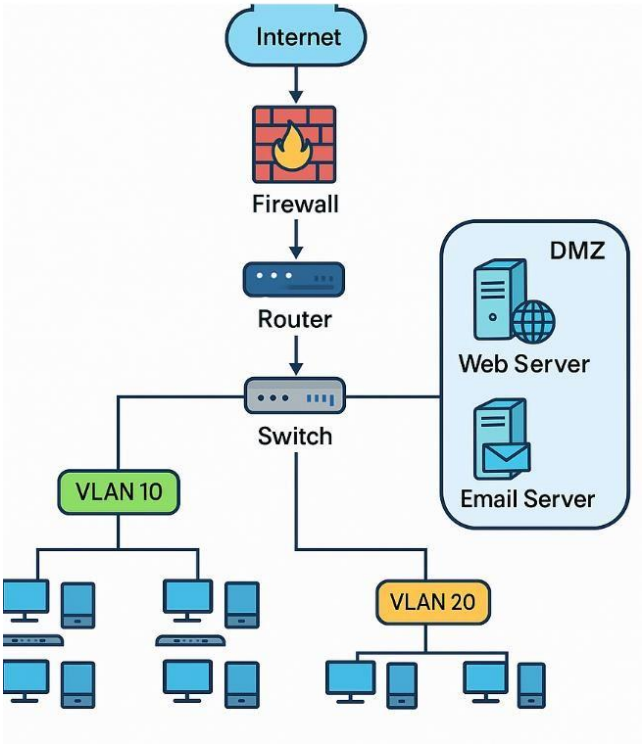

Рисунок 2.2 – Логічна структура з’єднань, VLAN, DMZ-сегмент

Рис. 2.2 ілюструє логічну структуру мережевих з’єднань на підприємстві із впровадженими віртуальними локальними мережами (VLAN) та сегментом DMZ. Центральним елементом виступає маршрутизатор, який отримує доступ до інтернету через фаєрвол. Саме фаєрвол здійснює первинну фільтрацію трафіку та

передає його до маршрутизатора, що, своєю чергою, з’єднаний із комутатором [27].

На рівні комутатора реалізовано поділ на VLAN 10 (наприклад, бухгалтерія та адміністрація) і VLAN 20 (відділ продажу), що дозволяє ізолювати трафік між сегментами й обмежити можливість горизонтального поширення загроз. Окремо винесено DMZ-сегмент, у якому розміщено публічні ресурси, такі як вебсервер і поштовий сервер. Це забезпечує додатковий рівень захисту: у разі компрометації DMZ зловмисник не отримає прямого доступу до внутрішньої мережі.

Таблиця, відображена в додатку А.1 дозволяє побачити архітектуру ключових пристроїв мережі, їх IP-адресацію, призначення та поточний стан. Особливу увагу слід звернути на частково активні або резервні пристрої, оскільки їх недоступність у критичний момент може спричинити порушення цілісності сервісів або втрату даних.

Загалом така логічна архітектура сприяє підвищенню рівня мережевої безпеки, централізації управління трафіком та зручному масштабуванню інфраструктури без шкоди для цілісності системи.

Для побудови якісної системи захисту та управління трафіком необхідно мати чітке уявлення про активне мережеве обладнання, яке забезпечує функціонування комп’ютерної мережі підприємства. Регулярний аудит цього переліку, а також оновлення прошивок та моніторинг стану обладнання є обов’язковою умовою підтримки надійної інфраструктури інформаційної безпеки підприємства [28].

У процесі аналізу мережевої інфраструктури особливу увагу було приділено налаштуванням основного маршрутизатора та комутаторів, оскільки саме ці пристрої контролюють маршрутизацію, розподіл трафіку, безпеку доступу та управління IP-адресацією.

Як видно з таблиці 2.1, основний маршрутизатор виконує функції NAT, DHCP та фільтрації трафіку за допомогою Access Control Lists (ACL), що дозволяє

регламентувати зовнішні з’єднання та зменшити вразливість системи до зовнішніх атак.

Таблиця 2.1 – Налаштування основного маршрутизатора та комутаторів підприємства

№	Пристрій	Інтерфейси / порти	Налаштовано ACL	NAT / PAT	DHCP-сервер	Коментар
1	MikroTik RB3011	eth1 – WAN, eth2-eth10 – LAN	ACL дозволяє лише HTTP, HTTPS, VPN	Ввімкнено NAT на eth1	Так, IPдіапазон 192.168.0.100–199	Статична маршрутизація + фаєрвол фільтрує UDP
2	Cisco Catalyst 2960-X	FastEthernet0/1–0/24	ACL між VLAN 10 і VLAN 20	Ні	Ні	VLAN 10 – офіс, VLAN 20 – відділ продажу
3	TP-Link TL-SG1024D	GigabitPort1 – 24	Не підтримується	Ні	Ні	Dumb switch, використовується для простого розгалуження

Основний комутатор Cisco має конфігуровані VLAN, що дозволяє сегментувати трафік за відділами і контролювати взаємодію між підрозділами підприємства [29].

Натомість простіші комутатори нижчого рівня (як-от TP-Link TLSG1024D) не підтримують розширені функції безпеки, що обмежує можливість гнучкого управління трафіком і вимагає уважного контролю за їх фізичним доступом. Реєстр інформаційних систем підприємствапоказано в додатку А.2

Отримані дані дозволяють зробити висновок про наявність структурованої, але частково уразливої мережевої інфраструктури. Сильними сторонами є впровадження VLAN, наявність сегменту DMZ та базова фільтрація трафіку. Водночас виявлено обмежену функціональність окремих пристроїв і необхідність оновлення політик доступу та обліку активів. Класифікація активів за критичністю та рівнем доступу відображена в таблиці додатка А.3

Однією з ключових складових захищеного інформаційного середовища є контроль над інформаційними системами, що функціонують у мережі підприємства. Для цього створюється реєстр основних сервісів, що дозволяє не лише бачити архітектуру цифрових процесів, але й виявляти критичні точки, які потребують підвищеного рівня захисту.

Зведення такого реєстру є основою для оцінки ступеня захищеності кожної системи, їх резервування, моніторингу активності та встановлення пріоритетів у реалізації заходів безпеки. Найбільш критичними для безперервної діяльності підприємства виявилися ERP, бухгалтерська система та поштовий сервер, оскільки саме вони обробляють фінансову, конфіденційну та комунікаційну інформацію [30].

Для систем із високим рівнем критичності рекомендовано забезпечити окремі політики доступу, сегментацію на рівні VLAN та регулярне резервне копіювання з ізольованим зберіганням копій.

Для ефективного управління інформаційною безпекою необхідно здійснювати класифікацію інформаційних активів за рівнем критичності та доступності. Такий поділ дозволяє визначити, які ресурси потребують пріоритетного захисту, а також хто має до них доступ.

Класифікація активів дозволяє впровадити диференційований підхід до безпеки: наприклад, активи з високою критичністю та обмеженим доступом потребують посиленого моніторингу, шифрування та багатофакторної аутентифікації. Публічні ресурси, навпаки, мають бути ізольовані від внутрішніх систем і контролюватися через DMZ-сегмент або окрему VLAN [31].

Така деталізація також сприяє підготовці до впровадження ISO/IEC 27001, де розмежування доступу й класифікація активів є обов’язковими елементами системи управління інформаційною безпекою.

Для візуального представлення взаємозв’язків між основними компонентами мережі підприємства створено схему, яка демонструє маршрути

даних між користувачами, робочими станціями, серверами та зовнішніми інтерфейсами. Вона дозволяє чітко простежити логіку переміщення інформації та виявити потенційні точки вразливості на рівні доступу або сегментації трафіку.

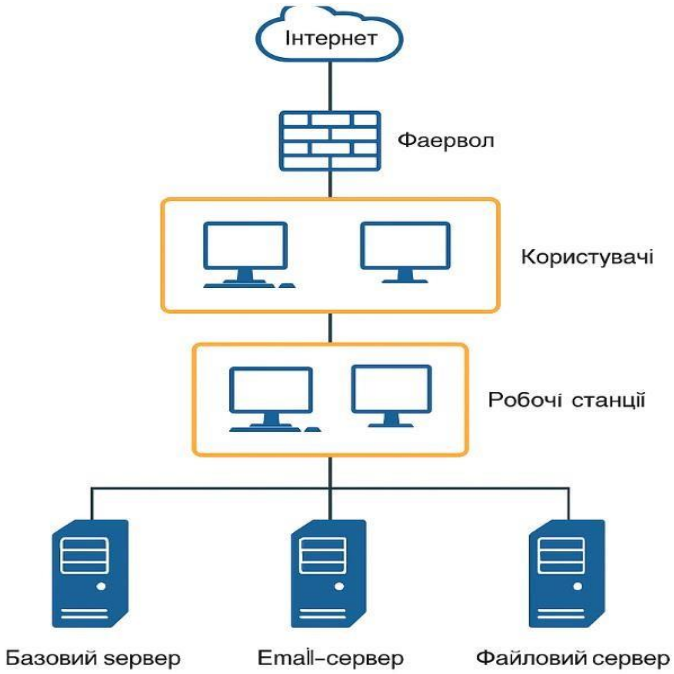

Рисунок 2.3 – Схема зв’язку між серверами, робочими станціями та зовнішніми інтерфейсами

На рис.2.3 в схемі показано, що вхідний трафік з інтернету спочатку проходить через фаєрвол, де здійснюється фільтрація. Далі дані передаються до робочих станцій користувачів, які підключені до внутрішньої мережі. Звідти забезпечується доступ до ключових серверів: баз даних, електронної пошти та файлів. Така архітектура дозволяє централізовано керувати інформаційними потоками, ізолювати критичні ресурси та здійснювати моніторинг на кожному етапі взаємодії [32].

2.2 Оцінка актуальних ризиків та вразливостей у системі захисту

Для забезпечення цілісної системи інформаційної безпеки критично важливо своєчасно ідентифікувати технічні вразливості в мережевій інфраструктурі. Нижче наведено результати аудиту, проведеного з метою виявлення таких зон ризику. Аналіз охоплює як обладнання, так і комунікаційні канали між підрозділами підприємства.

Таблиця 2.2 – Виявлені технічні вразливості в мережевому середовищі

№	Компонент	Тип вразливості	Деталі	Потенційна загроза
1	Сервер бухгалтерії	Застаріле ПЗ	Windows Server 2012 без оновлень	Експлойти, віддалене виконання коду
2	Wi-Fi точка доступу	Відсутність WPA2 Enterprise	Відкрите з’єднання, спільний пароль	Несанкціонований доступ
3	Комутатор TP-Link	Відсутність авторизації	Web-інтерфейс без пароля	Захоплення керування
4	Вебсервер	Незахищений порт 8080	Відкритий порт не фільтрується	Обхід основного фаєрволу
5	Email-сервер	Ввімкнена служба POP3	Старий протокол без шифрування	Перехоплення облікових даних

З табл. 2.2 можна зробити висновок,що наведені в ній дані свідчать про наявність системних технічних вразливостей, які значно підвищують ризик компрометації мережевої інфраструктури.

Особливу увагу слід приділити серверам із застарілим ПЗ, відкритим портам, які не фільтруються, та слабко захищеним Wi-Fi-точкам. Більшість із цих проблем пов’язані не з відсутністю засобів захисту, а з недостатнім супроводом, налаштуванням та оновленням. Це потребує негайного реагування через

впровадження патч-менеджменту, сегментації мережі та посилення політик доступу до обладнання [33].

Таблиця 2.3 – Аналіз безпеки обміну даними між підрозділами

№	Підрозділи	Тип з’єднання	Захист (шифрування/автентифікація)	Виявлені ризики
1	Бухгалтерія ↔ Архів	FTP (порт 21)	Відсутнє	Витік файлів через прослуховування
2	Продажі ↔ Керівництво	Email	TLS/STARTTLS частково	Можливість MITMатаки
3	Бухгалтерія ↔ ERP-сервер	HTTP	Без шифрування	Перехоплення даних клієнтів
4	Всі відділи ↔ Склад	VPN (PPTP)	Слабке шифрування	Вразливість до дешифрування трафіку

Результати проведеного аудиту інформаційної безпеки виявили критичні недоліки в архітектурі мережевої інфраструктури організації, які створюють серйозні загрози для конфіденційності, цілісності та доступності корпоративної інформації, оскільки в процесі передавання даних між різними структурними підрозділами активно використовуються морально застарілі та небезпечні протоколи зв'язку, які не відповідають сучасним вимогам кібербезпеки та міжнародним стандартам захисту інформації. Аналіз безпеки обміну даними між підрозділами показано в табл 2.3.

Серед виявлених проблемних технологій особливу тривогу викликає широке застосування протоколу FTP без будь-якого шифрування для передачі файлів між відділами, що означає передачу всієї інформації, включаючи облікові дані користувачів та конфіденційні документи, у відкритому вигляді через корпоративну мережу та потенційно через незахищені канали зв'язку з можливістю перехоплення будь-яким зловмисником, який має доступ до мережевого трафіку.

Використання протоколу HTTP замість захищеного HTTPS у критично важливих системах обліку та управління корпоративними ресурсами створює неприйнятний рівень ризику для фінансової та операційної інформації організації, оскільки всі дані, включаючи паролі користувачів, фінансові звіти, персональні дані співробітників та клієнтів, передаються через мережу без будь-якого криптографічного захисту, що робить їх легкою мішенню для кіберзлочинців.

Виявлені слабко захищені VPN-з'єднання на базі застарілого протоколу PPTP (Point-to-Point Tunneling Protocol) представляють особливо серйозну загрозу для безпеки віддаленого доступу співробітників до корпоративних ресурсів, оскільки цей протокол містить відомі криптографічні вразливості, які дозволяють зловмисникам відносно легко зламати шифрування та отримати доступ до корпоративної мережі, маскуючись під легітимних користувачів.

Усі ці небезпечні канали зв'язку створюють множинні вектори атак для кіберзлочинців, включаючи можливості для пасивного прослуховування мережевого трафіку з метою збору конфіденційної інформації, реалізації активних атак типу «людина посередині» (Man-in-the-Middle, MITM), коли зловмисник може перехоплювати, модифікувати та перенаправляти комунікації між легітимними учасниками обміну даними, проведення атак з підміни пакетів для впровадження шкідливого контенту або маніпулювання даними в режимі реального часу, а також здійснення різноманітних форм несанкціонованого втручання в бізнес-процеси організації з потенційно катастрофічними наслідками для операційної діяльності та репутації компанії.

Технічна реалізація атак на незахищені протоколи може включати використання широкодоступних інструментів перехоплення мережевого трафіку, таких як Wireshark, tcpdump або спеціалізовані хакерські утиліти, які дозволяють зловмисникам з мінімальними технічними навичками отримувати доступ до

критично важливої корпоративної інформації без необхідності подолання складних захисних механізмів.

Атаки типу MITM можуть бути реалізовані через компрометацію мережевого обладнання, ARP-spoofing, DNS-hacking або створення підроблених точок доступу Wi-Fi, що дозволяє зловмисникам не лише перехоплювати інформацію, але й активно маніпулювати нею, впроваджувати шкідливий код, крадіжки облікових даних або проводити фінансові махінації від імені організації.

Ризики підміни пакетів включають можливість впровадження шкідливого програмного забезпечення в легітимний трафік, модифікації фінансових транзакцій, фальсифікації звітності або порушення цілісності критично важливих баз даних, що може призводити до серйозних фінансових втрат, регуляторних санкцій та довгострокового пошкодження репутації організації.

Для усунення виявлених критичних вразливостей необхідно здійснити комплексну модернізацію мережевої інфраструктури з обов'язковим переходом до використання сучасних криптографічно захищених протоколів передачі даних, що включає заміну небезпечного FTP на SFTP (SSH File Transfer Protocol) або FTPS (FTP over SSL/TLS), які забезпечують надійне шифрування всіх передаваних файлів та облікових даних користувачів, впровадження протоколу HTTPS з використанням сучасних TLS-сертифікатів для всіх веб-додатків та систем обліку, що гарантує захист від перехоплення та модифікації даних під час їх передачі через мережу, а також заміну застарілих PPTP VPN-з'єднань на сучасні та безпечні рішення на базі протоколів IPsec, OpenVPN або WireGuard, які забезпечують військовий рівень шифрування та надійну автентифікацію користувачів.

Додатково необхідно впровадити систему централізованого контролю та моніторингу за всіма маршрутами обміну інформацією між структурними підрозділами, що включає створення детальної карти інформаційних потоків, впровадження політик сегментації мережі для обмеження латерального руху

потенційних зловмисників, налаштування систем виявлення вторгнень для моніторингу аномальної мережевої активності, а також розробку та впровадження комплексних політик безпеки, які регламентують використання мережевих протоколів, процедури автентифікації та авторизації користувачів.

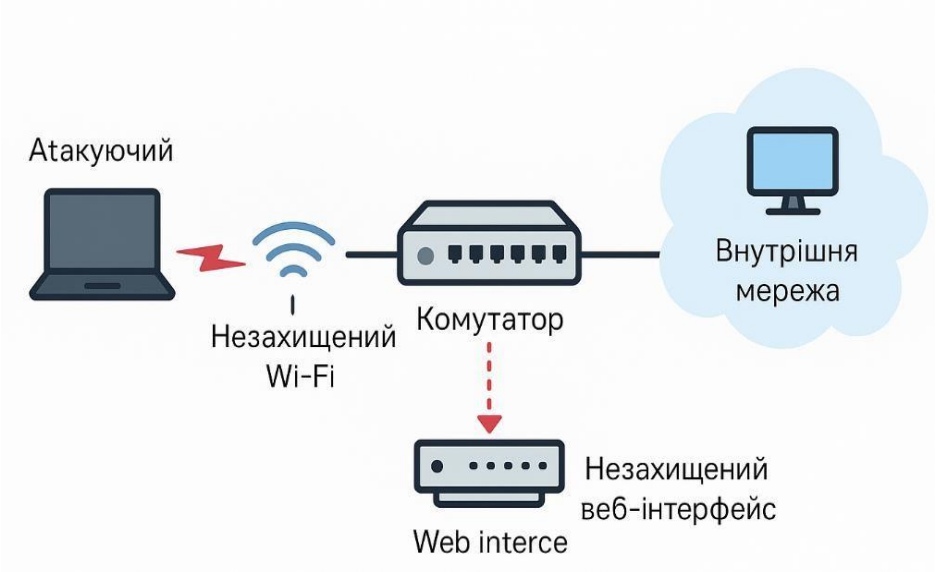

Рисунок 2.4 – Схема потенційного вектору атаки

На схемі візуалізується приклад ймовірної атаки через вразливі елементи мережі. Вхідна точка – Wi-Fi точка доступу з відкритим паролем, далі – експлуатація незахищеного вебінтерфейсу комутатора для отримання прав доступу до внутрішньої мережі. Схема потенційного вектору атаки відображено на рис. 2.4.

Таблиця 2.4 – Матриця оцінки ризиків ІБ на підприємстві

№	Вразливість	Потенційна загроза	Імовірність (1–5)	Вплив (1–5)	Рівень ризику (I×B)	Коментар
1	Відкритий порт 8080	Обхід фаєрволу	4	5	20	Потрібне негайне блокування
2	Wi-Fi без WPA2 Enterprise	Несанкціонований доступ до мережі	5	4	20	Рекомендована сегментація та шифрування
3	POP3 без шифрування	Перехоплення облікових даних	3	4	12	Слід перевести на IMAPS
4	FTPз'єднання між підрозділами	Витік фінансової інформації	3	5	15	Потрібна заміна на SFTP
5	Застаріле ПЗ (ERP)	Експлойти та несанкціонований доступ	4	5	20	Прямий ризик для критичної системи

Результати ідентифікації вказують на наявність критичних вразливостей, що можуть бути використані зловмисниками для несанкціонованого доступу до даних. Особливе занепокоєння викликає використання нешифрованих каналів обміну та застарілого програмного забезпечення. Матриця оцінки ризиків ІБ на підприємстві показано в табл. 2.4. Необхідно вжити заходів з оновлення компонентів, переходу на шифровані протоколи та обмеження відкритих портів [34].

Загальний аналіз показує, що підприємство має щонайменше три зони з критичним ризиком, що потребують негайних дій. Вони пов'язані з доступністю ззовні, відсутністю шифрування та експлуатацією застарілих платформ.

Рейтинговий аналіз дає змогу оптимізувати витрати ресурсів, починаючи з найкритичніших проблем. Першочерговими є дії, пов'язані з зовнішніми входами та системами, що мають високу цінність або доступність з інтернету.

Таблиця 2.5 – Рейтинговий аналіз ризиків за пріоритетністю реагування

№	Пріоритет	Ризик	Рівень ризику	Категорія впливу	Рекомендоване рішення
1	1	Відкритий порт 8080	20	Критичний	Блокування на фаєрволі
2	1	ERP на застарілій ОС	20	Критичний	Оновлення або ізоляція
3	1	Wi-Fi без захисту	20	Критичний	Перехід на WPA2 Enterprise
4	2	FTP між відділами	15	Високий	Міграція на SFTP
5	3	POP3 без шифрування	12	Середній	Вимкнення POP3, переведення на IMAPS

Рисунок 2.5 демонструє «теплову карту» ризиків, що дозволяє візуально оцінити їх критичність за двома параметрами: ймовірністю виникнення (по вертикалі) та впливом на підприємство (по горизонталі). Кожен ризик позиціонується у відповідній клітинці, а кольорова шкала – від зеленого до червоного – сигналізує про рівень загрози. Рейтинговий аналіз ризиків за пріоритетністю реагування показано в табл.2.5.

Як видно з діаграми, найнебезпечнішими є «ERP на застарілій ОС», «WiFi без захисту» та «Відкритий порт 8080», що потрапляють до червоного (критичного) сектору. POP3 без шифрування має нижчу ймовірність, але високий вплив, тому класифікується як середній ризик. Жовта зона включає ризики, що вимагають уваги, але не є терміновими – як-от «FTP між відділами» [35].

Цей підхід дозволяє чітко визначити пріоритети реагування та оптимізувати план дій із мінімізації вразливостей в інформаційній системі. Теплова карта може бути інтегрована в систему управління ІБ (наприклад, згідно ISO/IEC 27005) як візуальний інструмент для щоквартального перегляду загроз.

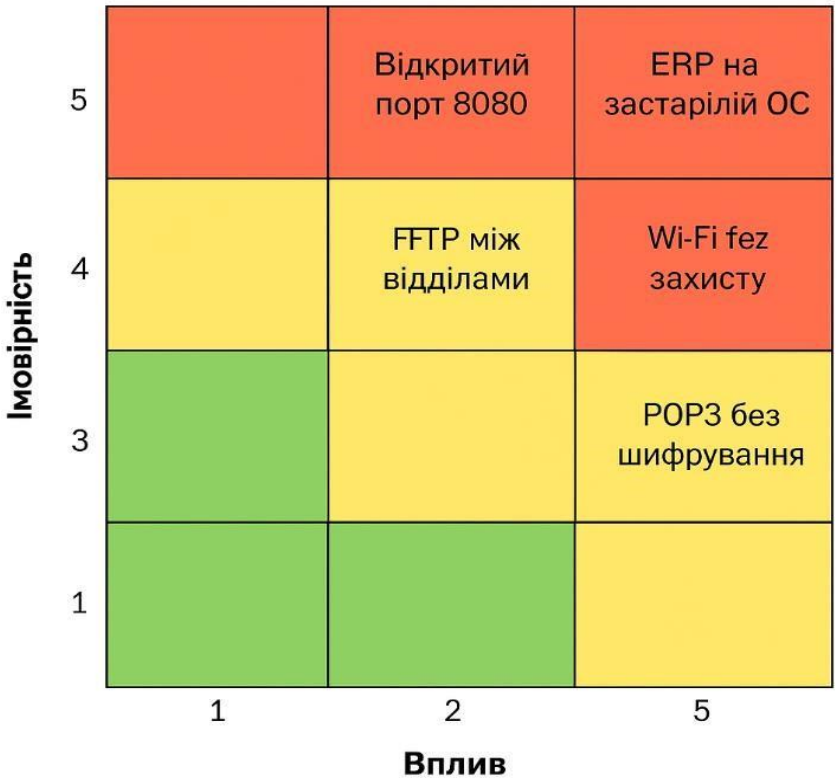

Рисунок 2.5 – Діаграма «Heat Map» ризиків за критичністю

Отже, результати аналізу вразливостей та оцінки ризиків вказують на наявність критичних зон у мережевій інфраструктурі підприємства. Зокрема, виявлено використання незашифрованих протоколів, відкриті порти та застаріле програмне забезпечення, які можуть бути легко експлуатовані. Побудована матриця ризиків і діаграма «Heat Map» дозволили визначити пріоритети реагування та сформувати основу для подальшої оптимізації системи захисту. Реалізація відповідних заходів дозволить суттєво зменшити ймовірність інцидентів інформаційної безпеки.

2.3 Виявлення недоліків у політиці безпеки, міжмережевих екранах, антивірусному захисті, контролі доступу

Ефективне управління інформаційною безпекою в будь-якій організації неможливе без впровадження та підтримання чіткої, всеохоплюючої та постійно актуалізованої системи контролю доступу користувачів до інформаційних систем, оскільки саме через недоліки в управлінні правами доступу відбувається значна частина інцидентів кібербезпеки, включаючи несанкціоновані витоки даних, внутрішні зловживання, компрометацію облікових записів та порушення принципів конфіденційності корпоративної інформації.

Система контролю доступу функціонує як фундаментальний захисний бар'єр, який відокремлює авторизованих користувачів від несанкціонованих, забезпечує дотримання принципу найменших привілеїв та гарантує, що кожен співробітник має доступ лише до тієї інформації та тих функціональних можливостей, які є абсолютно необхідними для виконання його професійних обов'язків, що мінімізує потенційну зону ураження у випадку компрометації окремих облікових записів або внутрішніх загроз з боку недоброчесних співробітників.

Політики доступу представляють собою детально структуровані документи та технічні конфігурації, які визначають фундаментальні принципи та конкретні механізми управління правами користувачів, встановлюючи чіткі критерії того, хто саме з персоналу організації має право отримати доступ до конкретних інформаційних ресурсів, до яких саме систем, баз даних, файлів, додатків та функціональних модулів цей доступ може бути наданий, з якими конкретними правами та обмеженнями (читання, запис, модифікація, видалення, адміністрування) користувач може оперувати з доступною йому інформацією, в які часові проміжки та з яких мережевих локацій такий доступ є дозволеним, а

також за яких умов права доступу можуть бути розширені, обмежені або повністю відкликані.

Дані політики охоплюють всю корпоративну мережу та всі категорії інформаційних активів, від загальнодоступних корпоративних ресурсів до висококонфіденційних комерційних таємниць, персональних даних клієнтів та критично важливих операційних систем, створюючи багаторівневу систему захисту, яка адаптується до специфічних потреб різних департаментів, проектів та бізнес-процесів організації.

Практичний аналіз поточної ситуації щодо управління обліковими записами в типовій корпоративній середі часто виявляє системні недоліки, які створюють серйозні ризики для інформаційної безпеки та операційної ефективності організації. Серед найпоширеніших проблем слід відзначити наявність численних «сирітських» облікових записів колишніх співробітників, які не були своєчасно деактивовані після звільнення персоналу, що створює потенційні точки входу для несанкціонованого доступу та ускладнює процеси аудиту безпеки.

Аналіз часто виявляє проблему накопичення надлишкових привілеїв, коли користувачі зберігають права доступу до систем та інформації, які більше не є необхідними для їх поточних функціональних обов'язків внаслідок зміни посад, переведення в інші департаменти або еволюції їхніх професійних ролей, що порушує принцип найменших привілеїв та збільшує потенційну зону ураження при компрометації облікових записів.

Система управління ролями та правами доступу в сучасних організаціях базується на концепції рольового контролю доступу (Role-Based Access Control, RBAC), яка передбачає створення стандартизованих ролей, що відповідають типовим посадовим функціям та відповідальності співробітників, з подальшим призначенням цих ролей конкретним користувачам відповідно до їхніх професійних потреб.

Ефективна реалізація RBAC включає створення ієрархічної структури ролей від базових користувачів з мінімальними правами до системних адміністраторів з розширеними привілеями, впровадження механізмів наслідування прав між рівнями ієрархії, забезпечення можливості тимчасового підвищення привілеїв для виконання специфічних завдань, а також створення спеціалізованих ролей для різних категорій зовнішніх користувачів, включаючи підрядників, консультантів, аудиторів та партнерів організації.

Кожна роль має бути чітко документована з детальним описом наданих прав, обґрунтуванням необхідності цих прав для виконання професійних функцій, вказівкою відповідальних осіб за призначення та відкликання ролі, а також регулярністю перегляду та актуалізації прав доступу.

Управління доступом до ключових інформаційних активів вимагає особливо ретельного підходу та впровадження додаткових рівнів захисту, оскільки компрометація критично важливих систем може призвести до катастрофічних наслідків для всієї організації.

Ключові інформаційні активи включають системи управління базами даних з конфіденційною корпоративною та клієнтською інформацією, фінансові системи та системи обліку, інтелектуальну власність компанії, системи управління персоналом з особистими даними співробітників, виробничі системи управління та промислові системи контролю, а також системи зовнішніх комунікацій та електронної пошти.

Як видно з таблиці 2.6, облікові записи не завжди відповідають принципу мінімального необхідного доступу. Деякі користувачі мають надмірні повноваження, а частина облікових записів використовує лише пароль без додаткових факторів захисту. Це створює передумови для зловживань або компрометації системи у разі витоку облікових даних.

Доступ до цих критичних ресурсів має регулюватися принципами подвійної автентифікації, логування всіх операцій доступу, обов'язкового схвалення

доступу керівництвом, регулярного перегляду прав доступу, а також впровадження технічних засобів моніторингу аномальної активності та автоматичного блокування підозрілих дій.

Таблиця 2.6 – Перелік активних користувачів, їх ролі та права доступу до систем

№	Користувач	Посада	Доступ до систем	Рівень доступу	Тип автентифікації
1	kovalenko.i	Головний бухгалтер	1С, ERP, пошта	Повний	Пароль
2	drozd.o	Менеджер з продажу	CRM, Email	Обмежений	Пароль
3	sysadmin	Адміністратор системи	Всі системи, сервери	Повний (root)	2FA
4	teteruk.v	Директор	ERP, пошта, фінанси	Повний	Пароль
5	intern23	Стажер	CRM-тест	Низький	Тимчасовий пароль

Практичний аналіз ефективності системи контролю доступу включає проведення регулярних аудитів прав користувачів, тестування процедур надання та відкликання доступу, аналіз логів доступу для виявлення аномальних патернів використання, оцінку відповідності поточних прав доступу актуальним функціональним потребам користувачів, а також перевірку дотримання встановлених політик безпеки всіма категоріями користувачів корпоративної мережі [36].

Таблиця 2.7 – Виявлені порушення політики доступу

№	Тип порушення	Приклад	Ризик	Рекомендація
1	Відсутність двофакторної автентифікації	Користувачі з повним доступом	Перехоплення облікових даних	Упровадження 2FA
2	Надмірні повноваження	Менеджер має доступ до бухгалтерії	Несанкціоновані дії	Обмежити доступ лише до CRM
3	Неактивні облікові записи	intern23 залишився активним	Потенційний злом	Видалити або призупинити
4	Відсутність журналювання входу	Відсутній аудит логінів до ERP	Втрата сліду активності	Активувати логування
5	Загальні паролі між користувачами	CRM доступ через один акаунт	Відсутність ідентифікації	Розподілити індивідуальні обліковки

Недотримання базових політик доступу в корпоративному середовищі створює каскадний ефект безпекових ризиків, який істотно збільшує ймовірність виникнення внутрішніх інцидентів інформаційної безпеки та може призвести до серйозних наслідків для операційної діяльності та репутації організації, оскільки відсутність чіткого контролю над правами користувачів і системами моніторингу їхньої активності створює сприятливе середовище для зловживань як з боку недоброчесних співробітників, так і для успішної реалізації зовнішніх атак через компрометовані облікові записи Виявлені порушення політики доступу показано в табл.2.7.

Серед найбільш поширених і небезпечних наслідків слабкого управління доступом слід виділити проблему несвоєчасного виявлення несанкціонованих дій користувачів, яка виникає внаслідок відсутності ефективних механізмів моніторингу та аудиту активності в реальному часі, що дозволяє зловмисникам тривалий час залишатися непоміченими в корпоративній мережі, поступово розширювати свої привілеї, збирати конфіденційну інформацію та готувати масштабні атаки на критично важливі системи. Втрата або пошкодження логів

системної активності представляє особливо серйозну загрозу, оскільки позбавляє організацію можливості проведення ефективного розслідування інцидентів, відновлення хронології подій, ідентифікації масштабів компрометації та вжиття адекватних заходів реагування, що може призвести до повторних атак через ті ж самі невиправлені вразливості.

Помилкове або зловмисне використання службових привілеїв становить окрему категорію ризиків, яка особливо загострюється в умовах недостатнього контролю за правами підвищеного доступу, коли співробітники з адміністративними або спеціальними привілеями можуть використовувати свої права для несанкціонованого доступу до конфіденційної інформації, модифікації критично важливих даних, обходу встановлених процедур безпеки або створення додаткових точок доступу для подальшого використання.

Ці проблеми набувають особливо критичного значення в контексті ERP-систем (Enterprise Resource Planning) та корпоративних баз даних, де зосереджена найбільш цінна та чутлива інформація організації, включаючи фінансові дані, комерційні таємниці, персональну інформацію співробітників і клієнтів, стратегічні плани розвитку, договірні відносини з партнерами та іншу критично важливу корпоративну інформацію.

ERP-системи, які інтегрують всі основні бізнес-процеси організації від фінансового обліку до управління персоналом і ланцюгами постачання, представляють особливо привабливу мішень для внутрішніх і зовнішніх зловмисників, оскільки успішна компрометація таких систем може надати доступ до практично всієї операційної інформації компанії.

Фінансова інформація, що обробляється в ERP-системах, включає банківські реквізити, дані про доходи та витрати, інформацію про інвестиції та борги, планові та фактичні показники діяльності, податкову звітність та іншу фінансово чутливу інформацію, несанкціонований доступ до якої може призвести не лише до прямих фінансових втрат через шахрайство або маніпуляції, але й до

серйозних регуляторних санкцій, судових позовів з боку акціонерів та інвесторів, а також довгострокової втрати довіри з боку фінансових партнерів і кредиторів.

Персональна інформація, що зберігається в корпоративних базах даних, охоплює широкий спектр чутливих даних про співробітників, клієнтів і партнерів, включаючи особисті ідентифікаційні дані, контактну інформацію, фінансові реквізити, медичну інформацію, дані про сімейний стан і соціальні зв'язки, професійну історію та оцінки ефективності, що робить ці системи особливо привабливими для кіберзлочинців, які спеціалізуються на крадіжці персональних даних для подальшого використання в схемах шахрайства, ідентитету та фінансових махінаціях.

Надійна робота міжмережевого екрану або фаєрволу представляє собою один з найбільш фундаментальних та критично важливих компонентів архітектури мережевої безпеки сучасної організації, функціонуючи як першочерговий бар'єр захисту між внутрішньою корпоративною мережею та потенційно ворожим зовнішнім інтернет-середовищем, а також забезпечуючи сегментацію та контроль трафіку між різними внутрішніми мережевими сегментами відповідно до встановлених політик безпеки та бізнес-вимог організації.

Ефективність фаєрволу залежить не лише від технічних характеристик обладнання та програмного забезпечення, але й від правильності конфігурації правил фільтрації, регулярності їх оновлення відповідно до змін в IT-інфраструктурі та актуальних загроз, а також від якості моніторингу та аналізу його роботи для своєчасного виявлення спроб обходу або атак на саму систему захисту.

Комплексний аудит міжмережевого екрану включає детальний аналіз всіх активних правил фільтрації трафіку з оцінкою їх актуальності, необхідності та відповідності поточним бізнес-потребам і політикам безпеки організації, що передбачає перевірку кожного правила на предмет його обґрунтованості,

виявлення застарілих або надлишкових правил, які можуть створювати непотрібні ризики або ускладнювати управління системою, а також ідентифікацію відсутніх правил, які необхідні для адекватного захисту нових сервісів або змінених бізнес-процесів. Аналіз напрямків взаємодії охоплює картографування всіх дозволених і заблокованих комунікаційних шляхів між різними мережевими сегментами. Активні правила файрволу підприємства наведені в табл.2.8.

Таблиця 2.8 – Активні правила файрволу підприємства

№	Правило №	Порт / Служба	IP-діапазон	Напрямок	Статус	Коментар
1	Rule-01	80 (HTTP)	0.0.0.0/0 → 192.168.0.10	Вхідний	Дозволено	Доступ до вебсайту
2	Rule-02	443 (HTTPS)	0.0.0.0/0 → 192.168.0.10	Вхідний	Дозволено	Захищений трафік
3	Rule-03	21 (FTP)	192.168.1.20 → 192.168.1.30	Вихідний	Дозволено	Обмін файлами між відділами
4	Rule-04	3389 (RDP)	0.0.0.0/0 → 192.168.0.50	Вхідний	Заборонено	Віддалений доступ заборонено
5	Rule-05	8080	0.0.0.0/0 → 192.168.1.15	Вхідний	Дозволено	Вразливий нестандартний порт

Детальний аналіз діапазонів IP-адрес включає перевірку всіх налаштованих мережевих об'єктів, груп адрес та діапазонів на предмет їх актуальності та точності, виявлення перекриттів або конфліктів між різними адресними просторами, оцінку відповідності налаштованих адрес реальній топології мережі, а також ідентифікацію надто широких діапазонів, які можуть створювати непотрібні ризики через надання доступу большему колу адрес, ніж це необхідно для бізнес-функцій. Виявлені слабкі налаштування файрволу показано в табл.2.9.

Таблиця 2.9 – Виявлені слабкі налаштування файрволу

№	Виявлений недолік	Потенційний ризик	Рекомендація
1	Дозвіл HTTP без примусу HTTPS	Витік конфіденційних даних	Примусове перенаправлення на HTTPS
2	Відкритий порт 8080	Обхід основного фільтра	Блокування або обмеження доступу
3	Універсальні правила (0.0.0.0)	Несанкціонований зовнішній доступ	Заміна на вузькі діапазони
4	Відсутність журналювання	Втрата слідів атак	Увімкнення логування для критичних правил
5	Дублювання правил	Непередбачувана поведінка системи	Оптимізація та перевірка конфігурацій

Особлива увага приділяється виявленню конфігураційних вразливостей, які можуть бути використані зловмисниками для обходу системи захисту, включаючи наявність правил «дозволити все» або занадто загальних правил, неправильну послідовність правил, яка може призводити до непередбачуваної поведінки фаєрволу.

Відсутність правил логування для критично важливих подій, слабкі або відсутні механізми автентифікації для віддаленого управління, використання стандартних паролів або сертифікатів, а також недостатня захищеність інтерфейсів управління може дозволити зловмисникам отримати контроль над самою системою захисту та використати її для приховування своєї злочинної діяльності або створення постійних каналів доступу до корпоративної мережі.

Наведені правила вказують на часткову відкритість до зовнішнього середовища, що є потенційно небезпечним, особливо у випадку нестандартних портів або використання застарілих служб. Присутність дозволеного трафіку по порту 8080 потребує особливої уваги, як і відкритий доступ до FTP-серверів.

Загалом аудит виявив ряд недоліків у конфігурації файрволу, які можуть бути експлуатовані як зсередини, так і ззовні. Особливо небезпечним є необмежений доступ до портів, використання широких діапазонів IP і відсутність

журналювання подій. Необхідне термінове оновлення політик безпеки для зменшення потенційного ризику інцидентів.

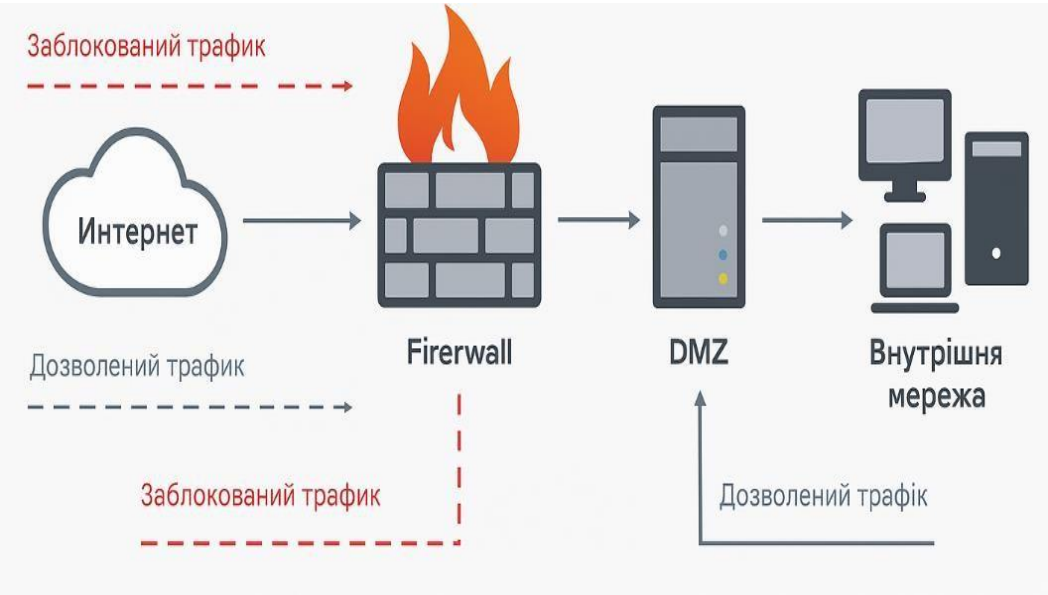

Рисунок 2.6 – Схема роботи міжмережевого екрану в поточному середовищі

Рисунок 2.6 ілюструє логіку роботи міжмережевого екрану у середовищі підприємства. Зовнішній трафік з інтернету спочатку обробляється фаєрволом, який виконує функції фільтрації: частина запитів дозволяється (наприклад, HTTPS до вебсервера в DMZ), інша блокується (наприклад, доступ до внутрішньої мережі напряму).

Фаєрвол також контролює вихідний трафік з внутрішньої мережі, дозволяючи тільки певні типи з’єднань, заздалегідь визначені в правилах. Важливим є те, що зв’язок між DMZ та внутрішньою мережею суворо обмежений: лише окремі сервіси можуть передавати дані з публічної зони до захищеної. Така схема забезпечує мінімізацію ризику при спробі зловмисника проникнути у внутрішню інфраструктуру через доступні ззовні сервіси.

Таблиця 2.10 – Активні правила файрволу підприємства

№	Порт / Служба	IP-діапазон	Напрямок	Дія	Коментар
1	80 (HTTP)	0.0.0.0/0 → 192.168.0.10	Вхідний	Дозволено	Доступ до вебсервера у DMZ
2	443 (HTTPS)	0.0.0.0/0 → 192.168.0.10	Вхідний	Дозволено	Захищений доступ до сайту
3	21 (FTP)	192.168.1.20 → 192.168.1.30	Вихідний	Дозволено	Обмін файлами між бухгалтерією і архівом
4	3389 (RDP)	0.0.0.0/0 → 192.168.0.50	Вхідний	Заборонено	Віддалений доступ вимкнено
5	8080	0.0.0.0/0 → 192.168.1.15	Вхідний	Дозволено	Тестовий доступ, не фільтрується

У процесі комплексної перевірки системи інформаційної безпеки підприємства було здійснено аудит налаштувань міжмережевого екрану, який відповідає за фільтрацію трафіку між зовнішніми та внутрішніми мережами.

Аналіз охоплював активні правила, конфігураційні слабкості, а також взаємозв’язки між зонами безпеки. Активні правила файрволу підприємства представленів табл.2.10.

Аналіз активних правил виявив низку потенційно небезпечних конфігурацій, зокрема дозвіл HTTP без обов’язкового перенаправлення на HTTPS та відкритий нестандартний порт 8080, що не захищений додатковими перевірками. Частина дозволеного трафіку надходить із будь-якої зовнішньої IPадреси, що підвищує ризики віддаленого вторгнення. Виявлені слабкі налаштування файрволу приведені в табл. 2.11.

Таблиця 2.11 – Виявлені слабкі налаштування файрволу

№	Недолік	Ризик	Рекомендація
1	Дозвіл HTTP без шифрування	Перехоплення даних	Примусове перенаправлення на HTTPS
2	Відкритий порт 8080	Обхід основного фільтрування	Закрити порт або застосувати фільтрацію
3	Широкий IP-діапазон (0.0.0.0/0)	Несанкціонований доступ ззовні	Обмежити до конкретних IP- або GEO-зон
4	Відсутність журналювання	Неможливість виявити інциденти	Активувати логування критичних подій
5	Повторювані правила	Непередбачувана робота фільтрації	Провести ревізію та оптимізувати записи

Аудит конфігурації показав, що хоча базова фільтрація трафіку реалізована, існує низка прорахунків, які ускладнюють відстеження потенційних атак і можуть бути використані для обходу системи. Необхідно запровадити принцип мінімального доступу, а також централізоване логування критичних транзакцій [37].

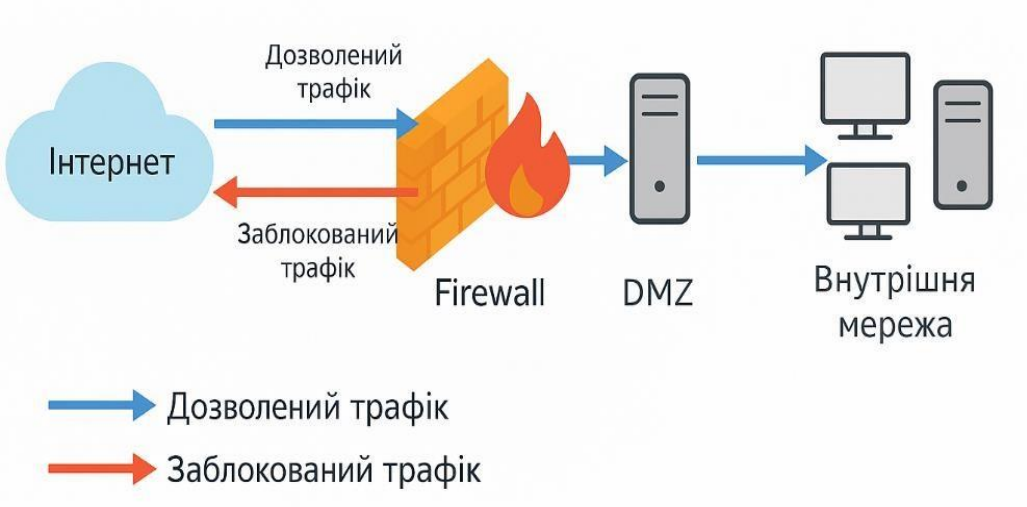

Рисунок 2.7 – Схема роботи міжмережевого екрану в поточному середовищі

Схема наочно демонструє, як міжмережевий екран виконує фільтрацію між чотирма ключовими зонами: Інтернетом, фаєрволом, демілітаризованою зоною (DMZ) та внутрішньою мережею. Дозволений трафік (синій) спрямовується

виключно до визначених серверів у DMZ або всередину мережі за заздалегідь визначеними правилами. Усі інші запити – особливо ті, що не відповідають політикам – блокуються (червоний трафік). Така побудова дозволяє контролювати кожен вектор трафіку, знижуючи ймовірність несанкціонованого доступу або атаки на внутрішні ресурси [38].

Отже, результати аудиту політик доступу, налаштувань файрволу та роботи антивірусного захисту виявили низку критичних недоліків, які можуть бути використані зловмисниками для проникнення або ескалації привілеїв у мережі. Виявлені надмірні повноваження користувачів, відсутність двофакторної автентифікації, відкриті порти та недостатній контроль логів потребують невідкладного усунення. Упровадження оновлених політик безпеки, оптимізація правил міжмережевого екрану та посилення контролю за доступом дозволять суттєво підвищити рівень захищеності IT-інфраструктури підприємства.

РОЗДІЛ 3 ШЛЯХИ ОПТИМІЗАЦІЇ ТА ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

3.1 Посилення аутентифікації та контролю доступу

В сучасному цифровому ландшафті, де периметр безпеки стає все більш розмитим через хмарні технології, віддалену роботу та мобільні пристрої, надійні механізми аутентифікації та контролю доступу перетворюються на фундаментальну основу будь-якої стратегії кібербезпеки. Аутентифікація, процес перевірки ідентичності користувача чи системи, та контроль доступу, механізм надання або обмеження прав на ресурси, є першою лінією оборони проти несанкціонованого проникнення.

Історично, захист базувався на простому поєднанні логіна та пароля, однак цей підхід вже давно продемонстрував свою вразливість перед сучасними загрозами, такими як атаки методом перебору (brute-force), фішинг, використання скомпрометованих облікових даних та соціальна інженерія. Тому для побудови стійкої та ефективної системи захисту комп'ютерної мережі необхідно впроваджувати комплексні та багаторівневі рішення, що значно ускладнюють завдання зловмисникам.

Ключовим напрямом посилення захисту є впровадження багатофакторної аутентифікації (Multi-Factor Authentication, MFA). Концепція MFA полягає у вимозі від користувача надати два або більше докази своєї ідентичності, що належать до різних категорій: «щось, що ви знаєте» (пароль, PIN-код), «щось, що у вас є» (апаратний токен, смартфон з додатком-аутентифікатором) та «щось, чим ви є» (біометричні дані, такі як відбиток пальця або сканування обличчя). Навіть якщо зловмисник викраде пароль користувача, без доступу до другого фактора (наприклад, фізичного пристрою) він не зможе отримати доступ до системи. Це створює потужний додатковий бар'єр для захисту критично важливих систем,

таких як сервери баз даних, адміністративні панелі управління, фінансові додатки та хмарні сервіси.

Впровадження багатофакторної аутентифікації (MFA) є критично важливим етапом у забезпеченні кібербезпеки. Процес реалізації потребує ретельного планування, оскільки необхідно враховувати як рівень безпеки, так і зручність для кінцевих користувачів. Надмірно складні механізми можуть демотивувати співробітників використовувати захищені методи доступу, тоді як занадто прості можуть залишати систему вразливою до атак.

Перед впровадженням MFA необхідно визначити, які методи будуть найбільш оптимальними для конкретної організації. Одним із найпоширеніших варіантів є використання SMS-кодів, які надсилаються на мобільний телефон користувача. Такий метод є простим у налаштуванні та не потребує встановлення додаткових програм, але має істотні недоліки. Одним із основних ризиків є можливість атак через підміну SIM-картки (SIM swap), що дозволяє зловмисникам отримати доступ до кодів аутентифікації.

Більш захищеним способом є застосування додатків-аутентифікаторів, які генерують одноразові паролі на основі часу (Time-based One-Time Password, TOTP). Такі програми, як Google Authenticator або Microsoft Authenticator, працюють незалежно від мобільної мережі, що робить їх значно стійкішими до атак перехоплення. Код змінюється кожні кілька секунд, і навіть якщо його буде викрадено, він швидко стане непридатним для використання.

Найнадійнішим рішенням для MFA є апаратні ключі безпеки, які підтримують стандарти FIDO2 та U2F. Ці пристрої використовують криптографічні методи для перевірки автентичності без передачі паролів, що робить їх практично невразливими до фішингових атак. Користувач просто підключає ключ до комп’ютера або використовує його бездротово, що забезпечує максимальний рівень захисту без необхідності введення кодів.

Таким чином, впровадження MFA вимагає балансування між безпекою та зручністю, а вибір методів залежить від конкретних загроз та технічних можливостей організації. Ефективна реалізація цього процесу значно знижує ризик несанкціонованого доступу та підвищує загальний рівень кібербезпеки.

Основні методи реалізації другого фактора аутентифікації:

- Одноразові паролі через SMS або електронну пошту: Код надсилається на зареєстрований номер телефону або email користувача.
- Додатки-аутентифікатори (TOTP): Програми для смартфонів (наприклад, Google Authenticator, Microsoft Authenticator), що генерують шестизначні коди, які змінюються кожні 30-60 секунд.
- Push-сповіщення: Запит на підтвердження входу надсилається на довірений пристрій (смартфон), де користувач може одним дотиком схвалити або відхилити спробу входу.
- Апаратні ключі безпеки (U2F/FIDO2): Фізичні пристрої (наприклад, YubiKey), що підключаються через USB або NFC і вимагають фізичної взаємодії (дотику) для підтвердження аутентифікації.
- Біометричні дані: Використання унікальних фізичних характеристик користувача, таких як відбиток пальця, сканування сітківки ока, розпізнавання обличчя або голосу.
- Геолокація та аналіз поведінки: Додаткові контекстуальні фактори, що аналізують типове місцезнаходження, IP-адресу, час входу та пристрій користувача для виявлення аномалій.

Після успішної аутентифікації наступним критичним етапом є контроль доступу. Тут домінуючою моделлю є управління доступом на основі ролей (Role-Based Access Control, RBAC). Замість того, щоб призначати права доступу кожному користувачеві індивідуально, RBAC дозволяє створювати ролі (наприклад, «Адміністратор», «Бухгалтер», «Розробник»), яким надаються певні набори дозволів. Користувачам потім призначаються ці ролі відповідно до їхніх

службових обов'язків. Цей підхід значно спрощує адміністрування прав, зменшує ризик людської помилки та полегшує аудит. Принцип мінімальних привілеїв (Principle of Least Privilege, PoLP) є ключовим аспектом моделі керування доступом на основі ролей (RBAC) і відіграє важливу роль у забезпеченні інформаційної безпеки організації. Його основна ідея полягає в тому, що кожен користувач, процес або система повинні мати лише той рівень доступу, який є строго необхідним для виконання своїх функцій. Це знижує ризик несанкціонованого використання ресурсів та мінімізує вплив потенційних загроз.

Одним із основних переваг PoLP є запобігання надлишковому доступу, який часто виникає у великих організаціях через необдумане або надмірно широке надання прав. Наприклад, співробітнику відділу кадрів немає необхідності отримувати доступ до конфігураційних файлів веб-сервера, так само як системному адміністратору не потрібен доступ до фінансових звітів. Невиправданий доступ до зайвих даних або налаштувань може спричинити як випадкові помилки, так і цілеспрямовані атаки.

Дотримання принципу мінімальних привілеїв також сприяє зменшенню ризику компрометації облікових записів. Якщо зловмиснику вдалося отримати контроль над аккаунтом одного із співробітників, шкода від цього буде обмежена лише тими ресурсами, до яких цей користувач мав доступ. Наприклад, якщо атакований обліковий запис має доступ лише до внутрішнього порталу для звітування, то зловмисник не зможе втрутитися у конфігурацію мережі чи базу клієнтів.

Для ефективного застосування PoLP необхідно регулярно переглядати рівні доступу, оцінювати актуальність ролей та впроваджувати автоматизовані механізми контролю. Це можуть бути системи періодичної ревізії прав доступу, налаштування двофакторної аутентифікації для критичних облікових записів та використання принципу Just-In-Time (JIT) для тимчасового надання привілеїв.

Таким чином, принцип мінімальних привілеїв є фундаментальним підходом до забезпечення безпеки інформаційних систем. Його правильне впровадження значно знижує загрози, пов'язані з неправомірним доступом, та сприяє більш структурованому та контрольованому управлінню правами у межах організації.Для наочності, порівняємо основні моделі контролю доступу в таблиці 3.1. Нарешті, для забезпечення довготривалої ефективності цих заходів необхідний систематичний аудит облікових записів та активності користувачів. Це безперервний процес, спрямований на виявлення та усунення потенційних ризиків.

Таблиця 3.1 – Порівняння моделей контролю доступу

№	Критерій	Дискреційна модель (DAC)	Мандатна модель (MAC)	Рольова модель (RBAC)
1	Принцип керування	Власник ресурсу визначає, хто має до нього доступ.	Система централізовано керує доступом на основі міток безпеки.	Доступ визначається роллю користувача в організації.
2	Гнучкість	Висока. Легко надавати та відкликати права.	Низька. Правила жорстко визначені системою.	Середня. Гнучка в межах визначених ролей.
3	Масштабованість	Низька. Складно керувати у великих системах.	Висока. Ефективна для систем з суворою ієрархією.	Висока. Ідеальна для корпоративних середовищ.
4	Приклад використання	Файлові системи (Windows, Linux).	Військові та урядові системи.	Корпоративні додатки, бази даних, хмарні платформи.
5	Основний недолік	Схильність до помилок користувачів, поширення прав.	Негнучкість, складність налаштування.	Потребує ретельного проектування ролей.

Аудит повинен включати регулярну перевірку активних облікових записів на предмет їх актуальності (видалення або блокування облікових записів звільнених співробітників), аналіз наданих прав доступу на відповідність принципу мінімальних привілеїв, а також моніторинг журналів подій (логів) для виявлення підозрілої активності. До такої активності можна віднести численні

невдалі спроби входу, спроби підвищення привілеїв, доступ до ресурсів у неробочий час або з нетипових геолокацій.

Впровадження цих трьох компонентів – багатофакторної аутентифікації, гранулярного контролю доступу та постійного аудиту – створює надійну, ешелоновану систему захисту, яка значно підвищує стійкість комп'ютерної мережі до сучасних кіберзагроз.

Рисунок 3.1 – Схема процесу багатофакторної аутентифікації

На рисунку 3.1 зображено типовий процес MFA. Користувач вводить свій пароль (перший фактор). Система перевіряє його і, якщо він правильний, надсилає запит на другий фактор, наприклад, push-сповіщення на смартфон. Користувач підтверджує вхід на своєму пристрої, після чого система надає йому доступ.

Рисунок 3.2 – Ілюстрація принципу мінімальних привілеїв в рамках RBAC

Рисунок 3.2 демонструє застосування RBAC та PoLP. Користувачі з різних відділів (Продажі, Фінанси, IT) мають різні ролі. Кожна роль надає доступ лише до тих ресурсів, які необхідні для виконання функцій відповідного відділу, блокуючи доступ до всіх інших, що мінімізує ризики.

3.2 Оптимізація міжмережевого екрану та захисту трафіку

Міжмережевий екран, або файрвол (firewall), є одним з наріжних каменів мережевої безпеки, що виконує функцію бар'єра між довіреною внутрішньою мережею та недовіреною зовнішньою, якою найчастіше є Інтернет. Його основне завдання – фільтрація мережевого трафіку на основі набору визначених правил, дозволяючи легітимний трафік і блокуючи шкідливий. Однак у сучасних умовах, коли атаки стають все більш витонченими, а мережева інфраструктура ускладнюється, стандартних налаштувань файрволу вже недостатньо. Для забезпечення надійного захисту необхідна його ретельна оптимізація, а також

впровадження додаткових заходів для захисту трафіку, таких як сегментація мережі та шифрування.

Першим кроком в оптимізації є ретельний аналіз та удосконалення поточних правил файрволу. З часом набори правил мають тенденцію «розростатися», накопичуючи застарілі, надто дозвільні або навіть конфліктні правила, що створює сліпі зони та потенційні вразливості. Аудит правил повинен починатися з переходу на політику «заборони за замовчуванням» (default deny). Цей підхід кардинально змінює логіку роботи файрволу: замість того, щоб дозволяти весь трафік, крім явно забороненого, він блокує абсолютно все, крім явно дозволеного. Це гарантує, що лише необхідний для бізнес-процесів трафік зможе проходити через периметр, що значно звужує поверхню атаки.

Під час проведення аудиту інформаційної безпеки одним із ключових аспектів є перевірка правил доступу та використання мережевих протоколів. Особливу увагу слід приділити виявленню незашифрованих протоколів, таких як HTTP, FTP, Telnet, оскільки їх використання значно підвищує ризик перехоплення критичних даних, включаючи облікові записи користувачів.

Незахищені протоколи передають дані у відкритому вигляді, без використання криптографічних механізмів, що робить їх вразливими до атак типу «людина посередині» (Man-in-the-Middle, MITM). У межах такої атаки зловмисник може перехопити інформацію, змінити її в реальному часі або просто отримати доступ до логінів та паролів без відома користувача. Особливо критичним це стає у випадках, коли системні адміністратори використовують Telnet для доступу до серверів або коли передача файлів здійснюється через FTP без шифрування.

Щоб мінімізувати ці ризики, всі незахищені протоколи повинні бути замінені на їхні безпечні аналоги, які використовують шифрування для захисту даних під час передавання. Зокрема, HTTP має бути замінений на HTTPS, що використовує SSL/TLS для забезпечення шифрування та автентифікації сторінок.

FTP слід замінити на SFTP (SSH File Transfer Protocol), який здійснює передачу файлів через зашифрований тунель. Telnet необхідно замінити на SSH (Secure Shell), що дозволяє адміністратору безпечно взаємодіяти із сервером, забезпечуючи надійне шифрування сеансів.

Також важливо не лише оновити політики доступу, але й перевірити конфігурацію мережевого обладнання, серверів та кінцевих пристроїв, щоб переконатися, що незашифровані протоколи не використовуються приховано або через неправильні налаштування. Це може включати налаштування обмежень у міжмережевих екранах (firewall), оновлення правил маршрутизації та введення обов'язкових вимог до використання лише зашифрованих каналів.

Таким чином, ретельна перевірка та усунення незахищених протоколів є необхідним кроком для забезпечення інформаційної безпеки. Впровадження сучасних криптографічних стандартів дозволяє значно знизити ризики перехоплення даних та гарантує захист конфіденційної інформації від потенційних атак.

Ключові кроки аудиту правил міжмережевого екрану:

- Перевірка політики за замовчуванням – переконатися, що останнім правилом для вхідного та вихідного трафіку є правило deny all (заборонити все).
- Виявлення надто дозвільних правил – шукати правила, що містять any (будь-який) в полях джерела, призначення або порту.
- Усунення застарілих та невикористовуваних правил – аналізувати лічильники спрацювань правил (hit counters) для виявлення тих, що не використовуються протягом тривалого часу.
- Перевірка на наявність "тіньових" правил (shadowed rules) – виявляти правила, які ніколи не спрацюють, оскільки їх перекривають більш загальні правила, розташовані вище у списку.
- Блокування небезпечних протоколів: Систематично забороняти використання незашифрованих та вразливих протоколів.

– Документування правил – кожне правило повинно мати чіткий опис, що пояснює його призначення, відповідальну особу та термін дії (якщо застосовно).

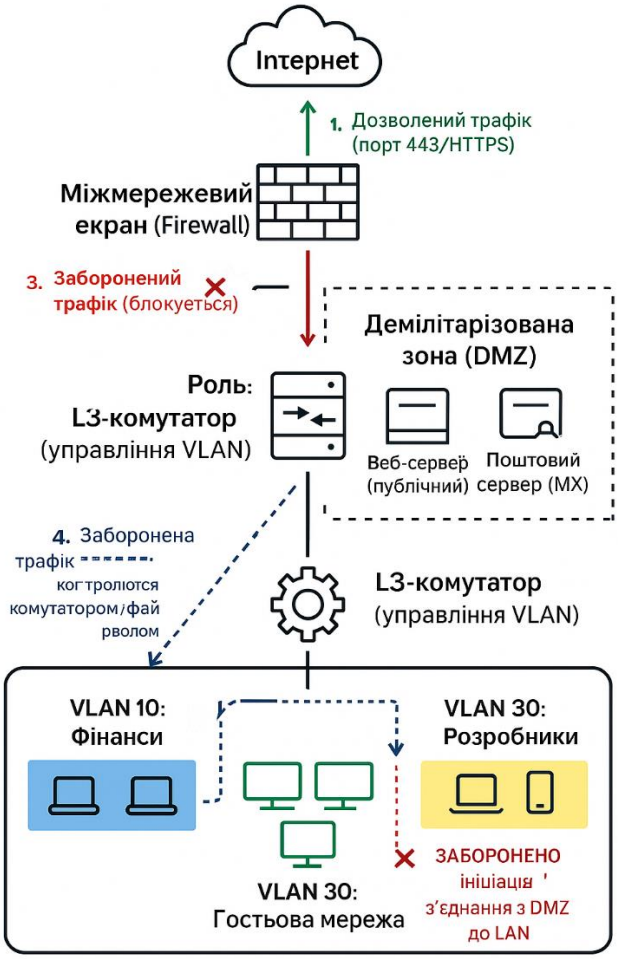

Рисунок 3.3 – Архітектура мережі з використанням VLAN та DMZ

На рисунку 3.3 показано, як Інтернет-трафік проходить через зовнішній файрвол. Запити до публічних сервісів (веб-сервер) спрямовуються в DMZ. Внутрішня мережа сегментована на VLAN для різних відділів і захищена внутрішнім файрволом, який контролює трафік як з Інтернету, так і з DMZ.

Наступним важливим заходом є сегментація мережі. Це практика поділу великої комп'ютерної мережі на менші логічні підмережі, або сегменти. Основна мета сегментації – обмеження поширення атаки. Якщо зловмисник скомпрометує

один сегмент, він не зможе вільно пересуватися по всій мережі, оскільки трафік між сегментами контролюється файрволом. Одним з найпоширеніших методів реалізації сегментації є використання віртуальних локальних мереж (VLAN). VLAN дозволяє групувати пристрої в логічні мережі незалежно від їх фізичного розташування. Можна створити окремі VLAN для відділу фінансів, розробки та для гостьових пристроїв, ізолювавши їх трафік один від одного.

Особливим типом сегментації є створення демілітаризованої зони (DMZ). DMZ – це проміжний сегмент мережі, розташований між внутрішньою (довіреною) мережею та зовнішньою (недовіреною). У DMZ розміщують сервіси, які повинні бути доступні з Інтернету, наприклад, веб-сервери, поштові сервери або DNS-сервери. Така архітектура захищає внутрішню мережу: навіть якщо сервер у DMZ буде скомпрометований, зловмисник не отримає прямого доступу до критичних корпоративних ресурсів, оскільки для цього йому доведеться подолати ще один рівень файрволу.

Третім компонентом захисту трафіку є його шифрування, особливо коли він передається через публічні мережі. Для цього широко використовуються віртуальні приватні мережі (VPN), які створюють зашифрований тунель між двома точками.

Найбільш поширеними технологіями є IPsec та SSL/TLS VPN. IPsec VPN часто використовується для з'єднання «сайт-сайт» (site-to-site), об'єднуючи офіси компанії в єдину захищену мережу, а також для віддаленого доступу співробітників. SSL/TLS VPN, у свою чергу, є популярним рішенням для надання доступу до конкретних веб-додатків через браузер без необхідності встановлення складного клієнтського ПЗ.

Таблиця 3.2 – Порівняння протоколів VPN для захисту трафіку

Характеристика	IPsec VPN	SSL/TLS VPN
Рівень моделі OSI	Мережевий рівень (L3)	Транспортний/Сеансовий рівень (L4/L5)
Основне застосування	Site-to-site з'єднання, повний доступ до мережі для віддалених клієнтів.	Віддалений доступ до веб-додатків та специфічних сервісів.
Складність налаштування	Висока. Потребує налаштування на обох кінцях тунелю.	Низька. Часто реалізується через веб-портал.
Клієнтське ПЗ	Зазвичай вимагає спеціалізованого клієнтського ПЗ.	Може працювати через стандартний веб-браузер.
Проходження через NAT	Може мати проблеми з проходженням (NAT Traversal).	Легко проходить, оскільки використовує стандартний порт 443 (HTTPS).
Гранулярність доступу	Надає повний доступ до мережі (менш гранулярний).	Дозволяє надавати доступ до окремих додатків (більш гранулярний).

Застосування зашифрованих тунелів у сучасній корпоративній мережевій інфраструктурі представляє собою один з найбільш ефективних та надійних методів забезпечення криптографічного захисту інформації під час її передачі через потенційно небезпечні канали зв'язку, оскільки ці технології створюють захищені віртуальні канали всередині існуючої мережевої інфраструктури, де всі дані автоматично шифруються на стороні відправника та розшифровуються лише на стороні легітимного одержувача, що робить перехоплену інформацію практично непридатною для використання несанкціонованими особами навіть у випадку успішної компрометації мережевих каналів передачі.

Криптографічні алгоритми, що використовуються в сучасних VPN-тунелях, включаючи AES з довжиною ключа 256 біт, RSA, ECDSA та інші провідні стандарти шифрування, забезпечують такий рівень криптографічної стійкості, який робить розшифрування перехопленої інформації практично неможливим навіть при використанні найпотужніших обчислювальних ресурсів та передових методів криптоаналізу, що дає організаціям впевненість у конфіденційності своїх комунікацій навіть при передачі через публічні мережі або потенційно скомпрометовані канали зв'язку.

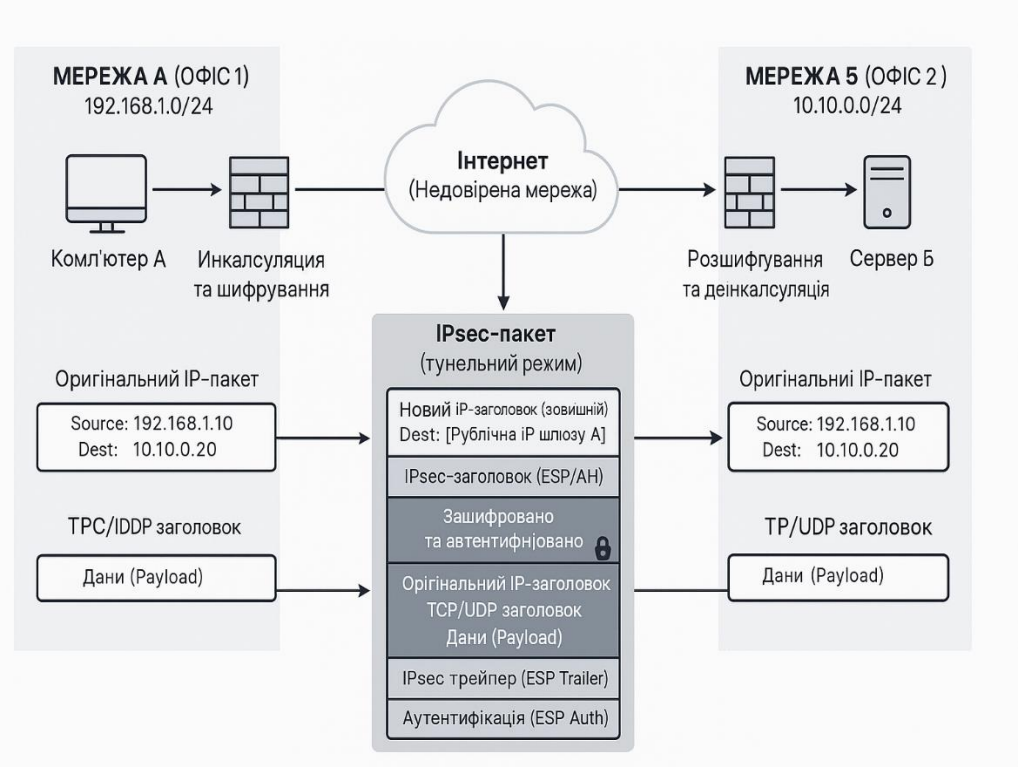

Рисунок 3.4 – Схема роботи IPsec VPN в тунельному режимі

Рис. 3.4 ілюструє, як IPsec VPN інкапсулює весь оригінальний IP-пакет (заголовок та дані) всередину нового IP-пакета з новими заголовками. Цей новий пакет шифрується і надсилається через публічну мережу (Інтернет) між двома VPN-шлюзами, забезпечуючи повну конфіденційність трафіку між двома захищеними мережами.

3.3 Впровадження сучасних рішень для виявлення загроз

Традиційні превентивні заходи безпеки, такі як файрволи та антивіруси, є необхідними, але вже недостатніми для протидії сучасному ландшафту кіберзагроз. Зловмисники постійно розробляють нові, більш витончені методи атак (zero-day, атаки без файлів, складні постійні загрози – APT), які здатні обходити стандартні засоби захисту. У зв'язку з цим парадигма безпеки

зміщується від виключно запобігання до комплексного підходу, що включає швидке виявлення, аналіз та реагування на інциденти. Для реалізації цього підходу необхідно впроваджувати сучасні рішення, що забезпечують глибоку видимість мережевих процесів та дозволяють проактивно виявляти загрози.

Центральним елементом сучасної системи виявлення є система управління інформаційною безпекою та подіями (Security Information and Event Management, SIEM). SIEM-система виконує функцію "нервового центру" безпеки, агрегуючи, нормалізуючи та корелюючи дані з величезної кількості джерел у режимі реального часу.

До таких джерел належать журнали подій (логи) з серверів, робочих станцій, мережевого обладнання (файрволів, комутаторів), систем виявлення вторгнень, антивірусів та додатків. Завдяки централізованому збору даних SIEM дозволяє аналітикам безпеки бачити повну картину того, що відбувається в мережі.

Основна цінність SIEM полягає в її здатності до кореляції подій. Система використовує набір правил для виявлення послідовностей подій, які окремо можуть здаватися нешкідливими, але разом вказують на потенційну атаку. Наприклад, SIEM може виявити ланцюжок, зокрема «невдала спроба входу на сервер з облікового запису А -> успішний вхід через 5 хвилин з того ж облікового запису, але з іншої країни -> спроба підвищення привілеїв».

Такий ланцюжок з високою ймовірністю свідчить про компрометацію облікового запису. При виявленні подібних інцидентів SIEM автоматично генерує сповіщення (алерт), що дозволяє команді безпеки негайно розпочати розслідування.

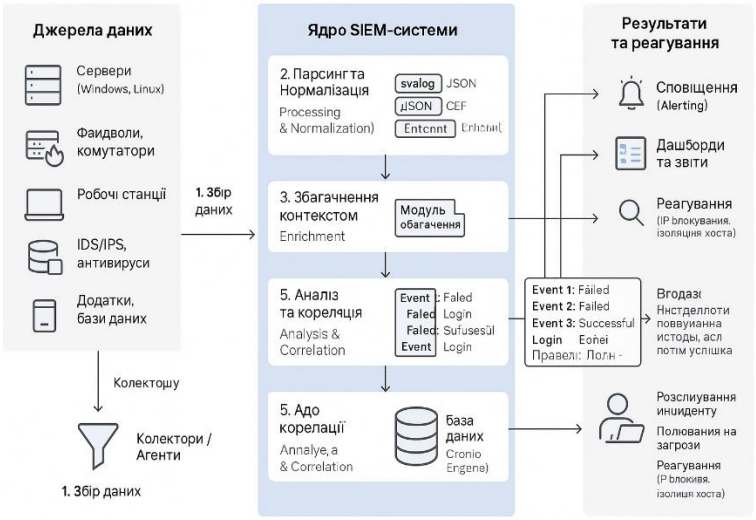

Рисунок 3.5 – Архітектура та принцип роботи SIEM-системи

На рисунку 3.5 показано, як дані з різноманітних джерел (серверів, файрволів, робочих станцій) надходять до колектора SIEM. Далі вони проходять етапи парсингу, нормалізації та збагачення контекстом. Ядро кореляції аналізує події за допомогою правил і виявляє інциденти, які відображаються на дашбордах та у вигляді алертів для аналітиків безпеки.

Доповненням до SIEM є системи виявлення та запобігання вторгненням (Intrusion Detection/Prevention Systems, IDS/IPS). IDS, як пасивна система, аналізує копію мережевого трафіку або активність на хості і, виявивши підозрілу дію, генерує сповіщення. IPS, у свою чергу, є активною системою, яка розміщується в розриві мережі (inline) і здатна не тільки виявляти, але й миттєво блокувати шкідливий трафік, не допускаючи його до цільової системи.

Типи систем виявлення та запобігання вторгненням:

– Мережеві IDS/IPS (NIDS/NIPS): Аналізують трафік, що проходить через певний сегмент мережі. NIPS встановлюється в розрив мережі для блокування атак, NIDS підключається до SPAN-порту комутатора для моніторингу.

– Хостові IDS/IPS (HIDS/HIPS): Встановлюються на окремих хостах (серверах, робочих станціях) та аналізують їхню внутрішню активність: системні виклики, зміни файлів конфігурації, активність процесів.

– Сигнатурні системи: Виявляють атаки, порівнюючи трафік або активність із базою даних відомих сигнатур (зразків) шкідливого коду або поведінки. Ефективні проти відомих загроз, але безсилі проти нових (zero-day).

– Аномалійні системи: Створюють «еталон» (baseline) нормальної поведінки мережі або хоста. Будь-яке значне відхилення від цього еталону вважається аномалією та потенційною атакою. Можуть виявляти нові загрози, але схильні до хибних спрацювань.

Для ефективного захисту рекомендується використовувати комбінацію NIPS на периметрі мережі та HIPS на критично важливих серверах. Це створює багаторівневий захист, де мережева система блокує атаки ззовні, а хостова захищає від внутрішніх загроз або атак, які змогли обійти периметр.

Останнім часом все більшого поширення набуває використання технологій машинного навчання (Machine Learning, ML) для автоматизованого аналізу аномального трафіку. Традиційні аномалійні IDS/IPS вимагають ручного налаштування порогів чутливості та часто генерують велику кількість хибних спрацювань.

ML-моделі, навчені на великих обсягах даних про нормальну поведінку мережі, здатні самостійно виявляти складні та нелінійні патерни, що вказують на аномалії. Системи аналізу поведінки користувачів та сутностей (User and Entity Behavior Analytics, UEBA) використовують ML для створення профілів нормальної активності для кожного користувача та пристрою. Це дозволяє виявляти такі загрози, як скомпрометовані облікові записи, внутрішні загрози (інсайдери) та повільні, приховані атаки, які важко помітити за допомогою традиційних правил кореляції.

Таблиця 3.3 – Порівняння систем виявлення (IDS) та запобігання (IPS) вторгненням

№	Параметр	Система виявлення вторгнень (IDS)	Система запобігання вторгненням (IPS)
1	Основна функція	Виявлення та сповіщення про атаку.	Виявлення та блокування атаки в реальному часі.
2	Режим роботи	Пасивний (out-of-band). Аналізує копію трафіку.	Активний (inline). Весь трафік проходить крізь систему.
3	Вплив на мережу	Не створює затримок, оскільки працює поза основним каналом.	Може вносити невелику затримку (latency).
4	Ризик відмови	У разі відмови системи моніторинг припиняється, але мережа продовжує працювати.	У разі відмови система може заблокувати весь легітимний трафік (стає "точкою відмови").
5	Реакція на загрозу	Інформує адміністратора, який приймає рішення.	Автоматично блокує шкідливий трафік згідно з політиками.

Інтеграція SIEM (Security Information and Event Management), систем виявлення та запобігання вторгненням (IDS/IPS) та рішень на основі машинного навчання (ML) формує цілісну, інтелектуальну екосистему для кібербезпеки. SIEM виступає основним центром збору, аналізу та кореляції подій безпеки з різних джерел, об’єднуючи логи серверів, мережевих пристроїв, додатків та систем автентифікації.

Однак традиційні SIEM-системи часто стикаються з проблемами «перевантаженості подіями» та великою кількістю хибнопозитивних сповіщень, що ускладнює ефективне реагування на реальні загрози. Доповнення SIEM механізмами IDS/IPS дозволяє не лише виявляти шкідливий трафік у реальному часі, а й оперативно блокувати спроби вторгнень або аномальну активність у мережі. IDS (Intrusion Detection System) аналізує сигнатури атак та шаблони поведінки, а IPS (Intrusion Prevention System) може автоматично реагувати на загрози, блокуючи небезпечні пакети чи з’єднання.

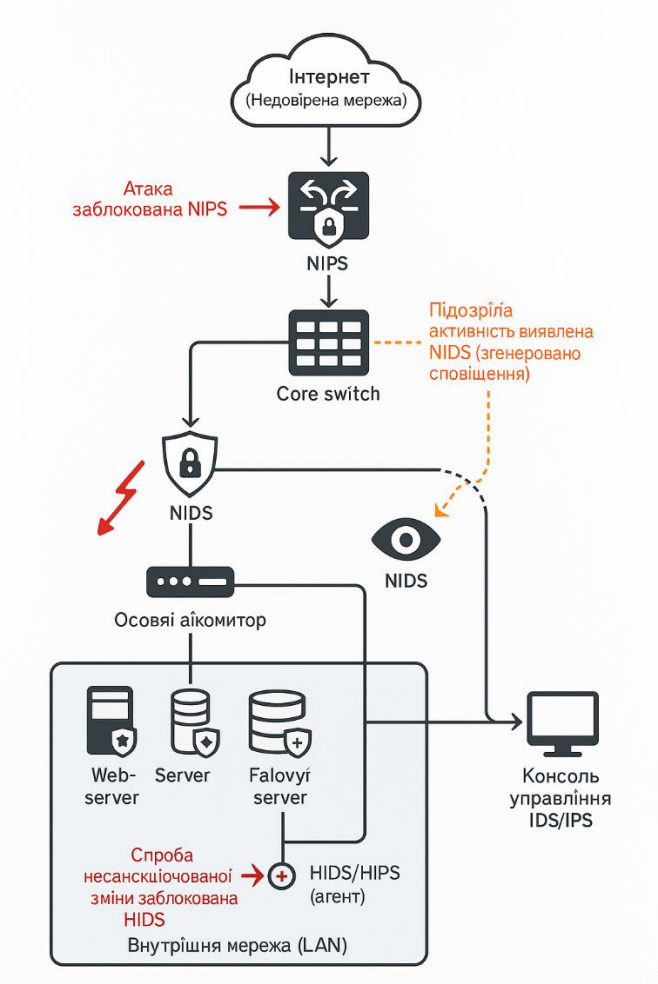

Рисунок 3.6 – Розміщення NIDS/NIPS та HIDS в мережі

Рисунок 3.6 ілюструє типову схему розміщення. NIPS встановлено на вході в мережу, одразу після файрволу, для блокування зовнішніх атак. NIDS підключено до SPAN-порту внутрішнього комутатора для моніторингу трафіку між сегментами. HIDS встановлено на критичних серверах для контролю їхньої внутрішньої активності.

3.4 Організаційні та технічні заходи для підвищення безпеки

Ефективний захист комп'ютерної мережі не може покладатися виключно на технологічні рішення. Найсучасніший файрвол або система виявлення вторгнень можуть виявитися безсилими, якщо співробітники компанії не дотримуються

базових правил кібергігієни, а в організації відсутні чітко визначені процеси та політики безпеки. Людський фактор залишається однією з головних причин успішних кібератак, чи то через фішингові листи, використання слабких паролів або випадкове розголошення конфіденційної інформації. Тому для побудови комплексної та стійкої системи захисту необхідно поєднувати технічні заходи з потужними організаційними компонентами, створюючи цілісну культуру безпеки.

Фундаментом організаційного захисту є розробка та впровадження корпоративних політик безпеки. Політики – це формалізовані документи, які визначають правила, процедури та обов'язки всіх співробітників щодо захисту інформаційних активів компанії. Вони слугують основою для прийняття рішень, налаштування технічних засобів та проведення аудитів.

Основні корпоративні політики у сфері інформаційної безпеки:

- Загальна політика інформаційної безпеки (Information Security Policy): Верхньорівневий документ, що визначає цілі, завдання та відповідальність керівництва за забезпечення безпеки.
- Політика прийнятного використання (Acceptable Use Policy, AUP): Правила використання співробітниками комп'ютерів, мережі, інтернету, електронної пошти та інших корпоративних ресурсів.
- Політика класифікації та обробки даних (Data Classification Policy): Визначає рівні конфіденційності інформації (наприклад, публічна, внутрішня, конфіденційна, таємна) та правила поводження з кожним типом даних.
- Політика контролю доступу (Access Control Policy): Описує принципи надання, зміни та відкликання прав доступу до систем та даних на основі ролей та принципу мінімальних привілеїв.
- Політика резервного копіювання (Backup Policy): Визначає, які дані підлягають резервуванню, з якою частотою, як довго зберігаються копії та хто несе відповідальність за процес.

– План реагування на інциденти (Incident Response Plan, IRP): Детальний покроковий план дій, який необхідно виконати у разі виявлення інциденту безпеки (від ідентифікації до відновлення та аналізу).

– Політика управління змінами (Change Management Policy): Процедури для безпечного впровадження змін в IT-інфраструктуру, щоб мінімізувати ризики виникнення нових вразливостей.

Однак наявність політик сама по собі не гарантує безпеки. Необхідно, щоб кожен співробітник знав, розумів і дотримувався цих правил. Це досягається через регулярні програми навчання та підвищення обізнаності персоналу. Мета таких програм – перетворити співробітників із "найслабшої ланки" на "людський файрвол". Навчання повинно бути безперервним та охоплювати актуальні загрози: як розпізнавати фішингові листи та повідомлення, правила створення та зберігання надійних паролів, небезпеки соціальної інженерії, правила безпечної роботи з мобільними пристроями та у публічних Wi-Fi мережах.

Ефективними методами є проведення симуляцій фішингових атак, які дозволяють співробітникам на практиці навчитися виявляти загрози, а також регулярні тренінги, вебінари та інформаційні розсилки. Навіть при найкращих превентивних заходах інциденти все одно можуть трапитися.

Тому критично важливим технічно-організаційним заходом є розробка надійної стратегії резервного копіювання та відновлення. Це єдиний гарантований спосіб відновити дані та працездатність систем після руйнівної атаки, наприклад, шифрувальника (ransomware), або апаратного збою.

Ефективна стратегія базується на правилі "3-2-1": мати щонайменше три копії даних, зберігати їх на двох різних типах носіїв, і одна з копій повинна знаходитись поза основним робочим майданчиком (off-site), бажано в ізольованому від основної мережі середовищі (air-gapped).

Необхідно чітко визначити два ключові показники: цільову точку відновлення (Recovery Point Objective, RPO) – максимальний допустимий обсяг

втрати даних, та цільовий час відновлення (Recovery Time Objective, RTO) – максимальний час, протягом якого система має бути відновлена. На основі цих показників обирається тип та частота резервного копіювання.

Таблиця 3.4 – Порівняння типів резервного копіювання

№	Тип копіювання	Опис	Швидкість створення	Необхідний об'єм сховища	Швидкість відновлення
1	Повне (Full)	Копіюються всі обрані дані.	Найповільніше.	Найбільший.	Найшвидше (потрібна лише одна копія).
2	Інкрементне (Incremental)	Копіюються лише дані, що змінилися з моменту останнього копіювання (будь-якого типу).	Швидке.	Найменший.	Найповільніше (потрібне повне + всі інкрементні).
3	Диференційне (Differential)	Копіюються лише дані, що змінилися з моменту останнього повного копіювання.	Середнє.	Середній (зростає з часом).	Середнє (потрібне повне + останнє диференційне).

Проте, просто мати резервні копії недостатньо. Необхідно регулярно тестувати механізми відновлення, щоб переконатися, що копії є цілісними, а процес відновлення працює належним чином. Без тестування компанія може виявити, що її бекапи пошкоджені або неповні, саме в той момент, коли вони найбільше потрібні.

Таким чином, поєднання чітких політик, обізнаного персоналу та надійної, перевіреної стратегії резервного копіювання та відновлення створює потужний фундамент, який доповнює та посилює технічні засоби захисту, формуючи цілісну та глибоко ешелоновану систему безпеки.

ВИСНОВКИ

У результаті проведеного дослідження здійснено комплексний аналіз сучасних методів та засобів захисту комп’ютерних мереж, що дозволив сформувати цілісне уявлення про принципи інформаційної безпеки, класифікацію загроз, ефективність превентивних заходів та стратегій реагування.

У першому розділі розглянуто теоретичні засади інформаційної безпеки, зокрема концепцію CIA-тріади (конфіденційність, цілісність, доступність), а також класифікацію загроз комп’ютерним мережам за природою виникнення та потенційним впливом. Проведений аналіз засвідчив, що у сучасному інформаційному просторі загрози характеризуються мультивекторністю та високою складністю реалізації, що вимагає системного підходу до їх нейтралізації.

Другий розділ присвячено аналізу існуючої системи захисту мережі підприємства. Детально розглянуто її фізичну та логічну архітектуру, структуру VLAN, DMZ-сегменти та налаштування міжмережевого екрану. Виявлено ряд критичних вразливостей, зокрема незахищені порти, використання застарілих протоколів передавання даних та надмірні повноваження користувачів, що потенційно можуть бути використані для компрометації системи. Проведена оцінка ризиків дозволила класифікувати загрози за рівнем ймовірності та потенційним впливом, сформувавши основу для розробки стратегії їхнього усунення.

Третій розділ присвячено шляхам оптимізації та удосконалення системи захисту комп’ютерної мережі. Запропоновано заходи з посилення аутентифікації та контролю доступу, включаючи впровадження багатофакторної аутентифікації (MFA) та модель управління доступом на основі ролей (RBAC). Оптимізовано політики міжмережевого екрану через переведення на принцип "заборони за замовчуванням", сегментацію трафіку та впровадження VPN для захисту

передавання даних. Окрему увагу приділено впровадженню SIEM-систем, IDS/IPS та механізмів аналізу аномалій для оперативного виявлення та реагування на загрози.

Практичне значення проведеного дослідження полягає у розробці рекомендацій щодо підвищення стійкості мережевої інфраструктури до сучасних кіберзагроз. Запропоновані рішення можуть бути використані для оптимізації безпекових політик підприємства, впровадження комплексного моніторингу подій та покращення механізмів контролю доступу.

Загалом, Ефективна система захисту комп’ютерної мережі має ґрунтуватися на багаторівневій безпеці, адаптивності до нових загроз та використанні інтелектуальних методів аналізу. Багаторівневий захист передбачає комплекс заходів, включаючи файрволи, сегментацію мережі, управління доступом, моніторинг загроз та резервне копіювання, щоб зменшити ризик компрометації системи. Адаптивність забезпечується регулярними оновленнями, впровадженням автоматизованих механізмів реагування та використанням машинного навчання для виявлення аномалій. Інтелектуальні методи аналізу, зокрема SIEM-системи та поведінковий аналіз користувачів, дозволяють виявляти складні загрози ще до їхньої активної реалізації. Успішне впровадження таких заходів сприяє зниженню ризиків, підвищенню стійкості мережевої інфраструктури та забезпеченню стабільної роботи інформаційних систем підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про інформацію». URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 20.02.2025)
2. Закон України «Про захист інформації в інформаційнотелекомунікаційних системах». URL: https://zakon.rada.gov.ua/laws/show/80/94вр#Text (дата звернення: 20.02.2025)
3. ДСТУ ISO/IEC 27002:2015. Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66911 (дата звернення: 23.02.2025).
4. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки. URL: https://online.budstandart.com/ua/catalog/docpage.html?id_doc=104399 (дата звернення: 25.02.2025)
5. Інформаційні технології. Методи захисту. Настанови щодо готовності інформаційно-комунікаційних технологій для неперервності роботи бізнесу. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104404 (дата звернення: 25.02.2025)
6. Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки. URL: https://online.budstandart.com/ua/catalog/docpage.html?id_doc=104405 (дата звернення: 03.03.2025)
7. Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. Частина 1. Принципи та процеси. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=104403 (дата звернення: 05.03.2025)

8. Cisco ASA 5506-X Firewall with FirePOWER Services. Cisco Systems. URL: https://www.cisco.com/c/en/us/products/security/asa-5506-x-firepowerservices/index.html (дата звернення: 10.03.2025)
9. Ubiquiti UniFi Security Gateway PRO (USG-PRO-4). Ubiquiti Networks. URL: https://www.ui.com/unifi-routing/usg-pro-4/ (дата звернення: 11.03.2025)
10. Fortinet FortiGate 60F Firewall. Fortinet. URL: https://www.fortinet.com/products/next-generation-firewall/fortigate-60f (дата звернення: 12.03.2025)
11. Hikvision DS-2CD2143G0-IS 4MP Dome Camera. Hikvision. URL: https://www.hikvision.com/en/products/IP-Products/Network-Cameras/Pro-Series/DS-2CD2143G0-IS/ (дата звернення: 15.03.2025)
12. Мережевий комутатор Cisco Catalyst 2960X-48FPD-L. Cisco Systems. URL: https://www.cisco.com/c/en/us/products/switches/catalyst-2960-x-seriesswitches/index.html (дата звернення: 19.03.2025)
13. Кібербезпека та ризики цифрової трансформації компаній / Ю. Когут. Київ: Сідкон, 2021.
14. Інформаційна безпека / О. Фармагей. Київ: Ліра-К, 2020.
15. Забезпечення інформаційної безпеки як функція сучасних держав: порівняльно-правовий аналіз / за ред. В. Цимбалюка. Київ: Юрінком Інтер, 2019.
16. Основи кіберпростору, кібербезпеки та кіберзахисту / за ред. І. Бойка. Львів: Видавництво Львівської політехніки, 2020.
17. ISO/IEC 27001:2022 Implementation Guide. BSI Group. URL: https://www.bsigroup.com/en-GB/iso-27001-information-security/ (дата звернення: 30.04.2025)

18. COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution. ISACA. URL: https://www.isaca.org/resources/cobit (дата звернення: 30.04.2025).
19. ITIL® 4 Practice Guide. AXELOS. URL: https://www.axelos.com/resource-hub/practice/readers-manual-itil-4-practice-guide (дата звернення: 05.05.2025)
20. NIST Cybersecurity Framework (CSF) 2.0. National Institute of Standards and Technology. URL: https://www.nist.gov/cyberframework (дата звернення: 21.05.2025)
21. NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide. National Institute of Standards and Technology. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf (дата звернення: 11.05.2025)
22. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems Requirements. URL: https://www.iso.org/standard/27001 (дата звернення: 11.05.2025)
23. COBIT 2019 Framework: Governance and Management Objectives. ISACA. URL: https://www.isaca.org/resources/cobit (дата звернення: 18.05.2025)
24. ITIL® 4 Foundation. AXELOS. URL: https://www.axelos.com/certifications/itil-service-management/itil-4-foundation/ (дата звернення: 18.05.2025)
25. CIS Critical Security Controls v8. Center for Internet Security. URL: https://www.cisecurity.org/controls/v8 (дата звернення: 21.05.2025)
26. Базилевич В. М., Мехед Д. Б., Ткач Ю. М. Комп'ютерні мережі. Протоколи, технології, обладнання: нав. посібник. Ніжин, 2018.
27. Городецька О. С., Гикавий В. А., Онищук О. В. Комп'ютерні мережі: нав. посібник. Вінниця, 2017.

28. Жураковський Б. Ю., Зенів І. О. Комп'ютерні мережі: нав. посібник. Київ, 2020.

29. Стівенс, У.Р. TCP/IP великим планом. К. : BHV, 2017.

30. Волтер Айзексон. Інноватори: Як група хакерів, геніїв та ґіків здійснила цифрову революцію. Київ: Наш Формат, 2017. с. 488. ISBN 978617-7279-81-4.

31. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи / О.А. Сороківська, В.Л. Гевко. – URL: http://nbuv.gov.ua/portal / Soc_Gum/Vchnu_ekon/2010_2_2/032- 035.pdf.

32. XSpiders. URL: https://www.ptsecurity.com/products/XSpider/. (дата звернення: 21.05.2025)

33. TRACE. URL: https://developer.mozilla.org/docs/Web/HTTP/Methods/TR ACE . (дата звернення: 21.05.2025).

34. Тарнавський Ю.А. Організація комп'ютерних мереж / Ю.А. Тарнавський, І.М. Кузьменко К.: КПІ ім. Ігоря Сікорського, 2018. 259 с. (дата звернення: 27.05.2025).

35. Танасійчук В. І., Сопко В. В. Захист інформації в комп'ютерних мережах. Київ: Університет «Україна», 2021. 240 с (дата звернення: 27.05.2025).

36. Державна служба спеціального зв'язку та захисту інформації України. Аналітичний огляд кіберзагроз за 2023 рік. Київ, 2024 (дата звернення: 30.05.2025).

37. Чумаченко В. Г., Коляденко С. В. Інформаційна безпека: сучасні загрози та методи захисту. Харків: НТУ "ХПІ", 2020. 198 с. (дата звернення: 30.05.2025)

38. Cisco. 2023 Cybersecurity Almanac: 100 facts and predictions. San Jose, 2023. URL: https://www.cisco.com/c/en/us/products/security/cybersecurityalmanac.html (дата звернення: 30.05.2025).