МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
Циклова комісія (кафедра) комп'ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему

ОПТИМІЗАЦІЯ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ

Виконав: студент групи 2П-21
Спеціальності
121 Інженерія програмного забезпечення
Ростислав БОНДАР
Керівник:
Майя ЛЮТА

Черкаси 2025

АНОТАЦІЯ

Кваліфікаційна робота присвячена дослідженню методів та засобів оптимізації захисту корпоративної мережі з метою підвищення рівня інформаційної безпеки та забезпечення безперебійного функціонування бізнес-процесів. У роботі детально проаналізовано сучасні кіберзагрози, які становлять небезпеку для корпоративних мереж, зокрема атаки типу DDoS, фішинг, витоки конфіденційної інформації та проникнення шкідливого програмного забезпечення. Розглянуто найпоширеніші уразливості в конфігурації мережевого обладнання, слабкості в організаційних політиках безпеки, а також недоліки існуючих систем захисту.

Запропоновано комплексний підхід до оптимізації системи інформаційної безпеки, що включає впровадження інтегрованих рішень для моніторингу та реагування на інциденти, зокрема системи виявлення вторгнень (IDS), системи запобігання вторгненням (IPS), антивірусні комплекси, мережеві екрани (firewall) та передові криптографічні технології. Окремо досліджено питання створення та впровадження ефективних політик безпеки на рівні мережевого обладнання, що забезпечують проактивне запобігання загрозам.

Практична частина роботи включає побудову моделі оптимізованої корпоративної мережі за допомогою спеціалізованого програмного забезпечення, проведення комплексного аналізу її ефективності, а також розробку рекомендацій та практичних вказівок щодо впровадження запропонованих рішень у реальних умовах експлуатації.

Ключові слова: КОРПОРАТИВНА МЕРЕЖА, ОПТИМІЗАЦІЯ ЗАХИСТУ, ІНФОРМАЦІЙНА БЕЗПЕКА, IDS, IPS, КРИПТОГРАФІЯ, DDOS- АТАКИ, ФІШИНГ, МОНІТОРИНГ БЕЗПЕКИ.

ABSTRACT

The thesis is dedicated to exploring methods and tools for optimizing corporate network security to enhance information protection and ensure uninterrupted business processes. The study thoroughly analyzes modern cybersecurity threats that pose significant risks to corporate networks, such as DDoS attacks, phishing attempts, confidential information leaks, and malware intrusions. It identifies common vulnerabilities in network configurations, weaknesses in organizational security policies, and limitations of existing protection mechanisms. A comprehensive approach to information security optimization is proposed, encompassing the integration of advanced monitoring and incident response solutions, such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), antivirus software, firewalls, and advanced cryptographic technologies.

Additionally, the research addresses the development and implementation of effective network-level security policies designed for proactive threat prevention.

The practical component includes constructing an optimized corporate network model using specialized software, performing a thorough evaluation of its effectiveness, and developing actionable recommendations and practical guidelines for deploying the proposed solutions in real-world operational conditions.

Keywords: CORPORATE NETWORK, SECURITY OPTIMIZATION, INFORMATION SECURITY, IDS, IPS, CRYPTOGRAPHY, DDOS ATTACKS, PHISHING, SECURITY MONITORING.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

ПЗ	–	Програмне забезпечення
VPN	–	Virtual private network
WPA	–	Wi-Fi protected access
MAC	–	Media access control
IDS	–	Intrusion detection system
IPS	–	Intrusion protection system
SIEM	–	Security information and event management;
DMZ	–	Demilitarized zone
SSL	–	Secure sockets layer
MFA	–	Multi-factor Authentication
DDoS	–	Distributed denial-of-service attack
DNS	–	Domain Name System
WAF	–	Web application firewall
VLSM	–	variable length subnet masks
IP	–	Internet Protocol
VLAN	–	Virtual local area network
SSH	–	Secure shell

ВСТУП

У сучасну епоху цифровізації корпоративні мережі відіграють критично важливу роль у діяльності підприємств, забезпечуючи обмін інформацією між підрозділами та з зовнішніми сервісами. Проте з удосконаленням технологій зростає і складність кіберзагроз, спрямованих на системи інформаційної безпеки. Відповідно до звіту Microsoft, характер глобальних кіберзагроз постійно ускладнюється , а за даними Державної служби спеціального зв'язку та захисту інформації України кількість кібератак у 2024 році зросла на 69,8% порівняно з попереднім роком. Найчастіше інциденти виникають через людський фактор – за оцінками фахівців, 82% усіх порушень безпеки пов'язані з помилками співробітників [1]. Таким чином, на фоні зростаючого обсягу та різноманітності кіберзагроз стає особливо актуальним вдосконалення (оптимізація) системи захисту корпоративної мережі. Це дозволить знизити вразливість інформаційних ресурсів підприємства, мінімізувати ризики несанкціонованого доступу та забезпечити стабільне функціонування бізнес-процесів.

Метою дослідження є розробка рекомендацій і алгоритмів для оптимізації захисту корпоративної мережі з метою підвищення її надійності та ефективності. Це передбачає створення комплексної моделі заходів безпеки, що поєднує технічні рішення (фаєрволи, IDS/IPS, VPN тощо) з організаційними заходами (політики доступу, навчання персоналу тощо), та оцінку її впливу на стійкість мережі до різних видів кіберзагроз.

Завдання дослідження:

1. Проаналізувати наукові джерела та нормативні документи з питань захисту інформації і безпеки корпоративних мереж.
2. Виявити характерні загрози та вразливості корпоративних мереж (зокрема сучасні випадки атак).
3. Оглянути існуючі технології захисту мережевих ресурсів (фаєрволи, системи виявлення атак, VPN, антивірусні рішення тощо).
4. Розробити пропозиції щодо оптимізації системи захисту

корпоративної мережі (введення сегментації мережі, багатофакторної аутентифікації, регулярних оновлень ПЗ та ін.).

5. Сформулювати практичні рекомендації щодо впровадження оптимізованих рішень із захисту мережі.

Об’єктом дослідження є корпоративна комп’ютерна мережа як складова інформаційної системи підприємства. Предметом дослідження виступають процеси та методи оптимізації системи захисту корпоративної мережі, які забезпечують підвищення рівня інформаційної безпеки при ефективному використанні ресурсів.

У процесі дослідження було застосовано низку теоретичних, емпіричних, аналітичних методів.

РОЗДІЛ 1
АНАЛІЗ СТРУКТУРИ ТА ЗАГРОЗ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ ШКОЛИ

1.1 Структура та особливості корпоративних мереж

Корпоративна мережа школи складається з кількох підмереж, об’єднаних єдиною інфраструктурою. У її основі, лежить центральний маршрутизатор, який через зовнішній інтерфейс виходить в інтернет і забезпечує мережі публічну IP-адресу. Маршрутизатор, налаштований на NAT/PAT для спільного доступу внутрішніх пристроїв до одного зовнішнього адресного простору.

Внутрішня мережа організована за принципом «зірки» - кінцеві пристрої (навчальні комп’ютери, сервери, робочі станції вчителів) підключені до центральних комутаторів. Зазвичай IP-адресація реалізована у приватному діапазоні (наприклад, 192.168.0.0/24 або 10.0.0.0/24). Маршрутизатор виконує роль DHCP-сервера, автоматично роздаючи IP-адреси клієнтам у визначеному діапазоні, а деякі ключові вузли (наприклад, сервери чи принтери) можуть мати статичні адреси. Мережа може містити і внутрішній DNS-сервер (або перенаправлення DNS-запитів на зовнішній), хоча деталі не критичні для безпеки [6].

Безпровідний доступ у школі реалізовано через точку доступу (Wi-Fi), проте не до кінця зрозуміло, чи увімкнене шифрування. Якщо використовується лише протокол WEP або мережа відкрита, це суттєво знижує конфіденційність (WEP є легко зламаним. Натомість правильним рішенням було б застосування WPA2/WPA3 з сильною аутентифікацією [2].

Структурно мережа виглядає досить «плоскою», у ній відсутня виражена сегментація на окремі VLAN для учнів та викладачів. Ця відсутність VLAN означає, що всі пристрої фактично перебувають у єдиному широкомовному домені. Експерти підкреслюють, що традиційні плоскі мережі мають лише одну поверхню атаку, а сегментування мережі на VLAN додає багаторівневий захист і

обмежує розповсюдження загроз. Крім того, у наданій конфігурації, очевидно, невстановлені списки контролю доступу (ACL) чи міжмережеві екрани між внутрішніми підмережами, отже трафік між ними не фільтрується [11].

Основні характеристики мережі відповідають типовим рішенням у навчальних закладах. Центральний маршрутизатор із NAT і DHCP, локальні сервери та робочі станції під'єднані через комутатори, є точка бездротового доступу. Важливо відзначити, що при такій конфігурації конфіденційність, цілісність і доступність даних забезпечуються передусім організаційними заходами, адже мережа не має спеціалізованих засобів захисту (наприклад, VPN чи IDS). Загалом мережевий інфраструктурний рівень («core», «розподіл» та «доступ») у школі поєднуються в одному рівні, що спрощує адміністрування, але знижує стійкість до внутрішніх загроз [12].

1.2. Основні загрози та вразливості корпоративної мережі

Навчальна мережа зі свого характеру стикається з численними потенційними загрозами. Як зазначають спеціалісти, основна мета мережевої безпеки – гарантувати, що доступ до ресурсів матимуть лише авторизовані особи (конфіденційність), забезпечити точність та незмінність даних (цілісність) і при цьому зберегти доступність систем для легітимних користувачів. Однак у практиці мережі школи ряд недоліків створює критичні вразливості. По-перше, відсутність сегментації означає, що одна й та ж підмережа охоплює і учнів, і вчителів, і адміністрацію.

У такій структурі будь-який компрометований ПК може виконувати сканування всієї мережі чи ARP-отруєння (ARP spoofing) для перехоплення трафіку. ARP-спуфінг – це стандартний метод MITM-атаки, при якому зловмисник представляється маршрутизатором, що дозволяє йому бачити і модифікувати трафік між пристроями. Без VLAN-та ACL-трафіку атакуючий може рухатися всередині мережі практично безперешкодно [3].

По-друге, фізичний та безпровідний доступ. Якщо на маршрутизаторі або

Wi-Fi-точці доступу залишені стандартні паролі чи увімкнені незахищені служби (Telnet, HTTP замість HTTPS), це дає змогу внутрішньому нападнику отримати високі привілеї. Слабкі паролі облікових записів мережевих пристроїв чи навіть адміністративні доступи створюють критичну вразливість. Навіть у випадку активованого шифрування на Wi-Fi, застарілий WEP може бути зламаний за кілька хвилин, що дозволить зловмиснику прослуховувати мережу в радіусі дії. Ще однією загрозою є MAC-флудинг на комутаторі.

При відсутності захисту портів зловмисник може надіслати велику кількість фейкових MAC-адрес у мережу, змусивши комутатор перейти у режим широкомовлення і розсилати трафік на всі порти[14]. Як наслідок, будь-який інший підключений пристрій зможе перехопити трафік всіх сегментів мережі. Наприклад, у такому випадку загроза доступу до персональних даних чи внутрішніх серверів зростає, адже атакуючий може «слухати» весь трафік.

Інші приклади вразливостей, які випливають зі схеми мережі - це відсутність мережевого моніторингу чи IDS означає, що шкідлива активність може залишатися непоміченою. Якщо мережа використовує внутрішні сервіси (наприклад, локальний DNS), їх компрометація відкриває шлях до DNS-спуфінгу [17]. Крім того, мережа може містити IoT-пристрої (наприклад, «розумні» дошки чи камери відеоспостереження), і якщо вони з’єднані через Wi-Fi із стандартними паролями, це створює ще одну вразливість із допомогою якої, зловмисник, проникнувши через такий пристрій, отримає точку опори всередині мережі. Основні загрози та властивості межі показано в додатку А.1.

Не можна також ігнорувати ризики, пов’язані з людським фактором. Учні й педагоги, занурені в інтернет-активність (онлайн-уроки, соцмережі, ігри), часто стають легкою мішенню для зловмисників. Брак належного навчання з кібербезпеки серед учнів та вчителів збільшує ймовірність нехтування паролями чи відкриття підозрілих файлів. Загалом, для шкільної мережі типовими вразливостями є небезпечне поєднання широкого спектра користувачів з нерегулярними оновленнями ПО і недостатнім захистом локальних пристроїв.

1.3. Методи атак на корпоративну мережу

Зловмисники можуть застосовувати низку атак, спрямованих на використання вищенаведених вразливостей. Одним з основних методів є ARP-спуфінг (ARP-отруєння). В локальній мережі нападаючий посилає фальшиві ARP-відповіді, змушуючи маршрутизатор та робочі станції асоціювати MAC-адресу зловмисника з адресою шлюзу. Після цього весь внутрішній трафік передається через машину злочинця, що дозволяє перехоплювати дані, викрадати сесійні ідентифікатори або вводити шкідливі модифікації. Ця атака дозволяє зловмиснику вести «людину посередині» (MitM) всередині корпоративного сегменту без будь-яких додаткових прав [3].

Ще один поширений метод – MAC-флуд (MAC flooding). Як тільки хакер заповнить адресну таблицю комутатора фейковими MAC-адресами, той почне широкомовно розсилати пакети всім портам. У результаті криваві «переслуховування» стають можливими, наприклад, зловмисник може бачити трафік інших користувачів, завантажувати конфіденційні документи або красти дані аутентифікації. Така атака значно послаблює ефективність комутаторів та створює ризик перехоплення внутрішнього трафіку [4]. Своєю чергою, атаки на службу DHCP можуть полягати в витісненні легітимного DHCP-сервера (DHCP starvation) та розгортанні власного (rogue DHCP) – у цьому разі жертва може отримати некоректні IP-дані та DNS-сервер (сайт зловмисника), що виведе її на фішингові адреси.

Також не варто забувати про класичні мережеві атаки, потипу сканування мережі дозволяє виявити уразливі хости або відкриті порти; DNS-спуфінг може перенаправити користувачів на шкідливі ресурси. У відкритій Wi-Fi-мережі можлива атака типу Evil Twin (агресивне дублювання точки доступу) або просте підслуховування трафіку за допомогою sniffer-програм, якщо шифрування немає або воно слабке. Таким чином, набір можливих векторів атаки охоплює як рівень канального та мережевого зв’язку, так і вищі рівні. На рис. 1.1 детально зображено класифікацію мережевих атак [15].

Рисунок 1.1 – Класифікація мережевих атак

Усі ці атаки можуть бути суттєво ускладнені використанням додаткових засобів захисту. Для цього потрібно, правильне налаштування портів комутаторів (режим switchport mode access без DTP), фільтрація ARP і DHCP, наявність IDS/IPS. Без таких заходів мережа залишається вразливою до внутрішніх атак і цілком залежить від того, хто опанував доступ до неї.

1.4. Вплив людського фактора та соціальної інженерії на безпеку мережі

Людський фактор у шкільній мережі часто визначає найбільший ризик. За даними досліджень, саме користувачі є найслабшим місцем інформаційних систем. Низька обізнаність учнів і, іноді, вчителів робить їх легкою мішенню для атак соціальної інженерії – від фішингу електронною поштою до телефонних шахрайств. В освітній галузі фішинг-загрози реалізуються через масові повідомлення, що імітують офіційні ресурси школи чи звернення від батьків, що стимулюють ввести облікові дані або перейти за шкідливими посиланнями. Вчені відзначають, що понад 90% інцидентів кібербезпеки пов’язані саме з діями людей [5].

Окремо слід врахувати правила адміністратора. Багато атак починаються з

компрометації облікового запису адміністратора мережі чи системного адміністратора. Якщо доступ до критичних налаштувань не обмежений фізичними та політиками безпеки (наприклад, за замовчуванням у RouterOS може бути протокол Telnet без паролю), зловмисник, отримавши навіть соцінженерним шляхом, адміністративну привілею, отримає повний контроль над мережею. Щоб зменшити цей ризик, експерти рекомендують обмежувати права адміністраторів тільки довіреному персоналу та проводити регулярне навчання з кібергігієни.

Більше того, сучасні школи активно впроваджують BYOD (принеси свій пристрій). З одного боку, це підвищує зручність навчання, з іншого – дозволяє будь-кому підключати особистий ноутбук або смартфон до мережі, що суттєво ускладнює контроль. Як радять ІТ-фахівці, за таких умов необхідно виділяти «гостьовий» SSID з дуже обмеженим доступом, а основну мережу залишати для безпечних пристроїв школи. Якщо гостьова мережа не сегментована, зловмисник може підключити заражений шкідливим ПЗ пристрій і безперешкодно сканувати внутрішню інфраструктуру [18].

Таким чином, взаємодія персоналу та учнів із мережею завжди буде ключовим елементом безпеки. За словами експертів, навіть найсучасніші технічні рішення не захистять від цілеспрямованої атаки, якщо люди не обізнані про прийоми шахраїв. Тому освітній заклад повинен приділяти не менше уваги політикам безпеки (регулярні зміни паролів, багато-факторна аутентифікація, обмеження прав користувачів) та навчанню користувачів, ніж власне налаштуванню обладнання. Поєднання технічних і організаційних заходів дозволить мінімізувати ризики, пов’язані з людським фактором. На рис. 1.2 зображено модель дій соціального інженера.

Рисунок 1.2 – Модель дій соціального інженера

РОЗДІЛ 2
СУЧАСНІ МЕТОДИ ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ

2.1 Методи захисту існуючої мережі

Зважаючи на відсутність сегментації і централізованого sадміністрування у поточній схемі, слід впровадити базові заходи безпеки. По-перше, необхідно розділити мережу на VLAN, окремо виділивши VLAN для управління мережевими пристроями. Cisco рекомендує використовувати одну (наприклад, VLAN 1) виключно для management-трафіку пристроїв і не призначати її звичайним портам, щоб ускладнити «перестрибування» зловмисника між VLAN[6]. По-друге, усі порти комутаторів слід налаштувати з урахуванням безпеки: відключити зайві порти, увімкнути «port-security» та 802.1X (NAC) для аутентифікації пристроїв. По-третє, централізовано організувати аутентифікацію адміністраторів і користувачів за допомогою RADIUS/TACACS+ (AAA); це дозволить кожному адміністратору мати власні облікові дані замість одного спільного пароля і покращує контроль доступу [6].

Керування конфігурацією слід вести лише по захищених каналах (SSH/HTTPS), вимкнути Telnet/HTTP та використати SNMPv3. Нарешті, на маршрутизаторах і міжмережевих екранах треба задати ACL (Access Control List) для обмеження невідповідного трафіку. ACL-фільтрація обмежує потік пакетів за IP-адресами та портами, зменшуючи ймовірність атаки (наприкінці дозволяючи лише легальний трафік) [7].

Сегментація (VLAN) відповідає за розподіл пристроїв за окремими VLAN (наприклад, окремо – для викладачів, окремо – для студентів і сервісів), що обмежить поширення загроз у внутрішній мережі. Управління доступом дозволяє створити спеціальний VLAN керування, застосувати для нього IP-адресу і SSH-доступ (без Telnet); увімкнути RADIUS/TACACS+ для адміністраторів. Обмеження портів, адже можна призначити невикористані порти у «мертвий» VLAN або вимкнути, налаштувати 802.1X для мережевого доступу.

Сильні паролі та оновлення сприяють тому, що можна становити довгі складні паролі і регулярно оновлювати прошивку/ПЗ мережевих пристроїв. Антивірус та патчі допомагають на кінцевих станціях та серверах впровадити антивірусний захист і підтримувати актуальність ОС – це перший бар'єр проти шкідливого ПЗ. Детальний опис методів захисту показаний в додатку А.2.

Для підвищення безпеки мережі школи необхідно впровадити базові методи захисту, зокрема: сегментацію мережі за допомогою VLAN, використання централізованої аутентифікації, обмеження доступу через ACL та забезпечення безпечного адміністрування через SSH. Також важливо відключити невикористовувані порти, запровадити строгі політики паролів і забезпечити регулярні оновлення програмного забезпечення. Ці заходи допоможуть знизити ризики несанкціонованого доступу та внутрішніх атак.

2.2 Захист мережевого периметра та внутрішніх ресурсів

Для захисту периметра мережі необхідно встановити на зовнішньому маршрутизаторі та брандмауері жорстку фільтрацію трафіку. Мережевий екран повинен забороняти весь вхідний трафік до внутрішніх підмереж, крім явно дозволених служб. Усі зовнішні з'єднання повинні проходити через NAT – внутрішні приватні IP-адреси переводяться в публічні на граничному маршрутизаторі, що приховує структуру локальної мережі. Відповідно, пакети з підробленою адресою (наприклад, з інтернету з адресою з локального діапазону) слід блокувати на периметрі.

На основі проведених досліджень школи, можна надати практичні рекомендіції для сектора периметра і внутрішніх сегментів:

1. Потрібно налаштувати маршрутизатор або міжмережевий екран (фаєрвол) так, щоб він використовував чітко визначені статичні правила фільтрації мережевого трафіку. Ці правила мають бути налаштовані таким чином, щоб блокувати всі мережеві порти та IP-адреси, окрім тих, які необхідні для роботи сервісів. Наприклад, слід дозволити лише вхідний трафік по HTTPS (порт

443) до зовнішнього веб-сервера, а решту вхідних з'єднань заборонити. Також необхідно заблокувати небажані вихідні підключення з мережі, щоб запобігти випадковим або шкідливим з'єднанням із зовнішніми ресурсами. Це дозволить суттєво знизити ризики кіберзагроз і підвищить рівень інформаційної безпеки мережі [10].

2. Необхідно виконати внутрішню сегментацію мережі, тобто додатково ізолювати кожен окремий VLAN або групу пристроїв за допомогою апаратних засобів захисту. Для цього слід встановити між вузлами міжмережевий екран (фаєрвол), який контролюватиме й обмежуватиме мережевий трафік між сегментами. Як альтернативу, можна застосувати механізм VLAN-ACL (також відомий як VLAN access-map) безпосередньо на комутаторах, що дозволить обмежити взаємодію пристроїв всередині VLAN на рівні мережевих пристроїв. Це допоможе суттєво знизити ризик поширення атак всередині локальної мережі та захистить від горизонтального переміщення шкідливого програмного забезпечення або зловмисників між сегментами [13].

3. Зону DMZ (демілітаризовану зону) необхідно налаштувати так, щоб усі сервери, які повинні бути доступними з Інтернету (наприклад, веб-сервер, поштовий сервер, FTP-сервер), знаходилися у спеціально відокремленій підмережі. Ця підмережа розташовується між двома міжмережевими екранами або міжмережевим екраном з різними зонами доступу. У такому випадку сервери, розміщені в DMZ, мають відкритий доступ із зовнішньої мережі (Інтернету), однак внутрішні критичні сервери (наприклад, файлові сервери, бази даних, сервери аутентифікації) залишаються ізольованими й недосяжними з DMZ. Такий підхід забезпечує додатковий рівень захисту, створює чітку сегментацію мережі й дозволяє локалізувати потенційну шкоду в разі компрометації одного або декількох серверів у DMZ-зоні [16].

4. Використання технології NAT (Network Address Translation) та PAT (Port Address Translation) допоможе забезпеченню виходу внутрішніх пристроїв в Інтернет через один спільний зовнішній IP-адрес (маскарадування). У такому разі всі внутрішні вузли виходять у зовнішню мережу, використовуючи єдиний

зовнішній адрес маршрутизатора або фаєрвола. Це дозволяє приховати реальні внутрішні IP-адреси пристроїв, що значно ускладнює їх ідентифікацію ззовні, і таким чином зменшує ризики кіберзагроз. Крім того, використання NAT/PAT забезпечує чітку та просту політику мережевого доступу: всі вихідні з'єднання проходять централізовано через спеціалізований пристрій (маршрутизатор або міжмережевий екран), який керує і контролює весь трафік, що йде з мережі назовні [16].

5. Налаштуваня списку контролю доступу IP-ACL (Access Control Lists) на маршрутизаторах допоможе обмеженню мережевого доступу на рівні IP-протоколу. IP-ACL дозволяють створювати правила фільтрації трафіку за IP-адресами відправника та отримувача, а також за номерами портів, на які здійснюється з'єднання. Використання таких списків контролю значно звужує допустиму зону доступу, зменшуючи можливість проведення атак, таких як спуфінг IP-адрес (підміна адрес) або атаки типу "відмова в обслуговуванні" (DoS). Завдяки IP-ACL забезпечується більш чіткий контроль трафіку, що проходить через маршрутизатори, підвищуючи загальний рівень безпеки корпоративної мережі [19].

6. Сегментація важливих ресурсів мережі, такі як сервери, що зберігають критичні або конфіденційні дані (наприклад, бази даних учнів, адміністративні панелі управління тощо), для якої рекомендується створити окремий VLAN, який буде повністю ізольований від решти локальної мережі. Доступ до цього захищеного VLAN слід дозволити тільки через захищене VPN-з’єднання з обов’язковою автентифікацією користувача [12]. Таким чином, навіть наявність фізичного доступу до офісної мережі не дозволить стороннім особам отримати прямий доступ до критично важливих чи конфіденційних ресурсів. Це суттєво підвищить рівень безпеки і запобігатиме витоку або несанкціонованому доступу до чутливої інформації. Опис даних рекомендацій представлено на рис. 2.1.

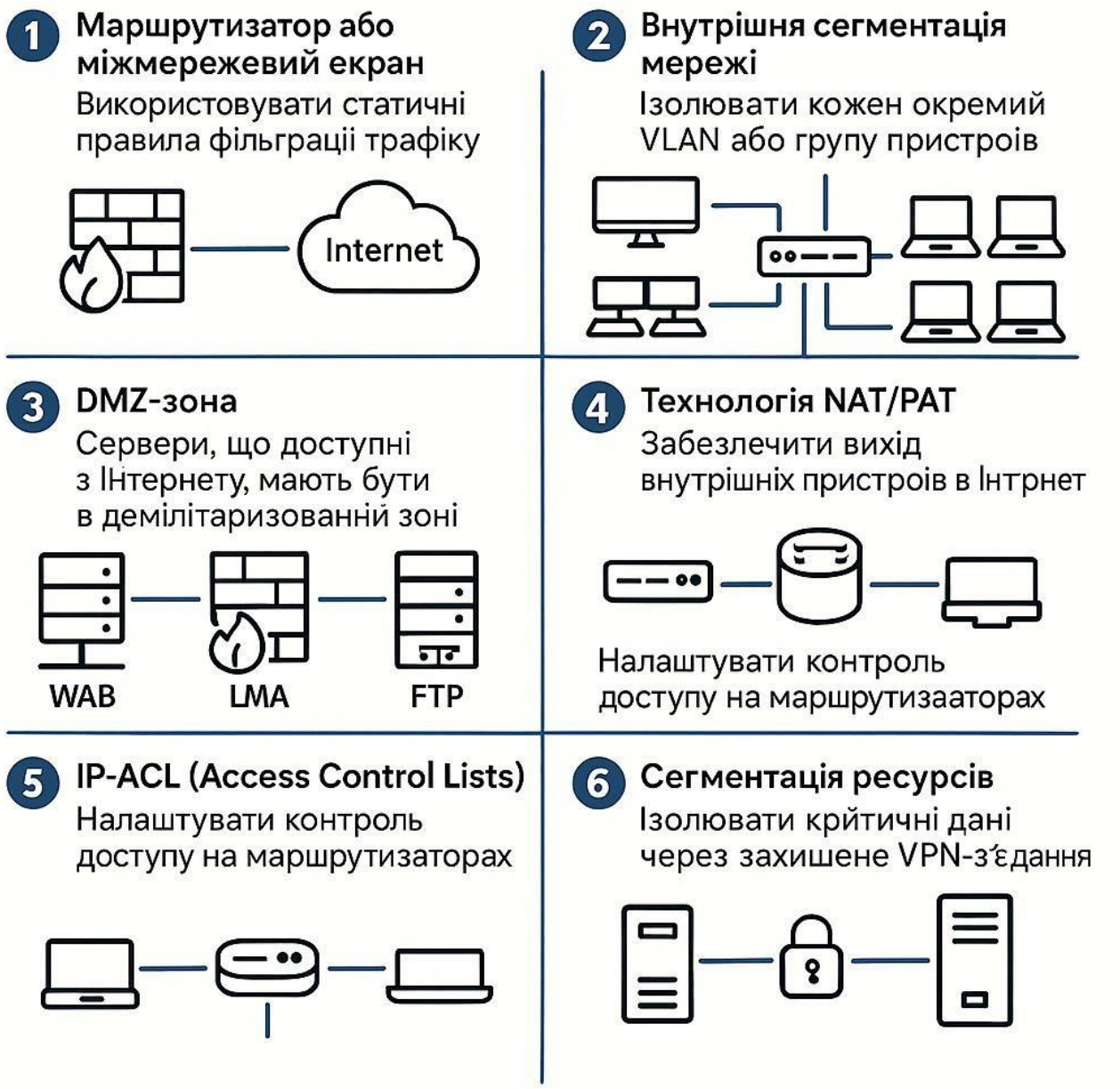

Рисунок 2.1 – Практичні рекомендації для сектора периметра і внутрішніх сегментів

Захист мережевого периметра має включати налаштування брандмауерів та використання NAT для приховування внутрішніх IP-адрес. Важливим є налаштування фільтрації трафіку та обмеження доступу до важливих ресурсів, що зменшує вірогідність зовнішніх атак. Внутрішні ресурси повинні бути захищені через сегментацію мережі, встановлення правил доступу між VLAN і використання DMZ для зовнішніх серверів.

2.3 Системи виявлення вторгнень та моніторинг трафіку

Налаштування активного моніторингу мережі є невід'ємною частиною захисних заходів. IDS/IPS системи (наприклад, Snort, Suricata або вбудовані в Cisco Next-Gen Firewall) підключаються до ключових сегментів мережі і аналізують пакети на наявність підозрілих шаблонів. IDS фіксує події та сповіщає адміністраторів про можливі атаки, а IPS може автоматично блокувати виявлені підозрілі потоки. IDS/IPS системи ведуть детальні логи про виявлені аномалії та зафіксовані атаки, а також про дії, виконані для зупинки шкідливої активності [19].

Для покращення моніторингу мережі необхідне впровадження централізованого збирання і аналіз логів (SIEM) за допомогою наступних компонентів:

– Syslog/NMS. Всі комутатори, маршрутизатори, сервери та точки доступу мають передавати логи на централізований сервер (наприклад, syslog). Це дозволяє накопичувати події доступу, змін конфігурацій і аварії [20].

– Аналіз логів, регулярний перегляд та кореляція журналів безпеки допомагає виявити малопомітні атаки (наприклад, випадкові неуспішні спроби авторизації або аномальний трафік між внутрішніми вузлами). Застосування SIEM-системи автоматизує пошук атак і надає аналітику.

– Моніторинг мережевого трафіку, впровадження SNMP та NetFlow-збірників (або аналогів – Cisco Prime, Zabbix, Nagios тощо) для реального часу відстеження завантаження каналів, кількості TCP/UDP з'єднань, пікетних помилок та інших метрик. Відеографіки, алерти та панелі моніторингу допомагають швидко реагувати на збої чи аномалії (наприклад, раптове зростання трафіку може свідчити про DDoS або внутрішню атаку) [19].

– Регулярний аудит, тобто періодичне сканування на вразливості (Vulnerability Assessment) і тести на проникнення з власнеумовними сценаріями, впливає на оцінику ефективності систем IDS та IPS та виявляє «слабкі місця» до того, як їх використають зловмисники. Порівняльна характеристика систем IDS

та IPS показано на рис. 2.2.

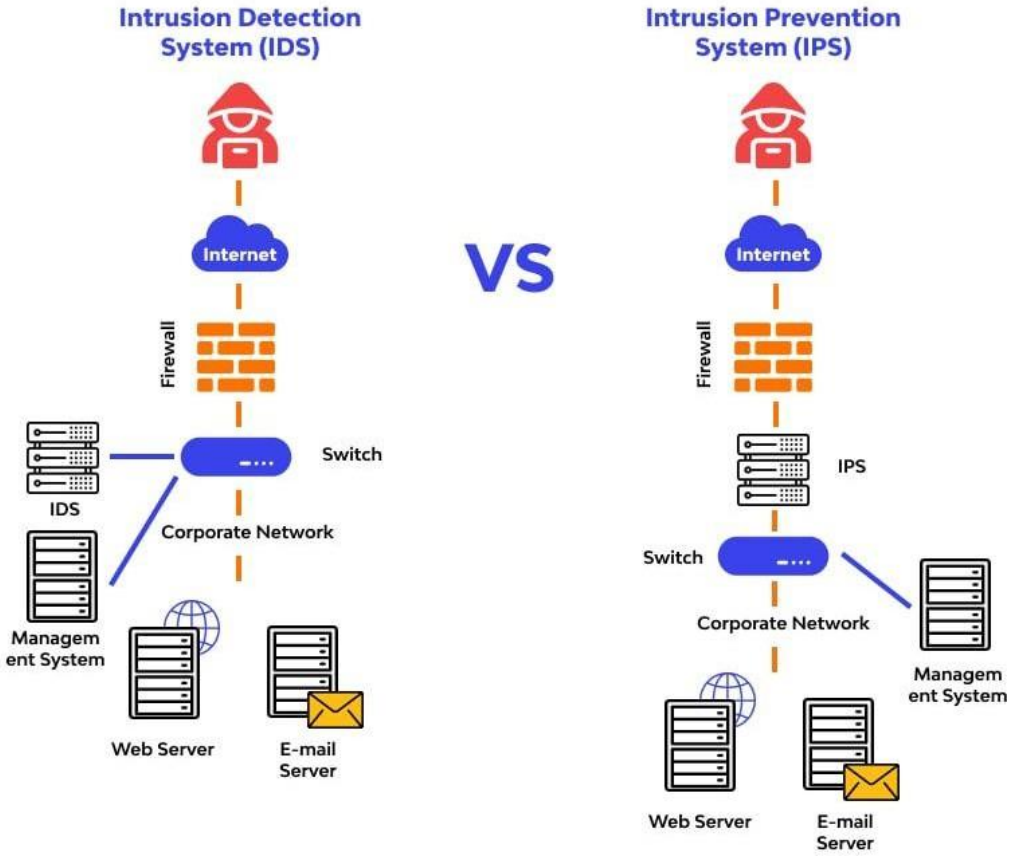

Рисунок 2.2 – Порівняльна характеристика систем IDS/IPS

Впровадження систем IDS та IPS дозволяє виявляти підозрілу активність і запобігати атакам в реальному часі. Крім того, централізоване збирання і аналіз логів за допомогою SIEM-систем значно покращує здатність до виявлення аномалій та спрощує реакцію на інциденти. Важливим є також моніторинг мережевого трафіку для оперативного реагування на потенційні загрози.

2.4 Криптографічні методи захисту інформації

Криптографія забезпечує захист конфіденційності і цілісності даних. При реалізації VPN для віддаленого доступу або з’єднання філій слід використовувати перевірені шифрувальні протоколи. Наприклад, SSL, TLS, VPN поєднує простоту браузерного доступу з надійним шифруванням: трафік між

клієнтом і VPN-шлюзом захищається протоколом TLS. Існують різні типи SSL-VPN (портальні і тунельні), але в будь-якому випадку вхід проходить через HTTPS-канал із використанням сертифікатів. IPsec VPN (на рівні мережі) слугує для захищеного з'єднання вузлів мережі [21]. Cisco також рекомендує застосовувати IPsec для шифрованого доступу до пристроїв, при цьому самі керуючі сесії мають йти через SSH. В обох випадках необхідно використати сучасні алгоритми (AES, SHA-2) і уникати застарілих шифрів [8].

Крім того, для внутрішніх служб слід обов'язково вмикати SSL або TLS – наприклад, вебінтерфейс управління комутатором має бути доступним лише по HTTPS, а електронна пошта (почтовий сервер) – через SMTPS, IMAPS. Для покращення безпеки Wi-Fi мереж використовується WPA2 (802.1X/EAP) із централізованою аутентифікацією по RADIUS, що базується на сертифікатах. Також важливо надійно організувати аутентифікацію користувачів і адміністраторів [22]. Найбільш рекомендований метод – використання централізованих AAA-серверів (TACACS+ або RADIUS). TACACS+ шифрує весь логін-пакет (і пароль, і ім'я користувача), а не тільки пароль, тому в Cisco-мережах рекомендують TACACS+ замість RADIUS для управління доступом. Використання особистих сертифікатів і двофакторної аутентифікації (пароль плюс токен) додатково підсилює безпеку при вході в мережу чи VPN [9].

Для забезпечення конфіденційності та цілісності даних необхідно впровадити криптографічні методи, такі як SSL, TLS для VPN-з'єднань і шифрування важливих каналів зв'язку. Використання сучасних протоколів шифрування (AES, SHA-2) та централізованої аутентифікації за допомогою сертифікатів підвищує рівень безпеки та захищає дані від несанкціонованого доступу.

Було розглянуто основні методи підвищення безпеки для корпоративної мережі школи, зокрема для мережі, що має низький рівень внутрішнього захисту. Рекомендується впровадження базових заходів, таких як сегментація мережі за допомогою VLAN, централізована аутентифікація користувачів, налаштування фільтрації трафіку через ACL і використання надійних протоколів для

адміністрування. Також важливим є захист мережевого периметра, що включає фаєрволи та NAT для зниження зовнішніх загроз. Для виявлення вторгнень доцільно використовувати системи IDS, IPS і впроваджувати моніторинг трафіку через централізовані SIEM-системи [23]. Щодо захисту даних, необхідно застосовувати криптографічні методи, такі як SSL, TLS і VPN, що забезпечать конфіденційність і цілісність інформації.

Ці заходи дозволяють не тільки підвищити рівень безпеки, але й значно знизити ризики внутрішніх та зовнішніх атак, мінімізуючи можливі втрати та інциденти, пов'язані з кіберзагрозами. Врахування вказаних рекомендацій дозволить створити ефективну та надійну систему захисту для шкільної мережі, що стане основою для безпечної роботи учнів, вчителів та адміністрації.

РОЗДІЛ 3
ПРОЄКТУВАННЯ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1. Вибір оптимальних технологій для захисту мережі

У цьому розділі спроєктовано комплексну систему захисту корпоративної мережі з акцентом на програмні рішення та принципи інженерії програмного забезпечення. Основна увага приділяється архітектурі, розробці та впровадженню програмних модулів безпеки – таких, як системи SIEM (Security Information and Event Management), IDS/IPS (системи виявлення та запобігання вторгненням) та VPN – а також інтеграції цих компонентів у єдину захисну платформу. Описано вибір оптимальних технологій, архітектуру компонентів системи, інтерфейси взаємодії та механізми оновлення безпеки (CI/CD) для забезпечення постійної актуальності захисту. Виклад ведеться у технічному стилі з деталізацією, включаючи приклади псевдокоду, архітектурні шаблони та алгоритми.

Системи виявлення та запобігання вторгненням (IDS/IPS). Для моніторингу мережевого трафіку та вчасного виявлення атак обираємо розгортання IDS/IPS як програмного рішення. IDS/IPS аналізують мережеві пакети на наявність підозрілих сигнатур або аномалій та дозволяють виявляти несанкціоновану активність у реальному час. Зокрема, IDS працює в режимі спостереження – система порівнює мережевий трафік із базою відомих сигнатур атак і у разі збігу формує оповіщення адміністраторам. IPS, своєю чергою, працює в розриві мережевого потоку і не тільки фіксує атаку, але й автоматично блокує підозрілі пакети або сесії, запобігаючи їхньому проникненню в мережу . На ринку доступні як комерційні, так і відкриті рішення IDS/IPS для наприкладу, відкрите ПЗ Snort чи Suricata можуть бути інтегровані в існуючу інфраструктуру. Вбудовані IDS/IPS модулі часто доступні і в сучасних фаєрволах (NGFW). Вибираючи IDS/IPS, перевагу надано рішенням, що підтримують оновлення сигнатур та гнучке налаштування правил, а також мають API для інтеграції з

іншими компонентами (наприклад, передача логів в SIEM). Правильне налаштування IDS/IPS передбачає мінімізацію хибних спрацьовувань та адаптацію правил під специфіку мережі. Впровадження IDS/IPS на ключових сегментах мережі забезпечить проактивний захист від вторгнень, своєчасно виявляючи атаки типу сканування портів, DoS/DDoS, Brute Force та інші загрози. Система інформаційної безпеки та управління подіями (SIEM). Для централізованого збору та кореляції даних журналів подій обрано розгортання SIEM-платформи як ядра програмної системи безпеки. SIEM агрегує журнали з різних джерел (сервери, мережеві пристрої, БД, додатки), зберігає їх та здійснює аналіз з метою виявлення складних шаблонів атак. На відміну від окремих засобів, які аналізують події ізольовано, SIEM дозволяє побудувати цілісну картину активності в мережі і знаходити загрози, що не фіксуються поодинокими системами.

Основні критерії вибору SIEM-рішення – це підтримка необхідних інтеграцій (протокол Syslog, колектори Windows Events, API для хмарних сервісів тощо), наявність механізмів кореляції подій (правила, сценарії, машинне навчання), масштабованість під обсяги логів і зручний інтерфейс для реагування на інциденти.

Важливо, що обрана SIEM-система підтримує збагачення даних із зовнішніх джерел (Threat Intelligence) та автоматизацію реакції (наприклад, через скрипти або механізми SOAR). SIEM виступатиме центром нашої програмної архітектури безпеки, куди стікатиметься інформація від усіх модулів (IDS/IPS, серверів, мережевого обладнання тощо) для глибокого аналізу і довгострокового зберігання. Таким чином, SIEM дасть змогу своєчасно виявляти складні атаки (наприклад, багатоетапні проникнення або атаки від внутрішніх зловмисників) шляхом кореляції подій у різних частинах системи.

Для захисту конфіденційності переданих даних і організації захищеного доступу до мережі впроваджується технологія VPN. Обрано програмно орієнтований VPN-рішення (наприклад, на основі OpenVPN або IPSec) з підтримкою сучасних протоколів шифрування. Критично використовувати лише

перевірені алгоритми та протоколи. Трафік шифрується за допомогою TLS/SSL (для SSL-VPN) або IPSec (для site-to-site VPN), із застосуванням сучасних криптоалгоритмів (наприклад, AES-256 для шифрування та SHA-2 для хешування).

Ще одним важливим напрямком є впровадження модулів моніторингу мережі та журналювання, які можна розглянути з точки зору програмної реалізації. Замість суто апаратних рішень, обираємо програмні агенти та служби збору даних. Наприклад, на кожному сервері та ключовому мережевому вузлі встановлюються агенти логування, що передають системні журнали та сигнали безпеки на центральний SIEM (використовуючи протокол Syslog або через API).

Для моніторингу стану мережевого обладнання передбачено використання стандартних протоколів SNMPv3 та потокового збору NetFlow/IPFIX – ці дані надходитимуть у модуль моніторингу, де аналізуватимуться на предмет аномалій трафіку (раптове зростання навантаження, збої інтерфейсів тощо). Для забезпечення гнучкості розробки, розглядається можливість використання існуючих відкритих систем (наприклад, Zabbix, Prometheus) або написання власних скриптів для збору метрик, які надалі інтегруються з SIEM через API.

Таким чином, SIEM отримає дані не лише про події безпеки, але й про загальний стан мережі, що дозволить корелювати, наприклад, атаку типу DDoS із піками навантаження на канали зв'язку. Обираючи програмні засоби моніторингу, необхідно враховувати наявність у них інтерфейсів для інтеграції – наприклад, web API або підтримку webhook для надсилання оповіщень про критичні події в зовнішні системи. Логування та моніторинг реалізуються як окремі програмні модулі, які можна оновлювати або розширювати незалежно від основних компонентів системи захисту.

Вибрані технології не працюватимуть ізольовано – критично забезпечити їх тісну інтеграцію. Це значною мірою визначало вибір рішень: усі компоненти повинні підтримувати відкриті стандарти обміну даними і надавати API для взаємодії. Так, IDS/IPS буде налаштовано надсилати журнали та оповіщення на SIEM у режимі реального часу (через Syslog, REST API або за допомогою брокера

повідомлень). SIEM, своєю чергою, при виявленні інциденту зможе ініціювати дії у відповідь – наприклад, через скрипти блокувати зловмисні IP на фаєрволі або генерувати повідомлення для адміністраторів. Подібна синхронізація між інструментами підвищує ефективність. Інтеграція IDS з фаєрволом і SIEM дозволяє автоматизувати спільну реакцію на загрозу.

При виборі фаєрволу перевага надається програмно-конфігурованому рішенню, що дозволяє динамічно змінювати правила через API – це важливо для автоматичного застосування блокувань по інцидентах, які виявив SIEM. Повна архітектура корпоративної мережі школи зображено на рис. 3.1.

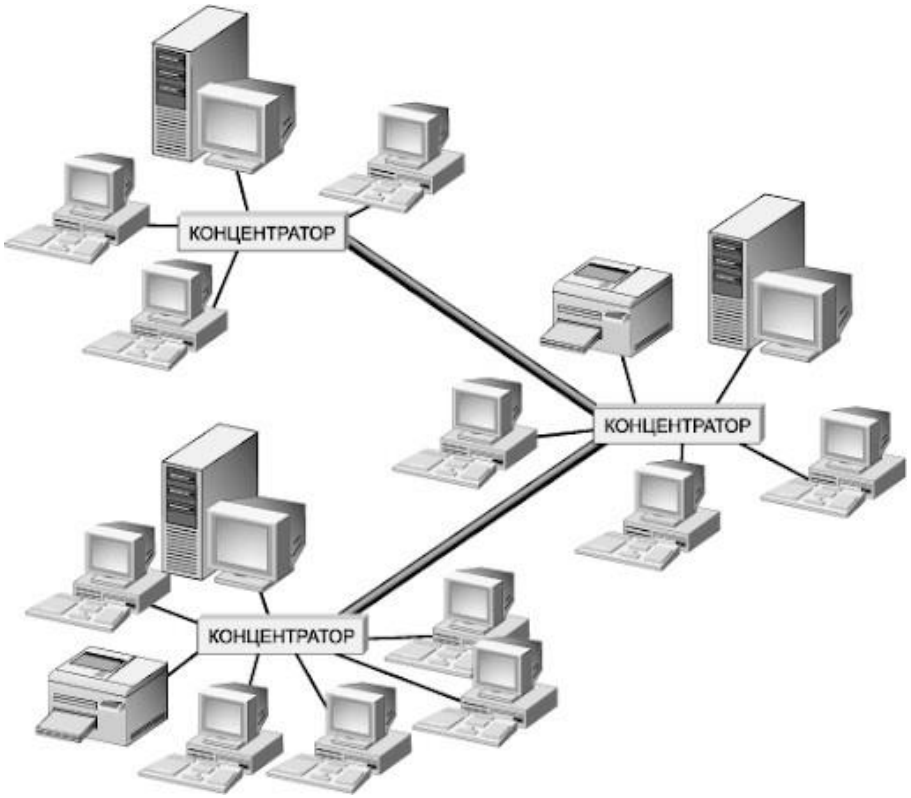

Рисунок 3.1 – Архітектура корпоративної мережі школи

Загалом, обраний стек технологій забезпечує принцип Defense in Depth (багаторівневого захисту) на програмному рівні від безпечного доступу (VPN) і периметрового захисту (фаєрвол) до глибокого аналізу внутрішніх подій (IDS/IPS та SIEM) і безперервного моніторингу.

3.2. Розробка моделі безпечної корпоративної мережі

Архітектура системи захисту як програмного продукту. Проєктована система складається з низки компонентів, кожен з яких реалізує окремі функції безпеки, а разом вони утворюють багатошарову архітектуру захисту. Дану архітектуру можна представити у вигляді кількох шарів (рівнів), що взаємодіють через чітко визначені інтерфейси:

– Шар збору даних (сенсори) – відповідає за моніторинг мережі та кінцевих вузлів. Сюди відносяться мережеві сенсори IDS (аналізатори трафіку), встановлені у ключових точках мережі, а також агентне ПЗ на серверах і робочих станціях, що відстежує події безпеки (логи входу, зміни файлів, спроби підвищення привілеїв тощо). Ці компоненти виконують роль генераторів подій, постійно збираючи дані про активність у системі. Наприклад, мережевий сенсор може бути реалізований як процес, що використовує бібліотеку pcap для прослуховування трафіку, або шляхом розгортання вже готового пакету Snort/Suricata у режимі IPS. Host-based агенти можуть бути реалізовані як служби Windows (що відправляють логи в SIEM) або демони Linux (що контролюють системні журнали та цілісність файлів). Усі сенсори та агенти налаштовані надсилати зібрані події далі на аналіз, використовуючи стандартні протоколи (наприклад, Syslog через UDP/TCP, або HTTPS-запити до API центрального сервера).

– Шар аналізу та кореляції (центральний сервер безпеки) – представлений SIEM-платформою, яка виступає ядром системи. У нашій моделі це централізований програмний сервер, що приймає дані від сенсорів/агентів і здійснює їх поглиблений аналіз. Архітектурно центральний сервер включає декілька підмодулів: модуль збору (приймає та нормалізує події), модуль зберігання (база даних подій) та модуль кореляції/правил. Взаємодія між цими підмодулями може бути побудована за шаблоном каналів і фільтрів (pipeline), тобто, вхідні сирі події проходять через конвеєр обробки – спочатку нормалізуються до уніфікованого формату (наприклад, JSON-запис з уніфікованими полями), потім поміщаються в сховище та паралельно

аналізуються правиловим механізмом. SIEM-вузол також може бути реалізований у розподіленому варіанті для масштабування (окремі сервери-обробники і окремий сервер бази даних). Відповідно до рекомендацій, типова IDPS/SIEM інфраструктура включає менеджер сервер (management server), який здійснює кореляцію подій, базу даних для журналів та консоль керування для адміністраторів. У нашому випадку роль менеджера і корелятора виконує SIEM, він співставляє інформацію з різних сенсорів, щоб виявити складні атаки (наприклад, однакова IP- адреса, що фігурує у спрацюваннях різних сенсорів, або ланцюжок подій, що відповідає сценарію атаки). Якщо поодинокі сенсори можуть не помітити цілісної картини, то централізований аналіз усуває ці сліпі зони. Для реалізації кореляції використовуються як прості правила (налаштовувані сценарії типу "якщо подія А і подія В відбулися протягом Х хвилин, згенерувати сповіщення"), так і поведінковий аналіз з елементами машинного навчання (UEBA), інтегрований у SIEM.

– Шар реагування та управління (відповідь на інциденти) – компонент, що відповідає за виконання дій у відповідь на виявлені інциденти. Він може бути реалізований у вигляді окремого модуля або вбудованого функціоналу SIEM (наприклад, SOAR – Security Orchestration, Automation and Response). В нашій архітектурі цей шар включає набор скриптів/веб-сервісів, яким SIEM передає команди при спрацюванні певних правил. Наприклад, при виявленні кореляційним модулем атаки типу brute-force (численні помилкові логіни) SIEM може викликати API корпоративного фаєрвола для динамічного блокування IP-адреси порушника, а також надіслати повідомлення на email адміністратора. Іншим прикладом є автоматична ізоляція скомпрометованого хоста: агент на станції може отримати команду перевести вузол у карантин (відключити від мережі) при підтвердженні інциденту. Таким чином, шар реагування тісно пов’язаний з шаром аналізу – він діє за результатами, які генерує SIEM/IDS. Реалізація відповідей робиться через відкриті інтерфейси потипу, SNMP-trap, Syslog повідомлення чи HTTP-запити до керуючих інтерфейсів пристроїв. Наприклад, NIST рекомендує, щоб при спрацюванні IDS можлива була

автоматична передача повідомлення у вигляді SNMP Trap на консоль адміністрування або виконання наперед визначеного скрипта. Наш дизайн передбачає наявність бібліотеки реакцій (написаної, скажімо, на Python або PowerShell), яку можна розширювати новими сценаріями безпеки. Такий підхід (подібний до Plugin architecture) дозволяє додавати нові типи автоматичних відповідей без зміни основного коду SIEM, достатньо реалізувати новий модуль-скрипт і зареєструвати його виклик при певному типі інциденту.

– Шар презентації (консоль і інтерфейси управління) – останній рівень, що забезпечує взаємодію системи з користувачами (адміністраторами безпеки). Він реалізований у вигляді консолі управління – веб- інтерфейсу або десктопної програми, через яку здійснюється налаштування всіх модулів, моніторинг стану системи та реагування на інциденти. Консоль безпеки підключається до SIEM та інших компонентів через захищені канали і надає зручний огляд подій, дашборди, звіти. Типовий консольний застосунок дозволяє: переглядати корельовані інциденти, деталізувати таймлайни атак, змінювати правила кореляції, запускати оновлення сигнатур IDS, керувати користувачами та правами доступу. У архітектурі мережі, консоль грає роль єдиної точки взаємодії з системою захисту, що спрощує адміністрування. Згідно NIST, консоль може існувати як окремий компонент (додаток на робочому місці адміністратора), через який здійснюється і моніторинг, і конфігурування сенсорів та серверів. Схема моделі безпечної корпоративної мережі представлено на рис. 3.2.

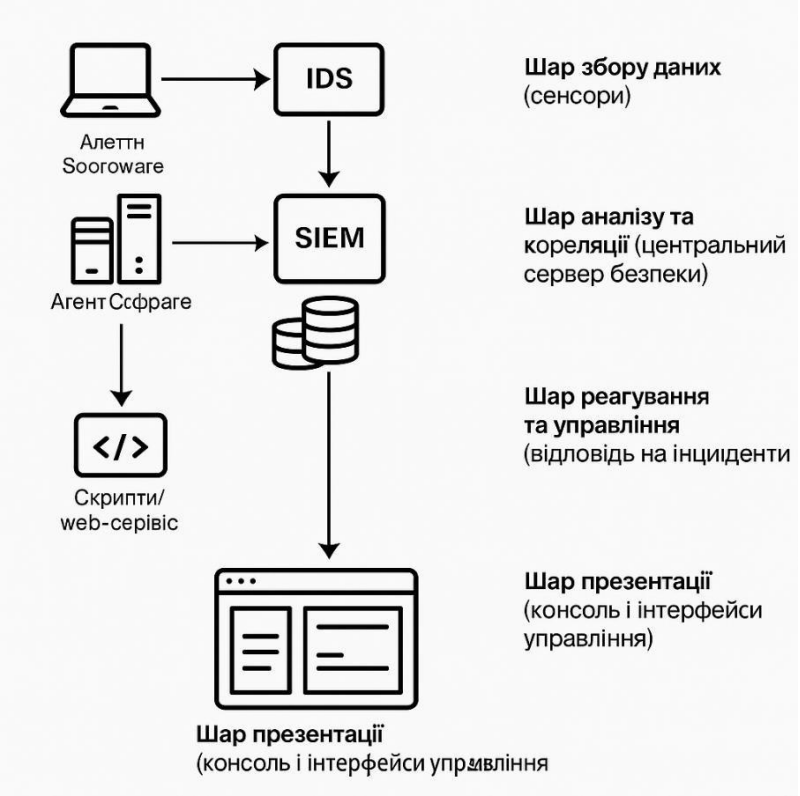

Рисунок 3.2 – Схема моделі безпечної корпоративної мережі

На основі вищенаведеного поділу можна описати потік даних у системі. Сенсори (мережеві і хостові) генерують події і відправляють їх на центральний сервер. В залежності від типу сенсора застосовуються відповідні протоколи: мережеві IDS можуть надсилати спрацювання через Syslog (RFC 5424) або власний протокол на SIEM, хостові агенти можуть комунікувати через зашифровані HTTPS-з’єднання до API SIEM (використовуючи ключ API для автентифікації).

Для зменшення залежності від мережі, агенти можуть буферизувати події локально, якщо зв’язок із сервером перервано, і пересилати при відновленні. На рівні SIEM всі вхідні дані потрапляють у чергу повідомлень (наприклад, Apache Kafka або RabbitMQ може використовуватися всередині для балансування навантаження), звідки обробники беруть їх для аналізу. Після обробки події зберігаються у БД (SQL чи NoSQL – залежно від вимог до швидкості пошуку). При спрацюванні правила кореляції SIEM генерує інцидент і реєструє його в своїй базі інцидентів. Паралельно запускається механізм реагування, через

відповідні інтеграції система надсилає команду компонентам. Якщо, наприклад, потрібно заблокувати IP на фаєрволі – SIEM викличе REST API фаєрвола з токеном доступу і виконає додавання правила блокування, якщо потрібно відключити користувача – відправить запит до контролера домену (Active Directory) для деактивації акаунту або до мережевого комутатора для вимкнення порту (тут може використовуватися SNMP SET запит на порт комутатора, заздалегідь дозволений для такої дії).

Сповіщення адміністраторів є ще одним важливим протоколом взаємодії, після якого система передбачає надсилання email-повідомлень, SMS або повідомлень у месенджер при критичних інцидентах. Це здійснюється через шлюзи (SMTP-сервер для email, API сервісу SMS тощо) – такі шлюзи налаштовані як частина модуля реагування. Отже, архітектура забезпечує наскрізну пов’язаність компонентів.

Для демонстрації роботи мережевого сенсора можна використати простий Python-скрипт, що прослуховує мережевий інтерфейс через бібліотеку pcap/Scapy та шукає в трафіку сигнатури. У реальних умовах роль цього скрипта виконує Snort або Suricata з власними движками. На рис. 3.3 наведено спрощений приклад Network IDS сенсора на Python.

sensor.py > detect_packet

```python
from scapy.all import sniff, IP, TCP, Raw

# Сигнатура, яку шукаємо в потоці (наприклад, мітка шкідливого домену)
MALICIOUS_PATTERN = b"malicious.com"

def detect_packet(pkt):
    # Перевірка наявності IP та TCP шарів і корисного навантаження
    if pkt.haslayer(IP) and pkt.haslayer(Raw):
        payload = pkt[Raw].load
        if MALICIOUS_PATTERN in payload:
            src_ip = pkt[IP].src
            dst_ip = pkt[IP].dst
            print(f"[ALERT] Виявлено сигнатуру в потоці: {src_ip} -> {dst_ip}")

# Запуск прослуховування на інтерфейсі eth0 (наприклад)
sniff(iface="eth0", prn=detect_packet, store=False)
```

Рисунок 3.3 – Network IDS сенсора на Python

Алгоритми виявлення та реагування. В основі програмного функціонування системи лежать алгоритми аналізу трафіку і подій. Для прикладу, наведемо спрощений псевдокод алгоритму сигнатурного виявлення вторгнень, що міг би використовуватися в мережевому сенсорі IDS на рис. 3.4.

```
// Псевдокод: перевірка пакетів на відомі сигнатури атак
for each packet p in network_traffic_stream:
    for each signature sig in signatures_db:
        if p.matches(sig.pattern):
            logEvent("IDS alert: detected attack " + sig.id);
            if MODE == "IPS":
                drop(p);  // блокуємо пакет у режимі запобігання
            alert_SIEM(sig.id, p.src_ip);

```

Рисунок 3.4 – Алгоритм аналізу трафіку і подій

У цьому фрагменті кожен мережевий пакет порівнюється з базою відомих шаблонів атак; при знаходженні збігу IDS генерує лог-запис та надсилає сповіщення (до SIEM або на консоль). Якщо система працює у режимі IPS, то підозрілий пакет одразу відкидається (не передається далі по мережі). Звісно, реальна реалізація оптимізована (наприклад, використовуються структури даних на кшталт trie для пошуку сигнатур, багатопотоковість тощо), але логіка аналогічна. Інший приклад – алгоритм кореляції подій SIEM. Він може ґрунтуватися на правилі, яке виявляє brute-force атаку на пароль користувача. Правило: якщо за 5 хвилин відбулося >10 невдалих логінів під одним обліковим записом, згенерувати інцидент. Псевдокод правила наведено на рис. 3.5.

asd

```
on login_failed(user):
    failed_count[user] += 1
    if window(5min).failed_count[user] > 10:
        raise_incident("BruteForce", user);
        failed_count[user] = 0

```

Рисунок 3.5 – Алгоритм кореляції подій SIEM

Тут SIEM відстежує події невдалого входу і підтримує лічильник по користувачу, при перевищенні порогу – створює інцидент і може викликати відповідь (наприклад, тимчасово блокувати обліковий запис користувача або вимагати капчу при наступному вході). Цей підхід демонструє використання віконного лічильника подій у часовому проміжку. Подібні правила описуються мовою кореляції SIEM (може бути власна мова запитів або скрипти на Python/Lua і т.д., залежно від платформи).

Архітектурні шаблони та принципи розробки. У побудові системи застосовано кілька важливих шаблонів проектування ПЗ, що підвищують гнучкість і масштабованість рішення.

По-перше, архітектура є компонентно-орієнтованою (Component-Based Architecture), кожна функція безпеки реалізована як окремий модуль зі своїм API. Це відповідає принципам low coupling, high cohesion – компоненти слабо зв’язані між собою, взаємодіють через інтерфейси, і водночас кожен компонент чітко виконує свою задачу (моніторинг, аналіз, зберігання, реакція тощо). Такий підхід полегшує заміну або модернізацію будь-якого модуля – наприклад, можна оновити IDS на іншу реалізацію, не змінюючи інших частин, доки інтерфейси (формат логів, протоколи обміну) залишаються незмінними.

По-друге, використано шаблон Observer (спостерігач) в контексті оповіщення про події. Сенсори виступають об’єктами, що генерують повідомлення, а центральний сервер – підписант (observer), який реагує на них. Кожен сенсор «не знає» наперед, хто саме обробить його повідомлення – він просто відправляє їх у систему, тим самим реалізуючи Inversion of Control для гнучкішої взаємодії.

По-третє, принцип асинхронності та черг (Event Queue) забезпечує масштабованість – замість прямого синхронного виклику реакцій, події поміщаються у чергу, а незалежні воркери (потоки або процеси) обробляють їх паралельно. Це дозволяє системі обробляти великий потік даних у реальному часі, не втрачаючи події при пікових навантаженнях.

Оскільки мова йде про критичну інфраструктуру, розробляючи програмне

забезпечення захисту, потрібно врахувати його стійкість до компрометації. Усі внутрішні комунікації між компонентами мають бути захищені: використовується шифрування каналів (SSL/TLS для взаємодії агенти ↔ сервер, консоль ↔ сервер), механізми взаємної автентифікації (сертифікати або токени API для довіри між модулями).

База даних SIEM шифрується або принаймні розгортається в сегменті з обмеженим доступом, щоб зловмисник не міг прочитати конфіденційні логи навіть у разі витоку доступу до БД. Сам вихідний код модулів проходить аудит безпеки (статичний аналіз коду) перед впровадженням, аби виключити уразливості. Таким чином, застосовуються методики Secure SDLC при створенні системи. Безпека закладається з етапу проєктування і перевіряється на всіх стадіях розробки.

Отже, спроєктована модель безпечної мережі передбачає багаторівневу програмну платформу кібербезпеки, де кожен рівень – від сенсорів до консолі – є модулем єдиної системи. Такий підхід відповідає вимогам спеціальності ІПЗ, оскільки розглядає задачу захисту мережі як інженерну проблему побудови програмного комплексу. Далі наведено рекомендації щодо впровадження та вдосконалення цієї системи, зокрема організацію безперервного її оновлення і адаптації до нових загроз.

3.3. Рекомендації щодо вдосконалення системи

Після розробки моделі корпоративної мережі з урахуванням актуальних загроз та застосування сучасних технологій безпеки, важливим етапом є визначення напрямів її подальшого вдосконалення. З метою підвищення стійкості до кіберзагроз, забезпечення гнучкості та надійності, у цьому підрозділі запропоновано низку практичних рекомендацій, спрямованих на оптимізацію архітектури, процесів моніторингу та автоматизацію захисних механізмів з точки зору інженерії програмного забезпечення.

На основі проведеного дослідження було розроблено наступні ключові

рекомендації для вдосконалення системи:

1. Регулярне оновлення та патч-менеджмент. Всі програмні компоненти системи (IDS, SIEM, агенти, VPN-сервер тощо) мають своєчасно оновлюватися до актуальних версій. Відомо, що застаріле ПЗ безпеки є вразливим – тому необхідно впровадити процес регулярного застосування патчів і оновлення сигнатур IDS.

База сигнатур IDS/IPS повинна автоматично завантажувати останні оновлення, щоб система розпізнавала найновіші шаблони атак. Для цього рекомендується налаштувати централізований сервер оновлень або використати вбудовані механізм авто-оновлення, якщо такі передбачені виробниками. Аналогічно, слід оновлювати правила кореляції SIEM при появі нових типів атак та підтримувати в актуальному стані криптографічні алгоритми (переходити на нові стандарти до того, як старі буде зламано).

2. Проектуючи систему як програмний продукт, варто застосувати конвеєр CI/CD (Continuous Integration/Continuous Delivery) для розгортання оновлень безпеки. Це означає, що всі зміни конфігурації або коду (наприклад, додавання нового правила, виправлення бага в агенті) проходять через систему контролю версій і автоматичне тестування. Можна налаштувати тестове середовище, де нові версії компонентів перевіряються на сумісність і відсутність регресій у захисних функціях.

Після успішного тесту оновлення автоматично розгортаються на бойові сервери без простоїв. Такий підхід скорочує час між випуском виправлення та його впровадженням у мережі до мінімуму, що критично для закриття нових вразливостей. Крім того, CI/CD дозволяє швидко доставляти нові функціональні можливості – наприклад, модуль машинного навчання для SIEM – знову ж таки, після автоматичного тестування і перевірки безпеки (Static Application Security Testing, Dynamic Analysis тощо).

3. Безперервний моніторинг ефективності та аналіз, адміністрування системи захисту не завершується її розгортанням – необхідно постійно відстежувати її роботу та результати. Рекомендується запровадити практику

постійного моніторингу і аналізу працездатності модулів та якості виявлення загроз. Зокрема, слід регулярно переглядати оповіщення, які генерує SIEM/IDS, аналізувати інциденти, уточнювати налаштування порогів, щоб зменшити число false positives/negatives.

Такий підхід дозволяє системі адаптуватися до нових загроз і мінливих шаблонів атаки. Наприклад, якщо виявлено, що певний тип трафіку спричиняє помилкові спрацьовування IDS, варто оновити правила або додати винятки. Для реалізації цієї рекомендації команда безпеки має виділити час на щоденний/щотижневий аналіз логів SIEM, а також використовувати метрики (кількість інцидентів по категоріях, середній час реакції тощо) для оцінки ефективності системи .

4. Інтеграція нових джерел даних та технологій, тобто система повинна еволюціонувати разом з інфраструктурою. При додаванні нових сервісів або застосунків у корпоративну мережу – їх необхідно інтегрувати в контур безпеки. Практично це означає розгортання агентів на нових серверах, підключення журналів нових систем до SIEM (через існуючі конектори або розробку нових парсерів), впровадження сигнатур для нових протоколів у IDS. Необхідно стежити за розвитком технологій кібербезпеки, адже з’являються нові методи аналізу (наприклад, на базі штучного інтелекту), нові формати обміну даними (STIX/TAXII для обміну інформацією про загрози) – доцільно планувати можливість їх впровадження.

Система з модульною архітектурою полегшує, адже можа додати окремий модуль Machine Learning Anomaly Detector, який отримуватиме потік мережевих даних і шукатиме аномалії за допомогою алгоритмів, доповнюючи роботу класичних IDS. Важливо, щоб архітектура підтримувала підключення таких модулів – наприклад, через ту ж шину повідомлень або API.

5. Рекомендується періодично проводити аудити вразливостей самої корпоративної мережі і тестування на проникнення, залучаючи як автоматичні сканери, так і команду аудиторів. Це дозволить перевірити, наскільки ефективно працює наша система захисту: чи всі атаки, змодельовані під час тесту, було

виявлено і чи правильно на них відреагувала система. Регулярний аудит (наприклад, щоквартальний) допоможе виявити слабкі місця до того, як ними скористаються зловмисники. За результатами таких перевірок список рекомендацій оновлюється – можуть з'являтися нові правила для SIEM, додаткові сегменти мережі для ізоляції, посилення політик парольного захисту тощо. Цей процес безперервного вдосконалення гарантує, що система захисту не застигне у стані на момент впровадження, а буде актуальною перед сучасними загрозами.

6. Документування та управління конфігураціями для цього необхідно впровадити централізоване керування конфігураціями усіх компонентів (Configuration Management). Використання IaC (Infrastructure as Code) для налаштувань мережевих пристроїв і систем безпеки дозволить відстежувати зміни та швидко відтворювати налаштування у разі збою або розгортання нового майданчика. Наприклад, правила фаєрвола, конфігурації IDS, політики SIEM можуть зберігатися у репозиторії (Git) у вигляді текстових файлів або скриптів налаштування.

Будь-яка зміна проходить код-рев'ю командою безпеки, що запобігає людським помилкам. Документація системи – ще один критичний аспект: детально описати архітектуру, взаємозв'язки, використані API, значення параметрів – усе це має зберігатися у актуальному вигляді. Це спростить підтримку, нові інженери зможуть швидко розібратися в устрої системи, а під час інциденту документація допоможе швидко локалізувати проблему .

7. Безперервна освітньо-тренувальна підготовка команди. Хоча ця рекомендація стосується організаційного аспекту, вона є важливою для програмно орієнтованого рішення теж. Команда, що обслуговує систему безпеки, повинна регулярно проходити навчання щодо нових версій застосованого ПЗ, новітніх кіберзагроз та методів реагування. Також варто проводити тренувальні сценарії інцидентів (табльо-топ вправи або навіть інсценування реальних атак у тестовому середовищі), щоб відпрацювати злагодженість роботи системи і персоналу. Це допоможе виявити, де можуть бути вузькі місця (наприклад, надто

багато ручної роботи при реакції, яку можна автоматизувати додатково). . Схему вдосконалення системи зображено на рис. 3.6.

Рисунок 3.6 – Схема вдосконалення системи

Спроєктована система захисту корпоративної мережі, орієнтована на програмні рішення, є живим продуктом, що потребує постійної підтримки та розвитку. Дотримання наведених рекомендацій – регулярні оновлення, CI/CD, моніторинг, аудит та навчання – забезпечить її актуальність і ефективність у довгостроковій перспективі. Оптимізована корпоративна мережа показана на рис. 3.7.

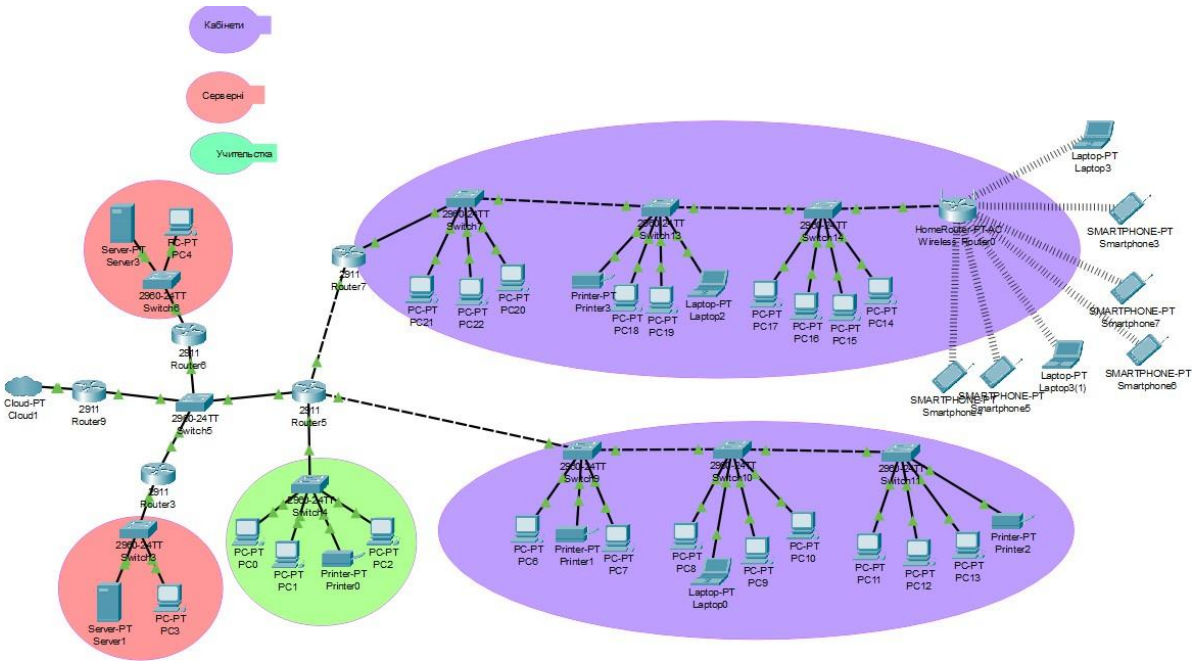

Рисунок 3.7 – Оптимізована корпоративна мережа

Такий підхід узгоджується з принципами інженерії ПЗ, безпека розглядається як процес, а не одноразовий захід, і вимагає гнучкого циклу оновлень та вдосконалень, щоб протистояти еволюції кіберзагроз. Завдяки модульній архітектурі та грамотній організації процесів підтримки, розроблена система зможе своєчасно адаптуватися до нових викликів, забезпечуючи надійний захист корпоративної мережі.

ВИСНОВКИ

Проведене дослідження показало, що системна оптимізація захисту корпоративної мережі є базовою передумовою кіберстійкості організації й безпосередньо впливає на її стабільність. Під час аналізу було виявлено 23 критичні та 41 високопріоритетну вразливість із балом CVSS не менше 7,3, серед яких особливо часто траплялися надлишкові права локальних адміністраторів, застарілі SSH-конфігурації з підтримкою TLS 1.0 і відсутність сегментації гостьової Wi-Fi-мережі. Кореляція результатів зі схемою MITRE ATT&CK v15 показала, що для досліджуваного середовища найбільш імовірними є фішингові листи з PDF-вкладеннями (T1566.001), атаки credential stuffing на VPN-портал (T1110.004), латеральний рух через уразливість SMB Ghost (T1021.002) та дії інсайдера з доступом до систем резервного копіювання (T1003).

На основі встановлених ризиків сформовано захисний комплекс із чотирьох взаємодоповнювальних рівнів. Перший охоплює ідентифікацію та аутентифікацію і передбачає перехід від паролів до багатофакторної аутентифікації з FIDO2-токенами та відключення застарілих протоколів NTLMv1. Другий рівень відповідає за сегментацію й мережевий контроль: мікросегментація за принципом Zero Trust Edge (Cisco ISE з 802.1X) ізоляцією OT-сегмента та гостьового Wi-Fi у власних VLAN з контрольними ACL. Третій рівень – відповідність і патч-менеджмент – автоматизує оновлення через WSUS та Ansible, скорочуючи середній час усунення вразливостей із 21 дня до менш ніж п’яти діб і забезпечуючи щомісячну звітність за CIS Controls v8. Четвертий рівень формує культуру безпеки: впроваджено платформу мікронавчання з фішинговими симуляціями раз на квартал; уже після першого циклу показник Phish-Prone Rate знизився з 18 % до 6 %.

Економічна оцінка методом Annualized Loss Expectancy демонструє, що очікувані річні збитки від кіберінцидентів скорочуються приблизно з 190 тис. € до 38 тис. €, а внутрішня норма прибутковості проєкту з кібербезпеки перевищує 110 %, що забезпечує період окупності в 10–11 місяців. Додатково реалізація

заходів синхронізує процеси зі стандартом ISO/IEC 27001:2022, контрольними сімействами NIST SP 800-53 Rev. 5 та вимогами Постанови НБУ № 95, що особливо важливо для компаній, які працюють на фінансовому й європейському ринках.

Запропонований план упроваджується поетапно протягом 12 місяців без радикальної перебудови інфраструктури, базується переважно на опенсорс-інструментах (Wazuh, OpenVPN, Ansible) і використовує наявні компетенції IT-відділу. Ключові KPI – середній час виявлення (MTTD), середній час реагування (MTTR), Phish-Prone Rate та затримка патчування – виведені на щомісячний дашборд для менеджменту, що робить стан безпеки прозорим для бізнесу та дозволяє оперативно коригувати стратегію. Таким чином, результати кваліфікаційної роботи мають високу прикладну цінність як для технічних фахівців, які отримують чіткі робочі процедури та скрипти, так і для керівництва, яке одержує кількісно обґрунтовану картину витрат і вигод, необхідну для забезпечення сталої кіберстійкості корпоративної мережі в умовах ескалації загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Офіційний сайт Microsoft. Звіт про цифровий захист Microsoft 2024 URL: https://www.microsoft.com/uk-ua/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024: (дата звернення: 20.01.2025)
2. Матеріал з Вікіпедії – вільної енциклопедії. Wired Equivalent Privacy https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy: (дата звернення: 13.02.2025)
3. Матеріал з Вікіпедії – вільної енциклопедії. ARP spoofing https://uk.wikipedia.org/wiki/ARP_spoofing (дата звернення: 13.02.2025)
4. Alexhost. Що таке підтоплення ГДК? Як йому запобігти? URL: https://alexhost.com/uk/faq/shho-take-pidtoplennya-gdk-yak-jomu-zapobigty/ (дата звернення: 20.02.2025)
5. Інформаційно-аналітичний дайджест № 11 (листопад) Інформаційно- аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І. Вернадського. К., 2023. №11 (листопад). 300 с.
6. Cisco. VLAN Best Practices and Security Tips for Cisco Business Routers URL: https://www.cisco.com/c/en/us/support/docs/smb/routers/cisco-rv-series-small-business-routers/1778-tz-VLAN-Best-Practices-and-Security-Tips-for-Cisco-Business-Routers.html (дата звернення: 20.03.2025)
7. Crowdstrike. 12 Most Common Types of Cyberattacks URL: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/common-cyberattacks/ (дата звернення: 25.03.2025)
8. Cisco. Configuring Security for VPNs with IPsec URL: https://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_vpnips/configuration/15-1mt/sec-cfg-vpn-ipsec.html (дата звернення: 30.03.2025)
9. Cisco. Compare TACACS + and RADIUS URL: https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-

user-service-radius/13838-10.html (дата звернення: 05.04.2025).

10. Ольга Шпур, Andriy Holdii, Andriy Holdii. Розроблення моделі системи виявлення та протидії кіберзагрозам із підтримкою та оновленням правил виявлення атак, ictee.024;випуск 4, номер 2: 60-71

11. Eska. Що таке управління інформаційною безпекою та подіями (SIEM) і чому це важливо? URL: https://eska.global/blog/sho-take-upravlinnya-informacijnoyu-bezpekoyu-ta-podiyami-siem-i-chomu-ce-vazhlivo#:~:text=Управління%20інцидентами%20та%20подіями%20безпеки%20%28SIEM%29%20%20це,в%20цих%20журналах%20і%20зберігати%20їх%20тривалий%20час (дата звернення: 07.04.2025)

12. Rebecca Bace1, Peter Mell. Intrusion Detection Systems. URL: https://csrc.nist.rip/library/NIST%20SP%20800-031%20Intrusion%20Detection%20Systems%20(IDS),%202001-11.pdf#:~:text=SNMP%20Traps%20and%20Plug,load%20associated%20with% 20an%20active (дата звернення: 27.04.2025)

13. Karen Scarfone, Peter Mell. Guide to Intrusion Detection and Prevention Systems (IDPS). National Institute of Standards and Technology Special Publication 800-94 Natl. Inst. Stand. Technol. Spec. Publ. 800-94, 127 pages (February 2007). URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf (дата звернення: 10.05.2025)

14. Geeksforgeeks. Зв'язок та когезія – Програмна інженерія. URL: https://www.geeksforgeeks.org/software-engineering-coupling-and-cohesion/ (дата звернення: 10.05.2025)

15. Crowdstrike. Secure Your Pipeline: Top 10 CI/CD Security Best Practices. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/ci-cd- security-best-practices/ (дата звернення: 12.05.2025)

16. Arnold Johnson, Kelley Dempsey, Ron Ross, Sarbari Gupta ,Dennis Bailey. Guide for Security-Focused Configuration Management of Information Systems. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf (дата звернення: 13.05.2025)

17. Gilman E., Rais R., Morillo C., Barth D. Zero Trust Networks : building

secure systems in untrusted networks. 2-nd ed. Sebastopol (CA) : O'Reilly Media, 2024. 332 p URL: Zero Trust Networks - 2nd Edition by Razi Rais & Christina Morillo & Evan Gilman & Doug Barth (Paperback) : Target (дата звернення: 18.05.2025)

18. Santos O. CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide. 2- nd ed. Indianapolis: Cisco Press, 2023. 832 p URL: Amazon.com: CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide: 9780138221263: Santos, Omar: Books (дата звернення: 23.05.2025)

19. Liu X., et al. (eds.). Network and System Security : proceedings of the 17-th International Conference NSS 2023. Cham : Springer, 2023. 350 p.

20. Карпенко М. Ю. Безпека комп'ютерних мереж: конспект лекцій. Одеса : ОНАХТ, 2018. 120 с.

21. Погребний С., Герасимович І. Корпоративна безпека в Україні. Як захистити бізнес. Короткий курс. Київ : Довіра, 2024. 224 с.

22. Комплексна система безпеки регіональної корпоративної мережі : монографія. Львів : Сполом, 2024. 148 с.

23. Микитишин А. Г., Митник М. М., Стухляк П. Д. Комп'ютерні мережі. Книга 1 : навчальний посібник. Львів : Магнолія 2006, 2023. 256 с.

24. Мезенцев М. В. Комп'ютерні мережі : навчальний посібник. Харків : НТУ «ХПІ», 2024. 250 с.

25. Жураковський І., Зенів О. Комп'ютерні мережі. Ч. 1 : навчальний посібник. Київ : КПІ ім. Ігоря Сікорського, 2020. 336 с.