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

КВАЛІФІКАЦІЙНА РОБОТА

на тему

АНАЛІЗ ЗАХИСТУ МЕРЕЖ ТА ЗАСОБІВ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ

Виконав: студент групи 1П-21
Спеціальності
121 Інженерія програмного забезпечення
Костянтин ХОХЛОВ
Керівник:
Майя ЛЮТА

Черкаси 2025

АНОТАЦІЯ

Кваліфікаційна робота «Аналіз захисту мереж та засобів виявлення кіберзагроз» присвячена підвищенню рівня кібербезпеки шляхом дослідження сучасних методів захисту мереж та інструментів виявлення загроз. Особливу увагу приділено аналізу кіберзагроз в інформаційних системах, зокрема, методам їх класифікації, а також технологіям захисту, таким як IDS/IPS, VPN, XDR, AI, та ML.

Метою цієї роботи є аналіз захисту мереж та засобів виявлення кіберзагроз, а також найефективніші підходи до забезпечення інформаційної безпеки.

Технології захисту мереж, включаючи SIEM, NGFW та Zero Trust, мають значний потенціал для підвищення рівня безпеки корпоративних і державних мереж. Основною причиною актуальності теми є зростання складності кібератак, таких як фішинг, DDoS та програми-вимагачі.

Ключові слова: КІБЕРБЕЗПЕКА, МОНІТОРИНГ, АУДИТ, КІБЕРЗАГРОЗИ, СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ, СИСТЕМИ ЗАПОБІГАННЯ ВТОРГНЕННЯМ, МАШИННЕ НАВЧАННЯ, ШТУЧНИЙ ІНТЕЛЕКТ, XDR, SIEM, ZERO TRUST, NGFW.

ABSTRACTS

The qualification work “Analysis of Network Protection and Cyber Threat Detection Tools” is dedicated to improving cybersecurity by studying modern network protection methods and threat detection tools. Particular attention is paid to the analysis of cyber threats in information systems, in particular, methods of their classification, as well as protection technologies such as IDS/IPS, VPN, XDR, AI and ML.

The purpose of this paper is to analyze network security and cyber threat detection tools, as well as the most effective approaches to ensuring information security.

Network security technologies, including SIEM, NGFW, and Zero Trust, have significant potential to improve the security of corporate and government networks. The main reason for the relevance of the topic is the growing complexity of cyberattacks, such as phishing, DDoS, and ransomware.

Keywords: CYBERSECURITY, MONITORING, AUDIT, CYBER THREATS, INTRUSION DETECTION SYSTEMS, INTRUSION PREVENTION SYSTEMS, MACHINE LEARNING, ARTIFICIAL INTELLIGENCE, XDR, SIEM, ZERO TRUST, NGFW.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

IPS – Intrusion prevention system

APT – Advanced Persistent Threat

IDS – Intrusion Detection System

SIEM – Security Information and Event Management

ML – Machine Learning

VPN – Virtual Private Network

PPTP – Point-to-point tunneling protocol

СКУД – система контролю і управління доступом

ETSI – Європейський інститут телекомунікаційних стандартів

NIST – The National Institute of Standards and Technology

HIDS – Host-based Intrusion Detection System

OSSEC – Open Source Host-based Intrusion Detection System

NIDS – Network Intrusion Detection System

AI – Artificial intelligence

SVM – Support Vector Machines

DL – Deep Learning

HEAT – Highly Evasive Adaptive Threats

IoT – Інтернет речей

XDR – Extended Detection and Response

SASE – Secure Access Service Edge

NGFW – Next-Generation Firewal

UTM – Urchin Tracking Module

SOAR – Security Orchestration, Automation and Response

ВСТУП

Актуальність теми визначена постійним зростанням кількості кібератак і складністю їхнього виявлення. Багато компаній та організацій натрапляють на проблеми, які пов’язані з недостатнім захистом їхніх мереж, що зобов’язує впровадження передових засобів моніторингу та аналізу загроз. Розвиток сучасних технологій, зокрема, машинне навчання та штучний інтелект, спроможні значно підвищити рівень автоматизації та точності виявлення кіберзагроз.

Швидкий розвиток інформаційних технологій та їх використання у всіх сферах життя зумовлюють не лише підвищенню можливостей, а й створюють нові виклики у сфері забезпечення безпеки. Одним із найважливіших елементів цього процесу є захист комп'ютерних мереж, які є базою функціонування інформаційних систем, як у приватних підприємствах, так і у державних установах. Інтеграція, оцифрування та зростання кількості підключених пристроїв значно збільшили рівень та кількість кіберзагроз, що можуть призводити до істотних економічних, соціальних та політичних наслідків.

Кіберзагрози є прогресивним явищем, що розвивається разом із розвитком технологій. Вони видозмінюються від простих вірусів і фішингових атак до кібервійн, організованих політичними діячами, державними структурами або хакерськими угрупуваннями. Наслідки таких загроз включають несанкціонований доступ до даних, порушення функцій систем, фінансові збитки та втрату довіри до інформаційних технологій. У зв’язку з цим, необхідність розробки та впровадження ефективних засобів виявлення кіберзагроз і забезпечення надійного захисту мереж стала надзвичайно актуальною.

Об'єктом дослідження є комп'ютерні мережі та інформаційні системи, які потребують захисту від кіберзагроз, а також самі засоби виявлення та протидії цим загрозам.

Предметом дослідження є процеси, технології та інструменти, що забезпечують захист комп'ютерних мереж від несанкціонованого доступу, атак і витоку інформації, а також методи виявлення, ідентифікації та реагування на кіберзагрози.

Дослідження охоплює технічні і організаційні аспекти захисту мережевої інфраструктури, а саме: мережеві протоколи безпеки; системи виявлення та запобігання вторгненням (IDS/IPS); сучасні підходи до моніторингу та аналізу трафіку; методи виявлення шкідливої активності; засоби реагування на інциденти.

Метою цієї роботи є аналіз захисту мереж та засобів виявлення кіберзагроз, а також найефективніших підходів до забезпечення інформаційної безпеки.

Завдання дослідження включають:

– Аналіз сучасних загроз, що впливають на безпеку комп’ютерних мереж.

– Дослідження основних методів та засобів захисту комп’ютерних мереж.

– Розгляд принципів роботи та класифікації систем виявлення кіберзагроз.

– Аналіз ефективності існуючих засобів виявлення вторгнень і атак.

– Розробка рекомендацій для вирішення виявлених загроз.

– Розробка детальних рекомендацій для підвищення ефективності кібербезпеки підприємств та організацій.

– Оцінка можливості інтеграції засобів виявлення загроз та її вплив на кіберзпеку організацій.

Практичне значення даного дослідження полягає у тому, що отримані результати можна застосувати для покращення кібербезпеки в організаціях, а також захисту мережевого середовища за допомогою новітніх технологій.

Рекомендації роботи можуть стати основою для подальших досліджень у сфері кібербезпеки, а також бути корисними для спеціалістів, які займаються розробкою та впровадженням систем захисту інформації.

Апробація роботи. Часткові результати кваліфікаційної роботи були апробовані на XVII Студентській науково-практичній конференції студентів, аспірантів та молодих вчених «Тенденції розвитку ІТ-технологій в Україні» [9].

РОЗДІЛ 1
ОСОБЛИВОСТІ ЗАХИСТУ МЕРЕЖ

1.1 Основи безпеки мереж

Безпека мережі – це галузь кібербезпеки, яка передбачає захист комп'ютерних мереж від кіберзагроз. Система мережевої безпеки надає всі засоби, необхідні підприємствам для запобігання кібератакам і боротьби з ними, зокрема, обладнання, програмне забезпечення, процедури та політики [1].

Основними загрозами безпеки є:

– Шкідливе програмне забезпечення – це будь-яка програма або код, створений з метою завдання шкоди комп'ютеру, мережі або користувачу. Воно може виконувати різні деструктивні дії, такі як викрадення даних, блокування доступу до системи, знищення файлів або шпигунство.

– Шпигунське програмне забезпечення – це програмне забезпечення, яке збирає інформацію про користувача без його відома. Воно може відстежувати, історію відвідування веб-сайтів і збирати конфіденційні дані, такі як паролі та номери кредитних карток.

– Фішингові атаки включають в себе надсилання шахрайських електронних листів або текстових повідомлень для отримання конфіденційної інформації від одержувачів. Повідомлення можуть виглядати так, ніби вони надіслані з довіреного джерела, але насправді їх відправляють шахраї.

– Програми-вимагачі – це зловмисні програмні забезпечення, які блокують користувачам доступ до їхніх комп'ютерів або мобільних пристроїв, доки не буде здійснено викуп. Видалити такі програми може бути складно, адже вони можуть пошкодити або видалити файли в системі користувача.

– DDoS-атаки – є одним із найнебезпечніших видів загроз. Це тип кібератаки, під час якої кілька систем переповнюють ціль трафіком, роблячи її недоступною для інших користувачів.

До основних компонентів забезпечення безпеки мережі належать:

– Брандмауер – бар’єр або фільтр між певною мережею та зовнішнім світом або Інтернетом загалом. Він відповідає за перевірку інформації, яка надходить або виходить з мережі, і відстеження цієї інформації.

– Контроль доступу – механізм обмеження та регулювання прав користувачів або систем на доступ до ресурсів, даних чи об'єктів. Він забезпечує безпеку інформації, дозволяючи лише авторизованим користувачам виконувати певні дії, такі як читання, запис, змінення або видалення даних.

– Сегментація мережі – процес розділення локальної мережі на декілька незалежних сегментів з метою збільшення загальної швидкості обміну даними.

– Intrusion prevention system (IPS). Програмна або апаратна система мережевої та комп'ютерної безпеки, яка виявляє вторгнення або порушення безпеки і автоматично захищає від них.

– Навчання співробітників. Одним із найефективніших заходів захисту мережі, які можуть вжити організації, є забезпечення того, щоб усі, хто має доступ до мережі організації, були навчені не загрожувати безпеці мережі [1].

Мережева безпека є критичним компонентом кібербезпеки і першою лінією захисту мережі від кібератак. Без належних заходів безпеки мережі залишаються вразливими до кіберзагроз, зокрема, несанкціонованого доступу та DDoS-атак. Завдяки впровадженню різних заходів мережевої безпеки організації можуть ефективно запобігати, виявляти та протидіяти цим загрозам.

Хоча мережева безпека в основному стосується підприємств із великими та складними комп’ютерними мережами, багато її інструментів і методів також можуть бути використані для захисту домашньої мережі.

Системи мережевої безпеки застосовують низку захисних заходів, щоб захистити від несанкціонованого доступу, викраденню конфіденційних даних і завданню фінансових, операційних або репутаційних збитків. Ці заходи

зазвичай призначені для використання спеціалізованого обладнання та програмного забезпечення.

Відділення безпеки вирішують, які стратегії, політики та процедури компанія буде впроваджувати для гарантії безпеки мережі. Впровадження різних стратегій також допомагає бізнес-мережам дотримуватися стандартів і правил безпеки. Після встановлення правил мережевої безпеки всі користувачі мережі повинні виконувати їх, щоб гарантувати належний захист.

1.2 Класифікація кіберзагроз

Поняття кіберзагроза стосується можливих небезпек, пов’язаних із застосуванням інформаційних технологій, мереж, програмного забезпечення та пристроїв, які можуть бути спрямовані на викрадення, модифікацію або знищення даних, а також на порушення нормальної роботи систем. Для ефективного захисту інформаційних систем важливо розуміти їхню природу, тому кіберзагрози класифікують за такими основними ознаками:

а джерелом виникнення:

– Зовнішні (джерела загроз знаходяться поза системою);

– Внутрішні (джерела загроз розташовуються всередині системи).

а характером впливу:

– Навмисні – дії, що виконуються згідно планів зловмисників, які спрямовані на порушення конфіденційності, незаконного доступу до інформації.

– Випадкові – виникають через ненавмисні дії співробітників, клієнтів, компаній. Також через збої в програмному забезпеченні чи апаратних засобах. Такі дії можуть призвести до: втрати конфіденційності, пошкодження інформаційної бази, некоректної роботи системи, відмови або несправності обладнання, тощо.

а способом реалізації:

– Мережеві атаки – атаки на розподілену обчислювальну систему, що здійснюються з метою отримання контролю. Як правило, метою мережевої атаки є порушення конфіденційності даних.

– Програмні загрози (віруси, хробаки, програми-вимагачі, кейлогери), пов'язані з небезпечним програмним забезпеченням, що має на меті порушення конфіденційності, цілісності або доступності даних, систем або мереж.

– Фізичний вплив – пошкодження фізичних носіїв інформації, пошкодження комп’ютерних систем, крадіжка обладнання, несанкціонований доступ до серверної сторонньою особою.

– Соціальна інженерія – спосіб маніпулювання людьми спеціальними методами впливу з метою отримання персональних даних для зловмисника.

а об’єктом впливу:

– Дані – за допомогою впливу на них таких загроз як несанкціонований доступ, навмисне або ненавмисне їх видалення, викрадення, порушення конфіденційності, шифрування з метою викупу (ransomware).

– Інформаційна система – сторонній вплив на працездатність програмного забезпечення, злом системи керування, порушення логіки роботи

– Мережева інфраструктура – атаки спрямовані на порушення роботи мережевих компонентів (маршрутизаторів, серверів, точок доступу, комутаторів тощо.).

а тривалістю впливу:

– Короткострокові – мають швидкий вплив, але обмежені у часі. Це можуть бути спроби фішингу або зараження шкідливим програмним забезпеченням, яке легко видаляється.

– Довготривалі – загрози тривалої дії, іноді непомітної для жертви. До них можна віднести шнигунське програмне забезпечення.

а рівнем організованості:

– Індивідуальні – здійснюються окремими особами, часто з використанням публічно доступних інструментів.

– Організовані – проводяться різними групами або організаціями. Ці загрози мають складну структуру, чітке планування, фінансування та цілі такі як шпигунство, саботаж, фінансове вимагання.

Також існує класифікація за цільовою аудиторією атак. Персональні загрози орієнтовані на окремих користувачів і часто пов’язані з крадіжкою особистих даних або фінансовими шахрайствами. Корпоративні загрози, у свою чергу, спрямовані на підприємства та організації, які зберігають важливу комерційну інформацію. Крім того, існує безліч загроз, які можуть впливати на національну безпеку.

Класифікацію також можна проводити за складністю атак. До одноразових атак належать швидкі та короткочасні дії, які можуть бути спрямовані, наприклад, на перевантаження сервера. Більш складними є атаки типу Advanced Persistent Threat (APT), які відзначаються тривалістю та високою організованістю. Вони можуть тривати місяцями й навіть роками, залишаючись непоміченими протягом тривалого часу, що дозволяє кібершпигунам систематично отримувати доступ до конфіденційної інформації.

1.3 Методи захисту мереж

Сучасні методи захисту мереж включають застосування систем виявлення та запобігання вторгненням, моніторинг та аудит інформаційних систем, використання віртуальних приватних мереж для захищених з'єднань, криптографічні технології для шифрування даних, а також управління доступом, що ґрунтуються на затверджених політиках безпеки.

До основних методів захисту мереж відносять:

або система виявлення вторгнень, яка зазвичай пов'язана з програмним забезпеченням або пристроєм, який відповідає за моніторинг онлайн-загроз, незалежно від того, чи знаходиться він в системі або мережі. Інформація про дивну активність зазвичай повідомляється адміністратору або збирається через систему Security Information and Event Management (SIEM).

Методи функціонування IDS:

– Виявлення аномалій. IDS може функціонувати для моніторингу комп'ютера, а також мережевої активності і після цього розділяти активність на нормальну або аномальну. Цей тип систем спочатку був розроблений для виявлення дивної активності. Підхід в основному заснований на використанні машинного навчання, за допомогою якого запам'ятовуються правильні моделі активності і порівнюються з новими/дивними. Цей підхід набагато кращий завдяки своїм узагальненим властивостям, але у вас можуть виникнути деякі проблеми з помилковими спрацьовуваннями.

– IDS на основі підпису. Цей напрям вважається більш традиційним і базується на пошуку певних шаблонів. У цьому методі шаблони означають те ж саме, що і підписи. Саме це допомагає в боротьбі з відомими кібератаками, але матиме певні проблеми з новими шаблонами.

– Виявлення на основі репутації. Оцінка репутації впливає на весь процес.

PS або система запобігання вторгненням функціонує шляхом виявлення загрозливої активності, повідомлення про таку активність і спроб запобігти таким загрозам. Як правило, IPS знаходиться відразу за брандмауером. Цей тип систем надзвичайно корисний для виявлення проблем, пов'язаних зі стратегіями безпеки, виявлення кіберзлочинців та ідентифікації загроз документам. Запобігання загрозливій активності відбувається в IPS шляхом модифікації змісту атаки, реконфігурації брандмауерів або іншими методами. Деякі користувачі сприймають IPS як розширення IDS, головним чином тому, що вони відповідають за моніторинг мережі.

Методи функціонування IPS:

– Моніторинг аналізу протоколів з урахуванням стану. Цей метод IPS функціонує шляхом порівняння всієї активності з узагальненими правилами, і таким чином виявляються відхилення.

– Моніторинг на основі підпису. Процес в методі IPS виявляє пакети в мережі, після чого стандартні шаблони (сигнатури) порівнюються з пакетами.

– Моніторинг на основі статистичних даних. Підхід функціонує шляхом перевірки мережевої активності, а порівняння проводиться на основі заздалегідь визначеної базової лінії. Ця лінія визначає основні характеристики, які вважаються нормальними, такі як використання певних протоколів або використовувана пропускна здатність. Якщо є певні проблеми з базовою конфігурацією, результат може бути хибнопозитивним.

– це технологія, яка створює безпечне з'єднання поверх менш захищеної мережі, такої як Інтернет. Вона дозволяє користувачам безпечно передавати дані, приховуючи свою IP-адресу та шифруючи інтернет-трафік, що забезпечує конфіденційність і захист особистої інформації. VPN також надає можливість обходити географічні обмеження, надаючи доступ до контенту, який може бути недоступним у певному регіоні. Це досягається шляхом підключення до серверів, розташованих в інших країнах, що дозволяє змінити віртуальне місцезнаходження користувача. Використання VPN є важливим для забезпечення безпеки в Інтернеті, особливо при підключенні через загальнодоступні Wi-Fi мережі, оскільки воно захищає дані від потенційних загроз і несанкціонованого доступу.

Сучасні види VPN підключення:

Point-to-point tunneling protocol (PPTP) – це тунельний протокол типу «точка-точка», який дозволяє комп'ютеру користувача встановлювати захищене з'єднання з сервером за рахунок створення спеціального тунелю в стандартній, незахищеною мережі. PPTP став відомий, тому що, це перший VPN протокол, який підтримала корпорація Microsoft. Всі версії Windows,

починаючи з Windows 95 OSR2, вже включають в свій склад PPTP-клієнт. Це найвідоміший і простий в налаштуванні варіант підключення до VPN-сервісу.

OpenVPN – це вільна реалізація технології VPN з відкритим вихідним кодом для створення зашифрованих каналів виду «точка-точка» або «сервер-клієнти» між комп'ютерами. Вона може встановлювати з'єднання між комп'ютерами, які знаходяться за NAT-firewall без необхідності зміни його налаштувань. Використання, цієї технології – вимагатиме від користувача встановлення додаткового програмного забезпечення для всіх операційних систем.

L2TP (Layer 2 Tunneling Protocol) – це мережевий протокол тунелювання канального рівня, що поєднує в собі протокол L2F (layer 2 Forwarding), розроблений компанією Cisco, і протокол корпорації Microsoft. Дозволяє створювати VPN із заданими пріоритетами доступу, однак не містить в собі засобів шифрування і механізмів аутентифікації (для створення захищеної VPN його використовують спільно з IPSec). За відгуками експертів, є найбільш захищеним варіантом VPN підключення, незважаючи на труднощі його налаштування.

риптографічні методи захисту інформації – це спеціальні методи шифрування, кодування або іншого перетворення інформації, в результаті якого її зміст стає недоступним без пред'явлення ключа криптограми і зворотного перетворення. Криптографічний метод захисту найнадійніший метод захисту, так як охороняється безпосередньо сама інформація, а не доступ до неї (наприклад, зашифрований файл не можна прочитати навіть у випадку крадіжки носія). Даний метод захисту реалізується у вигляді програм або пакетів програм.

Криптографічний алгоритм, названий алгоритмом шифрування, представлений деякими математичними функціями, одна використовується для шифрування, а інша – для розшифровки.

Розрізняється шифрування двох типів:

– симетричне (із секретним ключем);

– несиметричне (з відкритим і закритим ключем).

При симетричному шифруванні створюється ключ, файл разом з цим ключем пропускається через програму шифрування та отриманий результат пересилається адресатові, а сам ключ передається адресатові окремо, використовуючи більш захищений або дуже надійний канал зв'язку.

Несиметричне шифрування складніше, але і надійніше. Для його реалізації потрібні два взаємозалежних ключі: відкритий і закритий.

5. Обмеження доступу до інформації здійснюється відповідно до розділу II статті 6 Закону України Про доступ до публічної інформації [5].
ахист від витоку інформації технічними каналами забезпечують проектно-архітектурними рішеннями, проведенням організаційних і технічних заходів, а також виявленням портативних закладних пристроїв.

Організаційні заходи спрямовані на захист інформації заходи, проведення яких не потребує спеціально розроблених технічних засобів.

Технічні заходи – це апаратні та програмні засоби, які створенні для забезпечення безпеки інформаційних систем. Це можуть бути брандмауери, маршрутизатори, антивірусні системи, системи моніторингу, тощо.

7. Управління доступом – це основний елемент кібербезпеки, який дає змогу визначати, хто може отримувати доступ до певних даних, програм і ресурсів, а також за яких умов. Політики керування доступом забезпечують захист цифрового середовища. Іншими словами, вони забезпечують доступ відповідним користувачам, а всім іншим забороняють його.

Політики керування доступом в основному ґрунтуються на таких методах, як автентифікація й авторизація, що дають організаціям змогу перевіряти правдивість даних користувачів і їхнє право на доступ до певних ресурсів на основі пристроїв, розташування, ролей тощо.

Завдяки управлінню доступом зловмисники й інші неавторизовані користувачі не можуть викрасти делікатну інформацію, зокрема клієнтські дані або інтелектуальну власність. Це рішення також забезпечує захист від веб-загроз.

В управлінні доступом важливу роль також грає система контролю і управління доступом (СКУД) – сукупність програмних і апаратних засобів, які забезпечують захист об'єкта від несанкціонованого проникнення, які також формують реєстрацію входу-виходу людей або транспорту через задані «точки», наприклад: двері , ворота, турнікети, шлагбауми та інші.

СКУД має важливе значення в комплексній системі охорони підприємства, забезпечує збереження майна споруд і працівників.

Зазвичай система контролю і управління доступом складається з цілого ряду компонентів, починаючи з тих, які ідентифікують співробітника, і закінчуючи тими, що приймають рішення про надання доступу.

8. Аудит мережі – це дослідження поточного стану, конфігурації, працездатності і відмовостійкості корпоративної мережі.

Компоненти аудиту:

себічний аналіз корпоративної мережі та її компонентів (lan, wlan, wan, телефонія, безпека, управління і моніторинг);

иявлення «вузьких» місць, які роблять мережеву інфраструктуру вразливою і небезпечною з точки зору конфіденційності корпоративних даних;

цінка функціональності мережевих сервісів і їх відповідності конкретним вимогам бізнесу;

озробка рекомендацій по модернізації вже існуючих елементів мережевої інфраструктури або заміні на більш сучасні рішення, оптимізації і захисту.

Аудит мережі дозволяє виявити:

ожливі точки несанкціонованого проникнення;

ерелік сервісів і обладнання, що є вразливими для атак;

жерела вірусної активності всередині мережі;

ади організації мережевої інфраструктури, які знижують її надійність;

ричини низької якості роботи мережі або її низької продуктивності;

евідповідність мережі наявній документації.

Коли необхідний аудит мережі:

ідзначаються проблеми в роботі мережі, передачі сигналу або збої при наданні сервісів;

отрібна оцінка якості послуг, що надаються інтернет-провайдером;

еред початком робіт з модернізації мережі і після завершення, для оцінки результатів;

ри передачі мережевої інфраструктури на аутсорсинг.

9. Моніторинг мережі – це критично важливий IT-процес, при якому всі мережеві компоненти, такі як маршрутизатори, комутатори, брандмауери, сервери та віртуальні машини, відстежуються на предмет збоїв та продуктивності та постійно оцінюються для підтримки та оптимізації їх доступності.

Ключові аспекти моніторингу мережі:

– Відстеження в реальному часі – інструменти моніторингу мережі безперервно аналізують потік даних у мережі, надаючи інформацію в реальному часі про продуктивність пристроїв і загальної мережі. Ці інструменти фіксують і аналізують мережевий трафік, відстежуючи такі фактори, як використання пропускної здатності, затримка, втрата пакетів і час відповіді.

– Виявлення аномалій є важливим компонентом моніторингу мережі. Інструменти моніторингу встановлюють базову поведінку мережі, аналізуючи історичні дані та мережеві шаблони. Порівнюючи поточну активність мережі з цією базою, інструменти можуть виявляти незвичайні шаблони або дії, які відрізняються від нормальних. Ці аномалії можуть вказувати на потенційне порушення безпеки, технічну проблему або ненормальну поведінку мережі. Можливість вчасно виявляти й реагувати на такі аномалії підвищує безпеку мережі та допомагає підтримувати стабільне мережеве середовище.

– Сповіщення та звітування – виявлення аномалій або потенційних проблем (системи моніторингу мережі генерують сповіщення та детальні звіти). Ці сповіщення інформують адміністраторів про будь-які неправильності в продуктивності мережі, безпекових подіях або потенційних загрозах.

– Моніторинг безпеки мережі включає нагляд за мережевим трафіком для виявлення та пом'якшення потенційних загроз безпеці. Це включає моніторинг на предмет спроб несанкціонованого доступу, ненормальних передач даних або інших підозрілих дій, які можуть загрожувати безпеці мережі. Завдяки безперервному моніторингу мережевого трафіку адміністратори можуть оперативно виявляти порушення безпеки, аналізувати їх вплив і вживати необхідних заходів для обмеження та запобігання подальшої шкоди.

1.4 Огляд міжнародних стандартів у сфері кібербезпеки

Міжнародні стандарти з кібербезпеки – це документи з набором вимог, що стосуються безпеки інформаційних систем і даних. Вони потрібні для того, щоб допомогти організаціям забезпечувати захист корпоративної інформації, а також дотримуватися законодавчих норм.

Обов’язковим є Payment Card Industry Data Security Standard (PCI DSS) для всіх організацій, які мають справу з обробленням платежів, в усіх країнах світу.

В Україні використовують General Data Protection Regulation (GDPR) Європейського Союзу, який регулює захист персональних даних на території країн-учасниць. Він є обов’язковим для компаній, які мають справу з персональними даними громадян і резидентів ЄС, незалежно від розташування цих компаній. А отже, GDPR обов’язковий і для українських компаній, які взаємодіють із персональними даними осіб, що перебувають на території ЄС.

У межах ЄС і низки інших країн, зокрема Великої Британії, Австралії та США діє стандарт ISO/IEC 27001, який вимагає від організацій встановлення,

впровадження, збереження та постійного вдосконалення системи управління інформаційною безпекою [7].

Також серед міжнародних стандартів можна виділити наступні:

– ISO/IEC 15408 – це міжнародний стандарт, який визначає загальні критерії оцінки безпеки інформаційних технологій. Він забезпечує основу для визначення вимог безпеки та проведення оцінок безпеки IT-продуктів і систем. Багато структур кібербезпеки, стандартів і правил посилаються на ISO/IEC 15408 як основу для оцінки безпеки IT-продуктів і систем.

– Випущений у червні 2020 року Європейським інститутом телекомунікаційних стандартів (ETSI), стандарт EN 303 645 встановлює базові вимоги до кібербезпеки для споживчих товарів, підключених до Інтернету. ETSI EN 303 645 має важливе значення, оскільки це перший глобально застосовний стандарт кібербезпеки для споживчих пристроїв Інтернету речей, який ґрунтується на відгуках та досвіді світових галузевих, академічних та урядових гравців.

– стандарт кібербезпеки, який використовується для широкого спектру споживчих товарів, включаючи шлюзи Інтернету речей, монітори, дверні замки, телевізори та акустичні системи, а також побутову розумну техніку. Це правова база, яка описує вимоги до кібербезпеки для апаратних і програмних продуктів з цифровими елементами, що розміщуються на ринку Європейського Союзу. Тепер виробники зобов'язані серйозно ставитися до безпеки протягом усього життєвого циклу продукту.

– Закон DORA був створений, щоб посилити стійкість фінансових установ до цифрових загроз. Його головна мета – забезпечити здатність організацій функціонувати без збоїв навіть за умов кіберінцидентів, таких як атаки чи витоки даних. Це особливо актуально у фінансовій сфері, адже мова йде про безпеку коштів клієнтів і стабільність бізнес-процесів.

The National Institute of Standards and Technology (NIST) випустив багато різних стандартів, пов'язаних з кібербезпекою, розташованих на платформі

NIST Cybersecurity Framework. В основі платформи лежить ієрархічна структура основних підходів до інформаційної безпеки.

Директива Network and Information Security Directive 2 (NIS2) є ключовим законодавчим актом Європейського Союзу, який має на меті підвищити рівень кібербезпеки в країнах-членах ЄС. Її впровадження посилює вимоги до компаній, що працюють з критичними інфраструктурами, мережевими та інформаційними системами. Директива має особливе значення для українських компаній, які надають послуги європейським замовникам, особливо в сфері адміністрування програмного забезпечення, яке обробляє персональні дані громадян ЄС.

РОЗДІЛ 2
АНАЛІЗ ЗАСОБІВ ВИЯВЛЕННЯ КІБЕРЗАГРОЗ

2.1 Системи виявлення вторгнень та їх класифікація

IDS це технологія, яка здійснює моніторинг мережевого трафіку або активності системи з метою виявлення підозрілих дій, зловмисних атак або інших порушень безпеки. При виявленні потенційної загрози IDS повідомляє адміністратора або інші системи безпеки щоб той своєчасно зреагував.

За місцем збору інформації IDS поділяються на Host-based Intrusion Detection System (HIDS) – представник Open Source Host-based Intrusion Detection System (OSSEC), та Network Intrusion Detection System (NIDS) – Cisco Secure IDS, Dragon Enterasys.

HIDS є стратегічним компонентом кібербезпеки, розробленим для посилення захисту окремих пристроїв, таких як робочі станції, сервери або будь-які інші кінцеві точки в середовищі. На відміну від NIDS, яке здійснює моніторинг трафіку в мережі на наявність зловмисних дій, HIDS зосереджується на активностях, що відбуваються безпосередньо в системі. Такий підхід забезпечує багатошаровий захист, дозволяючи більш глибоко оцінити безпеку кожного індивідуального елемента в мережі.

NIDS – це тип IDS, який контролює вхідний трафік. Система аналізує активність трафіку, який надходить з пристрою або на нього. Вся активність порівнюється з наявною бібліотекою можливих атак, і як тільки виявляється щось дивне, адміністратор отримує сповіщення про це.

За швидкістю реагування IDS поділяють на:

– динамічні системи – ІКС UTM+, Рубікон (працюють у реальному часі);

– статичні системи – Hummingbird (аналізують мережу, перевіряють зміни мережевих сервісів).

Динамічні системи у реальному часі відстежують трафік на наявність аномальних ознак. Статичні здійснюють аналіз мережі, перевіряють зміни мережевих сервісів, надають дані про атаку та допомагають усунути заподіяну шкоду.

За механізмом ВА IDS виділяють:

– сигнатурні – Suricat;

– ВА – Snort, Bro-IDS.

У першому типі кожен пакет мережного трафіку порівнюється з шаблонами атак, які у базі даних атак. До переваг даного методу відносяться простота використання та низький показник хибних спрацьовувань при хорошому підборі сигнатури атак. Основними недоліками є необхідність збирання якісної бази сигнатур атак та складність детектування раніше невідомих або не внесених до бази атак.

Системи другого типу IDS, засновані на ВА, що аналізує дії, які відбуваються в мережі. Базова поведінка в мережі визначається адміністратором або за допомогою навчального набору даних при розробці системи. Дії, які не вписуються у рамки стандартної поведінки, вважаються аномальними. Аналіз трафіку щодо аномалії дає можливість виявляти атаки, невідомі системі раніше. До недоліків такого типу систем належать завдання правил визначення аномалій та сильна залежність ефективності роботи від них. [8].

2.2 Порівняльний аналіз інструментів для виявлення кіберзагроз

Для виявлення кіберзагроз використовують такі інструменти:

– це мережева IDS з відкритим кодом. Система виявляє атаки виключно на основі аналізу мережевого трафіку. Основним методом виявлення атак, використовуваним в системі, є виявлення зловживань на основі опису сигнатур атак. У системі використовується проста мова опису сигнатур атак, яка

повністю описана в документації і дозволяє адміністраторам доповнювати базу своїми сигнатурами. [10]

– це HIDS з відкритим вихідним кодом, яка забезпечує моніторинг у режимі реального часу, виявлення загроз та аналіз подій безпеки на різних платформах. ефективністю, що робить її популярною серед малого бізнесу, підприємств та ентузіастів безпеки.

– це безкоштовна, потужна платформа з відкритим кодом. Створена для виявлення загроз, моніторингу безпеки, відповідності вимогам та управління безпекою у хмарних середовищах, контейнерах та гібридних середовищах. Вона поєднує в собі функції SIEM та HIDS, надає малому та середньому бізнесу сильний інструмент для захисту від кіберзагроз.

– сніфер програма для аналізу мережевих пакетів і інших Ethernet мереж. розпізнає структуру найрізноманітніших мережевих протоколів, і тому дозволяє розібрати мережевий пакет, відображаючи значення кожного поля протоколу будь-якого рівня.

– безкоштовна відкрита платформа для обміну інформацією про кіберзагрози, яка має понад 100 тисяч учасників з 140 країн. Вона дозволяє фахівцям спільно працювати та виявляти загрози в реальному часі.

Порівняльний аналіз інструментів для виявлення кіберзагроз представлений в таблиці 2.1.

Таблиця 2.1 – Порівняльна таблиця інструментів для виявлення кіберзагроз.

№	Інструмент	Тип	Особливості	Призначення
1	Snort	NIDS (мережева IDS)	Відкритий код, виявлення атак через сигнатури, аналіз мережевого трафіку	Виявлення атак у мережевому трафіку
2	OSSEC	HIDS (хостова IDS)	Відкритий код, моніторинг у реальному часі, аналіз подій, масштабованість	Моніторинг і виявлення загроз на хостах
3	Wazuh	SIEM + HIDS	Відкритий код, виявлення загроз, моніторинг відповідності, підтримка хмарних і гібридних середовищ	Комплексне управління безпекою і виявлення загроз
4	Wireshark	Аналізатор трафіку	Відкритий код, розбір мережевих пакетів, підтримка багатьох протоколів	Аналіз і діагностика мережевого трафіку
5	AlienVault OTX	Платформа обміну інформацією	Відкрита платформа, обмін інформацією про загрози в реальному часі, понад 100 тисяч учасників	Спільна робота і обмін даними про загрози

2.3 Використання машинного навчання та штучного інтелекту для виявлення загроз

У сучасному інформаційному просторі кіберзагрози стають дедалі складнішими, динамічнішими та масштабнішими. Традиційні методи захисту, не завжди здатні ефективно протистояти новим видам атак, які змінюють свій характер, обходять фільтри або взагалі не мають відомих ознак.

Застосування Machine Learning (ML) та Artificial intelligence (AI) дозволяє системам безпеки вийти на новий рівень, оскільки ці технології здатні:

- автоматично аналізувати великі обсяги даних у режимі реального часу;
- виявляти приховані закономірності та відхилення від нормальної поведінки;
- адаптуватися до нових типів загроз без потреби ручного оновлення баз даних атак.

ML та AI дають змогу створювати системи, які навчаються на основі історичних даних, а згодом самостійно виявляють невідомі атаки або підозрілу активність у мережі. Це особливо актуально в умовах зростаючого навантаження на IT-інфраструктуру, з яким не завжди можуть упоратися фахівці з безпеки.

Досить широкого розвитку у сучасному світі набуває використання ML та AI у галузі кібербезпеки, адже вони допомагають виявленню аномалій та прогнозуванню потенційних загроз. Тому дана галузь потребує постійного удосконалення.

На рис. 2.1 показаний обсяг українського ринку кібербезпеки за певний період.

Рисунок 2.1 – Обсяг українського ринку кібербезпеки у 2016–2029 роках (млн дол. США) [17]

У кібербезпеці використовуються технології і методи AI для посилення захисту комп’ютерних систем, мереж і даних від кіберзагроз. AI допомагає автоматизувати виявлення загроз, аналіз великих обсягів даних, виявлення закономірностей і реагування на інциденти безпеки в режимі реального часу.

Основні сфери застосування AI для безпеки охоплюють виявлення аномалій, виявлення шкідливого програмного забезпечення, виявлення вторгнень, запобігання шахрайству, зведення інцидентів, звітність для зацікавлених сторін, а також створення та зворотну розробку сценаріїв.

Спеціалісти з безпеки часто використовують засоби генеративного AI, щоб допомогти в розслідуванні та відповіді. Оскільки ці інструменти використовують технологію обробки природної мови, люди можуть взаємодіяти з ними за допомогою людської мови, а не коду. Як випливає з назви, ці інструменти також здатні генерувати контент, тому вони можуть допомогти у створенні звітів, узагальненні інформації про безпеку та висновків, а також надавати детальні відповіді на запитання.

Агенти на основі AI автономно керують великими об’ємами завдань із безпеки та IT, дозволяючи людям зосередитися на проактивному захисті, тобто запобігти кібератакам ще до їх виникнення. Вони можуть розглядати фішинг, захист від втрати даних і оповіщення про внутрішні ризики, що надзвичайно тривало для людей. Агенти також здатні оптимізувати політики умовного доступу на основі даних користувача. Багато команд використовують агенти на основі AI, щоб виявляти й визначати вразливості та загрози, які потрібно вирішити, і визначити їх пріоритет [10].

Серед основних алгоритмів, що застосовуються для виявлення загроз, можна виділити:

- Random Forest, саме він ефективний для класифікації та виявлення шкідливої активності.
- Support Vector Machines (SVM) працює з великими даними, що характерно для мережевого трафіку.
- Нейронні мережі та Deep Learning (DL) здатні виявляти складні патерни в даних, що дозволяє виявляти нові типи атак.

Також існує досить багато технологій які використовують ML та AI, зокрема:

– ESET використовує машинне навчання у своїх продуктах з 1997 року, включаючи нейронні мережі та технологію DNA Detections для класифікації атак як чистих, шкідливих або потенційно небажаних.

– Vectra AI застосовує комбінацію контрольованого та неконтрольованого навчання для виявлення загроз у реальному часі, аналізуючи поведінку пристроїв та користувачів у мережі.

– Trend Micro впровадила "AI brain", який автоматизує захист від загроз, прогнозує атаки та оцінює ризики, зменшуючи навантаження на команди безпеки.

Принципи роботи ML:

– при зборі даних інформація може надходити з таких джерел, як бази даних, датчики або інтернет;

– після збору даних, їх потрібно обробити, щоб перевірити якість і придатність для аналізу;

– навчання алгоритму робити прогнози або приймати рішення на основі вхідних даних;

– модель ML аналізує вхідні дані та обирає найбільш значущі ознаки, що впливають на якість прогнозування;

– модель оцінюють після навчання, щоб визначити, наскільки вона відповідає бажаним критеріям;

– після успішного навчання та оцінки модель розгортають в реальних системах, де її роботу постійно моніторять для виявлення змін у продуктивності та своєчасного вдосконалення.

До методів ML можна віднести:

– Кероване ML – різні моделі тренують на вже помічених даних та готових відповідях. Алгоритм має обрати відповідь на гіпотезу: правильно чи неправильно, а людина – проконтролювати результат. Це відносно простий спосіб ML, який підходить для класифікації даних.

– Некероване ML – для навчання беруть інформацію без поміток. Алгоритм сам має зрозуміти закономірності та ознаки, які відрізняють об’єкти.

Підходить для прогнозування та автоматизованого очищення вхідних даних, розпізнавання та розуміння мови людини.

– Напівкероване ML – використовуються марковані та немарковані дані. Решту розмітки виконує сам алгоритм за заданими параметрами. Таке навчання корисне для обробки об’ємних файлів.

з підкріпленням – алгоритм навчається, використовуючи метод спроб і помилок. Цей спосіб грунтується на системі балів, які модель отримує залежно від дій.

Методи та типи ML представлені на рис. 2.2.

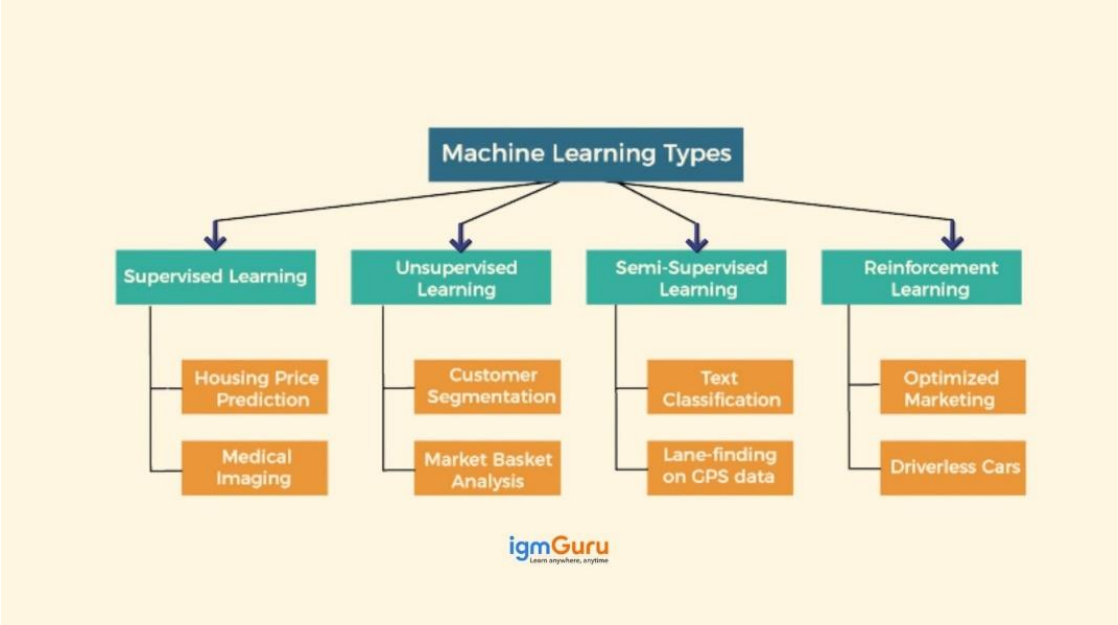

Рисунок 2.2 – Методи та типи ML [13]

Методи ML відіграють ключову роль у виявленні кіберзагроз, кожен з яких має свої переваги в різних сценаріях.

Навчання під наглядом використовується для виявлення відомих загроз, таких як віруси або фішингові атаки. Моделі навчаються на маркованих даних, що дозволяє їм точно класифікувати нові загрози на основі попереднього досвіду.

Неконтрольоване навчання використовується для виявлення невідомих або нових загроз шляхом аналізу аномалій у поведінці системи. Це особливо корисно для виявлення атак, які не мають очевидних ознак або сигнатур.

Напівконтрольоване навчання поєднує мічені та немічені дані для ефективного виявлення загроз навіть з обмеженою кількістю мічених прикладів. Це підходить для обробки великих обсягів даних, де повне маркування займає багато часу.

Навчання з підкріпленням дозволяє системам адаптивно реагувати на загрози в реальному часі, навчаючись на основі зворотного зв'язку з навколишнім середовищем. Це корисно для розробки стратегій реагування на складні та динамічні атаки.

Поєднання методів дозволяє створювати більш ефективні системи виявлення кіберзагроз та реагування на них, забезпечуючи ефективний захист в умовах постійного коливання загроз.

DL – це підвид AI та ML, який використовує багатошарові штучні нейронні мережі для забезпечення найбільшої точності в таких завданнях, як виявлення об’єктів, розпізнавання мовлення, мовний переклад та інші.

Штучні нейронні мережі отримують алгоритми та дані, обсяги яких постійно зростають. Це підвищує ефективність процесу навчання. Чим більше даних, тим краще навчання. Нейронна мережа з часом охоплює дедалі більше рівнів. Чим глибше ця мережа проникає, тим вища її ефективність.

На відміну від ML, для DL необхідне високопродуктивне обладнання, потужні графічні процесори, відеокарти тощо.

Потужні відеокарти допомагають дослідникам та фахівцям з аналізу даних пришвидшити навчання з декількох тижнів до декількох годин. Але замість того, щоб купувати дороге обладнання, навчання можна проводити на базі хмари.

На рисунку 2.3 показано різницю між простою та глибинною нейронною мережею. У простій мережі дані проходять через один прихований шар, що підходить для простих задач. У глибинній мережі є кілька прихованих шарів, які поступово виділяють важливі ознаки з даних і дозволяють розв’язувати складніші задачі, такі як розпізнавання зображень або мовлення

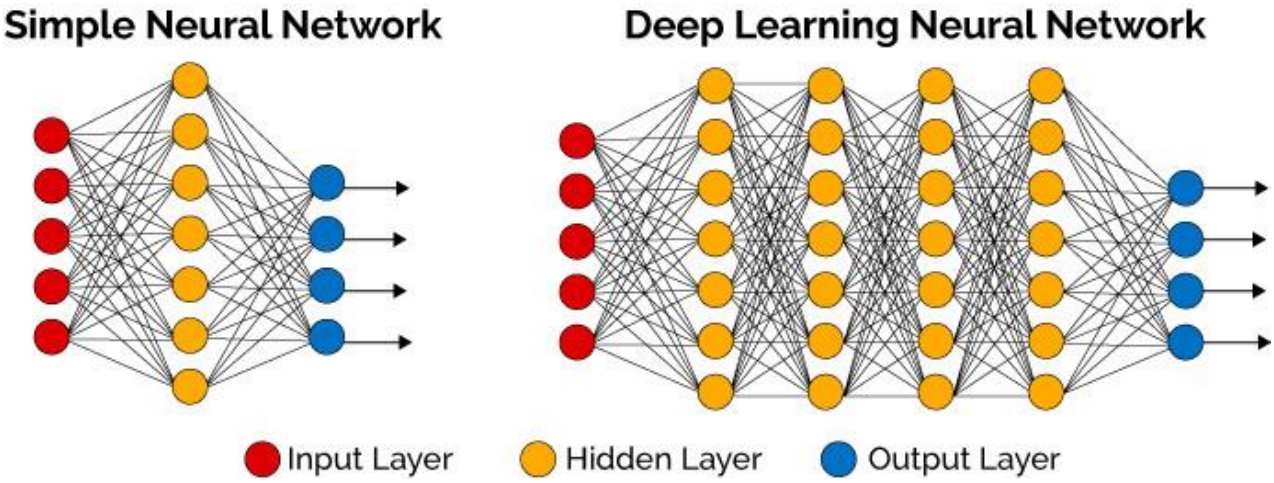

Рисунок 2.3 – Принцип роботи DL [16]

Застосування DL та AI у кібербезпеці підвищує ефективність захисту інформаційних систем, дозволяючи швидко адаптуватися до нових загроз та зменшити до мінімуму ризики для користувачів.

Розуміння DL може допомогти фахівцям виявляти загрози набагато швидше, комбінуючи його з ML. Оскільки DL активно використовують в соціальній інженерії, створюючи підробки голосів, відео та фото (deepfakes), щоб змусити співробітників платити великі гроші, тому необхідно впроваджувати відповідні заходи захисту якнайшвидше, щоб запобігти, подекуди, катастрофічним наслідкам.

Використання DL в кібербезпеці дає змогу автоматично виявляти та реагувати на загрози, аналізуючи великі обсяги даних. Це забезпечує швидке виявлення шкідливих програм, фішингових атак та інших кіберзагроз, навіть якщо вони раніше не були відомі. IDS та інструменти аналізу мережевого трафіку також використовують DL для ідентифікації аномальної поведінки, яка може свідчити про спробу атаки.

2.4 Моніторинг мережевого трафіку для забезпечення безпеки

У сучасному цифровому ландшафті загроза порушення безпеки та кібератак стає все більш поширеною. Без належних заходів захисту організації

ризикують розкрити конфіденційні дані, підірвати довіру клієнтів і зазнати фінансових втрат. Саме тут моніторинг мережі відіграє вирішальну роль. Завдяки постійному моніторингу мережевого трафіку та аналізу шаблонів підозрілі дії можна швидко виявляти, що дозволяє командам безпеки швидко реагувати та запобігати потенційним загрозам безпеці.

Однією з ключових переваг моніторингу мережі є його здатність надавати сповіщення та звіти про інциденти безпеки в реальному часі. За допомогою вдосконалених інструментів і технологій моніторингу організації можуть отримати цінну інформацію про свою мережеву інфраструктуру, виявивши будь-які порушення або аномалії, які можуть вказувати на потенційне порушення безпеки. Постійно відстежуючи мережу на наявність ознак вторгнення або спроб несанкціонованого доступу, мережеві адміністратори можуть негайно вжити заходів для зменшення ризиків і запобігання ескалації потенційних загроз. Такий проактивний моніторинг не тільки допомагає захистити конфіденційні дані, але й забезпечує загальну цілісність і конфіденційність мережі.

Проактивний моніторинг мережі є важливим у виявленні та вирішенні проблем до того, як вони вплинуть на користувачів. Завдяки постійному моніторингу мережевої інфраструктури та аналізу показників продуктивності в режимі реального часу організації можуть випереджати потенційні проблеми. Цей проактивний підхід дозволяє компаніям негайно вживати заходів, мінімізуючи час простою та забезпечуючи зручну роботу користувача.

Однією з ключових переваг проактивного моніторингу мережі є можливість виявлення та усунення вузьких місць у мережі до того, як вони спричинять збої. Ретельно відстежуючи використання пропускної здатності мережі та визначаючи зони перевантаження, організації можуть розподіляти ресурси більш ефективно та оптимізувати продуктивність мережі. Це не тільки підвищує продуктивність користувачів, але й запобігає потенційним збоям у роботі, які можуть зашкодити бізнес-операціям. Крім того, проактивний моніторинг дозволяє організаціям виявляти та усувати загрози безпеці на ранніх

стадіях, захищаючи конфіденційні дані та забезпечуючи дотримання галузевих норм. Загалом, будучи проактивним у моніторингу мережі, підприємства можуть підтримувати безпечне та надійне мережеве середовище, сприяючи позитивній взаємодії з користувачем.

Моніторинг мережевого трафіку є ключовим елементом кібербезпеки в сучасних інформаційних системах. Процес передбачає безперервне спостереження, аналіз та інтерпретацію даних, що циркулюють у мережі, з метою виявлення потенційних загроз, аномалій та несанкціонованих дій.

Згідно з дослідженням, моніторинг мережевого трафіку включає кілька етапів, зокрема, збір даних за допомогою датчиків або проксі-серверів, фільтрація для усунення непотрібного трафіку, аналіз для виявлення вразливостей і атак, а також зберігання результатів для подальшого аналізу і реагування. Такий підхід дозволяє своєчасно виявляти підозрілу активність, яка може свідчити про кібератаки або порушення політик безпеки. [15]

Моніторинг мережі використовує різні інструменти та методи для спостереження, аналізу та звітування про активність мережі. Нижче наведені ключові аспекти моніторингу мережі:

1. Відстеження в реальному часі виконується за допомогою інструментів моніторингу мережі, які безперервно аналізують потік даних у мережі, надаючи інформацію про продуктивність пристроїв і загальної мережі. Ці інструменти фіксують і аналізують мережевий трафік, відстежуючи такі фактори, як використання пропускної здатності, затримка, втрата пакетів і час відповіді. Шляхом моніторингу продуктивності мережі в реальному часі адміністратори можуть швидко виявляти вузькі місця, перевантаження або проблеми з продуктивністю і вживати відповідних заходів для оптимізації мережі.

2. Виявлення аномалій є важливим компонентом моніторингу мережі. Інструменти моніторингу встановлюють базову поведінку мережі, аналізуючи історичні дані та мережеві шаблони. Порівнюючи поточну активність мережі з цією базою, інструменти можуть виявляти незвичайні шаблони або дії, які відрізняються від нормальних. Аномалії можуть вказувати на потенційне

порушення безпеки, технічну проблему або ненормальну поведінку мережі. Можливість вчасно виявляти й реагувати на такі аномалії підвищує безпеку мережі та допомагає підтримувати стабільне мережеве середовище.

3. При виявленні аномалій або потенційних проблем, системи моніторингу мережі генерують сповіщення та детальні звіти, які інформують адміністраторів про будь-які неправильності в продуктивності мережі, безпекових подіях або потенційних загрозах. Детальні звіти надають інформацію про використання мережі, тенденції та потенційні області для поліпшення. Сповіщення та звіти дозволяють адміністраторам вживати негайних корективних дій, таких як розслідування інциденту, усунення вразливостей у безпеці або оптимізація конфігурацій мережі.

4. Моніторинг безпеки мережі включає нагляд за мережевим трафіком для виявлення та пом'якшення потенційних загроз безпеці. Включно з моніторингом на предмет спроб несанкціонованого доступу, ненормальних передач даних або інших підозрілих дій, які можуть загрожувати безпеці мережі. Завдяки безперервному моніторингу мережевого трафіку адміністратори можуть оперативно виявляти порушення безпеки, аналізувати їх вплив і вживати необхідних заходів для обмеження та запобігання подальшої шкоди.

Деякі рішення та інструменти моніторингу мережевої безпеки для виявлення загроз кібербезпеці:

– це рішення для управління політиками мережевої безпеки, яке допомагає організаціям автоматизувати та впорядкувати політики мережевої безпеки. Воно підтримує правильне налаштування правил брандмауера, маршрутизаторів та інших пристроїв безпеки, забезпечуючи належний захист мережевих активів. AlgoSec захищає організації від неправильних конфігурацій, які можуть призвести до появи шкідливих програм, програм-вимагачів та фішингових атак, а також дає командам безпеки можливість проактивно моделювати зміни в IT-інфраструктурі.

– Американська компанія SolarWinds пропонує низку рішень для управління та моніторингу мережі, включаючи засоби моніторингу мережевої безпеки, які дозволяють виявляти зміни у політиках безпеки та потоках трафіку. Вона надає інструменти для візуалізації мережі та допомагає виявляти та реагувати на інциденти безпеки. Однак для деяких організацій розгортання SolarWinds може бути складним, оскільки клієнтам доводиться купувати додаткове обладнання для локальної мережі.

– це дистрибутив Linux із відкритим вихідним кодом, призначений для моніторингу мережевої безпеки. Він об'єднує кілька інструментів моніторингу, таких як Snort, Suricata, Bro та інші, в єдину платформу, що спрощує налаштування та управління комплексним рішенням для моніторингу мережевої безпеки. Як варіант з відкритим вихідним кодом, це одне з найбільш економічних рішень, доступних на ринку, але для його ефективного налаштування під потреби вашої організації можуть знадобитися додаткові ресурси для розробки.

– Elastic ELK Stack – це комбінація трьох інструментів із відкритим вихідним кодом: Elasticsearch, Logstash та Kibana. Він зазвичай використовується для аналізу даних журналів та подій. З його допомогою можна централізувати журнали, проводити аналіз у режимі реального часу та створювати панелі моніторингу мережевої безпеки. Набір інструментів забезпечує високоякісну кореляцію великих масивів даних та надає командам безпеки широкі можливості для підвищення безпеки та продуктивності мережі за допомогою автоматизації.

– Cisco Stealthwatch – це комерційне рішення для аналізу та моніторингу мережевого трафіку. Воно використовує NetFlow та інші джерела даних для виявлення та реагування на загрози безпеці, моніторингу поведінки мережі та забезпечення видимості мережевого трафіку. Це високоефективне рішення для аналізу мережевого трафіку, що дозволяє аналітикам безпеки виявляти загрози, що проникли в мережеві активи, до того, як вони встигнуть завдати серйозної шкоди.

– Suricata – це інструмент IDS/IPS з відкритим вихідним кодом, який може аналізувати мережевий трафік щодо загроз. Він пропонує високопродуктивні функції та підтримує правила, сумісні зі Snort, що робить його гарною альтернативою. Suricata була розроблена пізніше, ніж Snort, тому вона підтримує такі сучасні функції робочого процесу, як багатопоточність та вилучення файлів. На відміну від Snort, Suricata підтримує правила виявлення на рівні додатків та може ідентифікувати трафік на нестандартних портах на основі протоколу трафіку.

(раніше Bro) – це фреймворк для аналізу мережі з доступним вихідним кодом, який націлений на надання детальної інформації про мережеву активність. Він може допомогти виявити та проаналізувати потенційні інциденти безпеки та часто використовується разом з іншими інструментами NSM. Інструмент допомагає фахівцям з аналітики безпеки класифікувати та моделювати мережевий трафік за протоколами, полегшуючи перевірку великих обсягів даних. Як і Suricata, він працює на рівні програм і має функцію розрізняти протоколи. [12]

Основні особливості рішень полягають у здатності аналізувати різні типи трафіку, виявляти аномальну поведінку в мережі та надавати засоби для виявлення та аналізу кіберзагроз. Моніторинг допомагає забезпечити безпеку мережі та допомагає організаціям виявляти та вирішувати проблеми з безпекою, зменшує ризики для бізнесу та забезпечує стабільну роботу мережі.

РОЗДІЛ 3
ОСНОВНІ НАПРЯМКИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ЗАСОБІВ ЗАХИСТУ МЕРЕЖ

3.1 Особливості розвитку сучасних кіберзагроз

Кількість і складність кіберзагроз зростає у геометричній прогресії. Кібератаки стають все частішими, непомітними та більш руйнівними. Зростає кількість інцидентів як на побутовому так і на державному рівнях. Водночас кіберзлочинці активно користуються новітніми технологіями, такими як AI, ML, автоматизовані скрипти, що дозволяє їм здійснювати атаки з більшою ефективністю та складністю, ніж раніше. Згідно з аналітичними оглядами, використання таких технологій створює додаткові вразливості, які зловмисники можуть використати для атак на конфіденційність та критично важливі системи.

Дедалі частіше залучаються AI-технології для підвищення ефективності злому. Злочинці застосовують алгоритми ML для автоматизації підбору паролів, створення фішингового контенту високої точності та обходу виявлення.

Системи генеративного AI здатні з високою правдоподібністю імітувати стилі листування реальних осіб, що ускладнює виявлення фішингових повідомлень традиційними методами. У той же час фахівці з кібербезпеки використовують AI для проактивного виявлення аномалій у мережевому трафіку та автоматизації реагування на інциденти. Одним із ключових напрямів розвитку у захисті інформаційних систем стає саме поєднання машинного навчання з попереднім обміном кіберрозвідкою (threat intelligence) для швидкого виявлення нових загроз.

Серед новітніх загроз виділяють атаки типу Highly Evasive Adaptive Threats (HEAT). Вони використовують динамічно генеровані шкідливі посилання та файли, щоб уникнути виявлення сучасними системами

кіберзахисту. Такі атаки можуть обходити URL-фільтрацію та систему багатофакторної автентифікації завдяки швидкій зміні доменів та розміщенню шкідливого коду в JavaScript, що ускладнює його статичний аналіз. HEAT-атаки розроблені саме для подолання традиційних меж та захисних бар'єрів у мережах, і зараз це одна з основних загроз для бізнесу та державних структур.

Однак, найпоширенішими і найнебезпечнішими формами кіберзагроз залишаються програми-вимагачі. Зловмисне програмне забезпечення-шифрувальник (ransomware) блокує доступ до файлів або системи, а потім вимагає викуп за відновлення контролю. У 2023 році близько 72,7 % усіх організацій у світі стали жертвами кібератак за участю програм-вимагачів. Найбільше від кібервимагань страждають великі компанії, тоді як малі та середні підприємства також залишаються у зоні ризику. Цей тип загроз є особливо небезпечним для критичних об'єктів. Під час останніх глобальних хвиль атак було зафіксовано відключення мереж енергопостачання, охоплення медичних систем тощо. Серед ключових мотивів поширення ransomware – фінансовий зиск, вимагання даних та зниження довіри до інфраструктур опонентів.

Техніки соціальної інженерії, зокрема фішинг, залишаються одними з найбільш ефективних інструментів у руках кіберзлочинців. Вони полягають у масованій розсилці підроблених повідомлень (електронною поштою, SMS, у месенджерах), що імітують довірених відправників (банки, державні органи, відомі компанії тощо). У 2023 році фішингові атаки та їх мобільна версія «смішинг» значно активізувалися. За останніми даними, приблизно 41 % усіх кіберінцидентів були пов'язані з фішингом або зломом електронної пошти. Зловмисники застосовують глибинні техніки маскування контенту та попередньо вивчають структуру корпоративних або державних листів, щоб зробити підробку максимально правдоподібною. Унаслідок такого соціального інженірингу жертви розкривають свої облікові дані або конфіденційну інформацію, що відкриває зловмисникам шлях до внутрішніх мереж і подальших руйнівних дій.

Уразливість об’єктів критичної інфраструктури (енергетика, транспорт, банки, охорона здоров’я) стає головною вразливістю національної безпеки. Кібератаки на системи управління такими об’єктами можуть призвести до економічних збитків і навіть загрожувати життю людей. Розвиток технологій і масштабне підключення об’єктів «smart city» до мережі Інтернет значно розширює поле для проникнення.

Досить великої популярності набуває поняття «гібридної загрози», яке передбачає поєднання військових, політичних, економічних та кіберметодів для досягнення стратегічних цілей. Кіберскладова у гібридних конфліктах набуває все більшої ваги внаслідок атаки на інформаційні системи супротивника. За допомогою них можна впливати на громадську думку, знищувати дані чи руйнувати інфраструктуру без явного вторгнення. Отже, кіберзагрози стали невід’ємною частиною гібридних конфліктів у сучасному світі. Цифровізація державних служб і громадських комунікацій відкриває нові можливості впливу, зокрема, дезінформація через контрольовані медіа, масові кібератаки з метою підриву роботи ключових об’єктів, витоки даних як засіб шантажу. Оскільки гібридні загрози поєднують різнорідні засоби (лабораторне кіберзлочинство, інформаційні спецоперації, фізичний саботаж тощо), їх нейтралізація вимагає скоординованої відповіді на внутрішньому і міжнародному рівнях.

Швидке розширення екосистеми Інтернету речей суттєво впливає на карти загроз, адже до мережі підключається все більше сенсорних пристроїв, побутової техніки та промислових контролерів, що часто мають обмежений захист. Дослідження глобальних трендів за останні 20 років показують, що розгортання IoT і кіберзагрози взаємопов’язані внаслідок збільшення числа розумних пристроїв, що зумовлює зростання шкідливих мережевих ботнетів та пошук нових вразливостей на рівні заліза. З іншого боку, девайси IoT можуть слугувати засобом розповсюдження атак, утворюючи додаткові точки входу в корпоративні мережі. Аналітика також підкреслює, що захист IoT-пристроїв потребує більшої уваги, оскільки ці мережі стають невід’ємною частиною критичної інфраструктури та бізнес-процесів.

Протидія сучасним загрозам вимагає комплексних засобів захисту і продуманих стратегій. У першу чергу це означає багатошаровий захист, який передбачає регулярне оновлення операційних систем і програмного забезпечення, встановлення антивірусних програм і систем виявлення вторгнень, багатофакторна автентифікація користувачів, шифрування даних тощо. Також критично важливо навчати персонал правильно реагувати на підозрілі повідомлення і впроваджувати централізоване збирання та аналіз журналів подій (SIEM-системи). Існує необхідність «цілісного» підходу, що поєднує технологічні рішення з підвищенням обізнаності користувачів та міжнародною співпрацею. Зокрема, сучасні розробки вказують на потребу в автоматизованому обміні інформацією про загрози (threat intelligence) між організаціями та прискоренні автоматичного реагування на атаки, що знижує вразливість систем при нових серіях інцидентів.

Швидка еволюція технологій веде до появи нових напрямків атак (від використання AI до HEAT-методів). Для забезпечення надійного захисту необхідна постійна модернізація засобів безпеки, інтегрована система моніторингу й аналізу аномалій, а також освітня робота з персоналом та обмін досвідом на національному й міжнародному рівнях. Усі ці заходи мають бути спрямовані на підтримку гнучкості і стійкості інформаційних інфраструктур перед лицем новітніх кіберзагроз.

3.2 Огляд новітніх технологій для захисту мереж

Кіберзагрози розвиваються стрімко, адже зловмисники застосовують дедалі витонченіші методи, а кількість підключених до мережі пристроїв невпинно зростає. У зв’язку з цим і безпека мереж потребує постійного удосконалення технологій захисту. Сучасні напрями вирішення даних проблем поєднують в собі масштабне відстеження подій, глибоку аналітику та автоматизоване реагування.

Серед основних принципів, переваг та особливостей впровадження ключових інструментів мережевого захисту можна виділити наступні:

1. Системи SIEM збирають, нормалізують та аналізують журнали подій із численних джерел – серверів, додатків, мережевих пристроїв, фаєрволів тощо. Вони надають єдиний центр зору на безпекову активність організації. Вони працюють за допомогою централізованого збору і кореляції логів у реальному часі з різних елементів інфраструктури, а також займаються пошуком відомих сигнатур атак та аномалій.

Серед переваг систем SIEM можна виділити те, що вони дозволяють виявити загрози у режимі реального часу і прискорювати реагування на інциденти. Крім того, такі системи полегшують виконання вимог стандартів безпеки, надаючи звіти відповідності. За допомогою SIEM аналітики можуть автоматично корелювати інформацію з різних джерел, що допомагає виявляти складні атаки, які важко помітити при розгляді окремих записів.

SIEM-системи часто інтегруються з іншими рішеннями (IDS/IPS, системами керування ідентичностями). Для ефективної роботи потрібні високопродуктивні обчислювальні ресурси, адже обсяги логів можуть бути дуже великими. Розгортання вимагає налаштування правил кореляції і регулярного оновлення бази сигнатур загроз.

2. IDS та IPS призначені для моніторингу мережевого трафіку і виявлення небезпечних дій. IDS лише сповіщає про підозрілі дії, а IPS може блокувати їх.

IDS/IPS сканують усі пакети в мережі, порівнюючи їх з відомими шаблонами атак або нормальними моделями поведінки. При виявленні спроби експлуатації вразливості система піднімає тривогу (IDS) або одразу перериває з’єднання (IPS).

Системи виявлення/запобігання вторгненням здатні зупиняти атаку на ранніх етапах. Вони зменшують потенційну шкоду, припиняючи маніпуляції з вразливими пристроями ще до успішного проникнення. У багатьох реалізаціях IDS/IPS включені у сучасні фаєрволи, що дозволяє застосовувати їхні функції на межі мережі та у центрах обробки даних.

Для їх ефективності потрібне регулярне оновлення бази сигнатур і правил аналізу. IDS/IPS корисні як на периферії мережі, так і всередині її сегментів. Їх часто розгортають у поєднанні з SIEM, адже журнали подій та сповіщення можуть передаватися на єдину панель моніторингу.

3. Extended Detection and Response (XDR) має можливість поєднання даних від різних систем безпеки для комплексного виявлення та реагування на загрози. Збір та об'єднання телеметрії з багатьох джерел (ендоінтів, серверів, хмарних середовищ, мережевого трафіку, електронної пошти) допомагає автоматично корелювати події. Завдяки цьому XDR створює єдину картину безпеки організації.

Даний підхід надає можливість краще виявляти загрози, що, в свою чергу, домагає глибшому їх аналізу. Досліджуючи всі події разом, система може виявляти складні, багатокрокові атаки, які самі по собі могли б бути непоміченими. Впровадження XDR значно скорочує час реагування, алде об'єднані дані дозволяють пріоритизувати інциденти, а автоматизовані механізми реагування знімають рутинне навантаження з аналітиків. Тобто XDR-системи автоматично вміють ізолювати уражені пристрої чи блокувати шкідливі процеси, не чекаючи втручання людини.

Особливостями даного підходу є його можливість інтегруватися в наявні системи, зокрема SIEM, що, в свою чергу, вимагає високого ступеня сумісності між ними. Важливою є наявність широких аналітичних можливостей для кореляції даних у реальному часі.

4. Zero Trust (концепція «нульової довіри») змінює традиційний підхід до безпеки. Тобто, будь-який доступ (навіть зсередини мережі) виконується лише за умови повної автентифікації та авторизації, тому кожен запит вважається новим.

Zero Trust забезпечує захищений авторизований доступ до ресурсів організації, які можуть бути розподілені між локальною інфраструктурою і хмарами. Користувачі та пристрої можуть працювати з будь-якої точки, але

після кожного запиту виконується перевірка прав доступу та відповідності політикам безпеки.

Серед ключових елементів Zero Trust можна виділити ретельну ідентифікацію користувачів і пристроїв, мікросегментацію мережі, шифрування зв’язку та безперервний моніторинг сеансів. Для впровадження архітектури Zero Trust часто використовують технології Secure Access Service Edge (SASE), SDP та системи контролю доступу на базі ролей. Такий підхід дозволяє значно зменшити площину атаки й оперативно заборонити потенційно скомпрометовані сегменти чи облікові записи.

5. Next-Generation Firewal (NGFW) – це еволюція традиційних фаєрволів із більш детальною перевіркою трафіку. Вони можуть відрізняти конкретні додатки незалежно від того, які порти вони використовують.

На відміну від традиційних фаєрволів, в NGFW вбудовані IDS/IPS і функції глибокого огляду пакетів. Вони можуть використовувати зовнішні сервіси розвідки загроз, щоб оперативно розпізнавати та блокувати нові види атак. Такий інтелектуальний брандмауер дає значно ширшу видимість активності в мережі і краще захищає від складних загроз, які створюють цілеспрямовані атаки та витік даних.

NGFW зазвичай замінює традиційний кореневий брандмауер у мережі організації. Розгортання NGFW може підвищити затримки в мережі, тож для важливих сценаріїв часто встановлюють декілька пристроїв або кластеризують їх для масштабованості.

6. Urchin Tracking Module (UTM) об’єднує в одному пристрої кілька базових функцій безпеки, тобто консолідація багатьох сервісів, таких як брандмауер, IPS/IDS, антивірус, антиспам, фільтрація веб-контенту, в одній апаратній або віртуальній платформі. UTM-пристрій охоплює весь трафік мережі і застосовує до нього послідовно різні методи захисту.

Завдяки єдиній панелі управління можна централізовано моніторити та контролювати безпеку мережі. Це спрощує адміністрування, особливо для невеликих та середніх організацій. UTM дозволяє спростити IT-

інфраструктуру, шляхом відсутності потреби у численних пристроях. Регулярні оновлення антивірусних сигнатур та фільтрів є критичними для підтримки ефективного захисту.

7. Інтернет речей (IoT) додає у мережі десятки й сотні нових пристроїв, часто з обмеженими засобами захисту. IoT-пристрої розміщують в окремих віртуальних локальних мережах чи VLAN, ізольованих від критичних ресурсів. Таке розділення обмежує розповсюдження потенційних атак, якщо один з пристроїв буде скомпрометований.

Традиційні засоби мережевого захисту розширюють шляхом спеціалізованих IDS/IPS для IoT. Поширеним підходом є застосування систем поведінкового аналізу. Вони відстежують трафік IoT-пристроїв і попереджають користувачів при виявлені незвичні патерни.

На пристроях впроваджують сертифікати, цифрові ключі або багатофакторну автентифікацію, щоб лише авторизовані девайси могли підключатися.

Критично важливо автоматизувати оновлення прошивок і програмного забезпечення IoT, щоб закривати відомі вразливості. Регулярне патчування та управління життєвим циклом пристроїв значно знижує ризик небезпеки.

8. Сучасні системи захисту активно використовують AI і автоматизацію для підвищення ефективності, зокрема алгоритми ML допомагають обробляти великі обсяги даних безпеки, зокрема, логи, мережеві пакети тощо, та виявляти у них приховані закономірності. Завдяки цьому система здатна помічати ранні ознаки атаки, які людина могла б пропустити, і передбачати нові загрози. AI-підходи ефективні проти еволюційних алгоритмів зловмисників, адже здатні виявляти аномальну поведінку при високому обсязі подій.

Серед новітніх систем захисту, які використовують AI та автоматизацію можна виділити наступні:

- Платформи Security Orchestration, Automation and Response (SOAR), які інтегрують різні інструменти безпеки й дозволяють прописувати сценарії реакції на інциденти. Це означає, що виявлення загрози може одразу

призводити до блокування зловмисного трафіку, ізоляції уражених вузлів без участі людини. Таке автоматичне реагування зменшує затримки й навантаження на аналітиків. Системи швидко визначають критичні події та запускають заздалегідь налаштовані дії, що значно скорочує час на локалізацію інциденту та мінімізує збитки.

– AI також використовується для поліпшення якості сигналів від IDS/IPS, брандмауерів та інших сенсорів. Системи User and Entity Behavior Analytics аналізують поведінку користувачів і машин, дозволяючи відрізняти випадкові помилки від цілеспрямованих атак.

Новітні технології захисту мереж створюють багаторівневий екран проти сучасних кіберзагроз. Комбінація SIEM, IDS/IPS, XDR, NGFW, UTM, Zero Trust – забезпечує всебічний моніторинг і адаптивний захист. Використання AI та автоматизації додає цьому набору здатність самонавчатись і реагувати практично в реальному часі. Експерти відзначають, що через складність і динаміку сучасних атак відмова від застарілих рішень та впровадження інтелектуальних платформ стає критично важливою. Саме постійне оновлення і інтеграція описаних підходів дозволяють організаціям своєчасно виявляти нові загрози, ізолювати інциденти та мінімізувати ризики. Відтак упровадження цих передових технологій є ключем до протидії сучасним кібератакам та збереження кіберстійкості підприємства.

3.3 Основні проблеми впровадження сучасних засобів захисту

Складність кіберзагроз, серед яких атаки з використанням AI/ML, програми-вимагачі та фішинг, вимагає новітніх рішень, зокрема, XDR, SASE чи сучасних NGFW. Впровадження цих технологій стикається з технічними, організаційними та економічними перешкодами, які потребують комплексного підходу для подолання.

1. Технічні загрози становлять основну перешкоду для ефективного захисту мереж. Системи, які аналізують мережевий трафік і виявляють

аномалії, потребують обробки величезних обсягів даних у реальному часі. Зростання кількості підключених пристроїв через IoT створює значне навантаження, яке багато систем не здатні обробляти без затримок. Така платформа як Splunk втрачає продуктивність при обробці великих потоків даних, що уповільнює виявлення загроз. Перехід до хмарних рішень, таких як AWS Security Hub, вирішує проблему масштабованості, зменшуючи залежність від локального обладнання та підвищуючи швидкість обробки.

Несумісність із застарілим обладнанням створює додаткові труднощі. Організації використовують маршрутизатори та сервери, які не підтримують сучасні протоколи безпеки чи технології аналізу аномалій. Поетапна модернізація інфраструктури, починаючи з критичних компонентів, усуває ці вразливості. Заміна старих мережевих пристроїв на моделі, сумісні з NGFW, забезпечує надійний захист зв’язку.

Складність налаштування захисних систем становить ще одну проблему. Платформи, які корелюють дані для виявлення загроз, вимагають точного визначення правил і параметрів. Некоректна конфігурація призводить до хибнопозитивних результатів, ускладнюючи ідентифікацію реальних атак. Автоматизація цього процесу за допомогою інструментів штучного інтелекту, таких як IBM Watson, спрощує налаштування та зменшує залежність від висококваліфікованих фахівців.

На рис. 3.1 показано діаграму розподілу впливу технічних проблем на ефективність захисту. Проблема масштабованості становить 40% через зростання трафіку від IoT-пристроїв, несумісність обладнання – 35% через застарілі пристрої, а складність налаштування – 25% через потребу в точній конфігурації. Діаграма підкреслює необхідність пріоритизації масштабованості при модернізації інфраструктури, оскільки ця проблема має найбільший вплив.

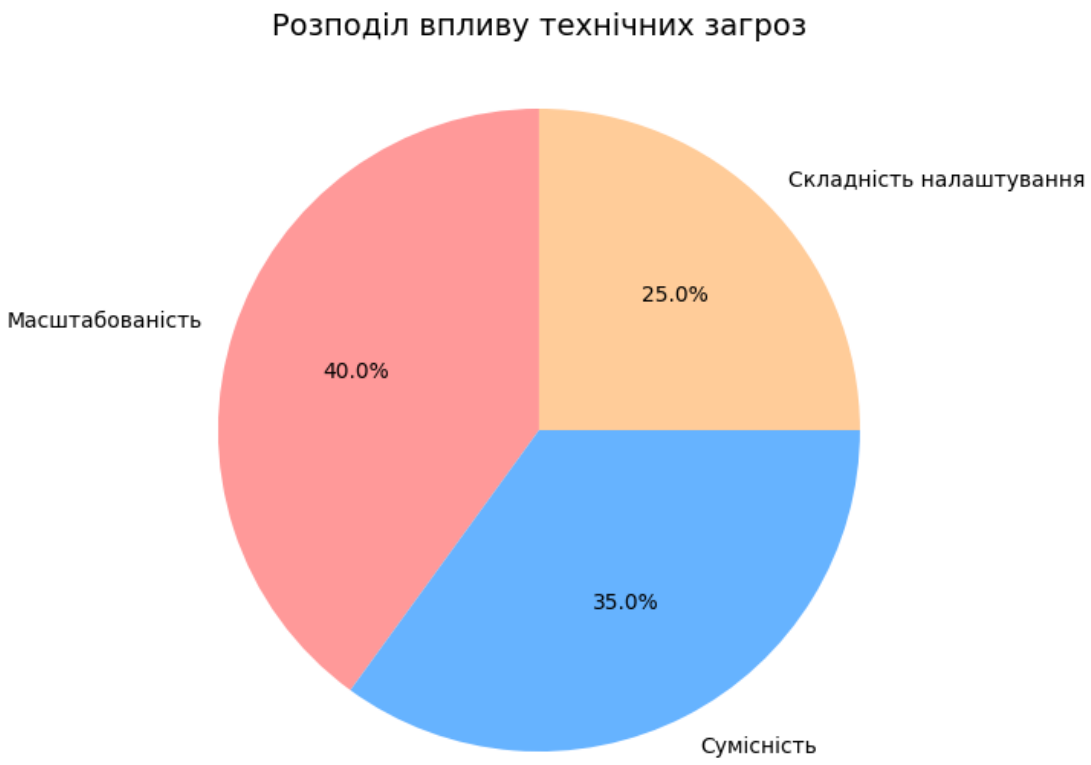

Рисунок 3.1 – Діаграма впливу технічних загроз на ефективність захисту

2. Організаційні загрози значно ускладнюють впровадження сучасних засобів захисту. Технології, які використовують штучний інтелект і машинне навчання для прогнозування загроз, потребують фахівців із глибокими знаннями, яких часто бракує. Регулярні програми навчання, зокрема сертифікація за стандартами Cisco CCNP Security, підвищують компетентність персоналу. Такі ініціативи дозволяють ефективно використовувати системи, зокрема XDR, без залучення зовнішніх консультантів.

Відсутність чітких регламентів безпеки знижує ефективність захисту. Якщо у системі контролю права доступу не визначені, то це всеодно призводить до несанкціонованих дій. Розробка політик, які відповідають міжнародним стандартам, оптимізує ресурси та підвищує ефективність захисту, обмежуючи доступ до критичних даних.

Опір персоналу новим технологіям, спричинений сприйняттям їх як ускладнення робочого процесу, гальмує адаптацію. Програми навчання, які

демонструють переваги моделі Zero Trust, підвищують готовність до змін і зменшують вплив людського фактора.

3. Економічні загрози створюють значні перешкоди для організацій, адже впровадження сучасних технологій, таких як NGFW чи XDR, вимагає значних інвестицій у обладнання, програмне забезпечення та навчання. Міжмережевий екран Palo Alto Networks коштує десятки тисяч доларів, що недоступно для малих організацій. Хмарні платформи, такі як Microsoft Defender XDR, знижують витрати на інфраструктуру, роблячи захист доступним для ширшого кола компаній.

Обмежене фінансування організацій і малих підприємств, ускладнює оновлення застарілих систем. Державно-приватне партнерство та грантові програми забезпечують необхідне фінансування для модернізації, дозволяючи впроваджувати сучасні захисні рішення.

У таблиці 3.1 загально описано основні загрози впровадження сучасних засобів захисту.

Таблиця 3.1 Основні загрози впровадження сучасних засобів захисту

№	**Категорія**	**Загроза**	**Опис**	**Ілюстрація**
1	Технічні	Масштабованість	Обробка великих обсягів трафіку без затримок	Зростання IoT-пристроїв
		Сумісність	Несумісність із застарілим обладнанням	Маршрутизатори без сучасних протоколів
		Складність налаштування	Високі вимоги до конфігурації систем	Хибнопозитивні результати SIEM
2	Організаційні	Дефіцит кадрів	Недостатня кількість фахівців із AI/ML	Обмежене використання XDR
		Відсутність політик	Нерозроблені регламенти безпеки	Несанкціонований доступ до даних
		Опір змінам	Низька готовність до адаптації	Сприйняття Zero Trust як ускладнення
3	Економічні	Високі витрати	Значні інвестиції в обладнання та навчання	Вартість NGFW Palo Alto Networks
		Обмежене фінансування	Недостатнє фінансування для оновлення систем	Застарілі системи критичної інфраструктури

Для вирішення виявлених загроз можна виділити наступні рекомендації:

– заміна застарілого обладнання, зокрема, маршрутизаторів із підтримкою сучасних протоколів безпеки, усуває проблему сумісності та підвищує захист;

– поєднання сигнатурного аналізу (як у Snort) із поведінковим аналізом (як у XDR), забезпечує захист від існуючих і нових загроз, таких як програми-вимагачі;

– регулярні тренінги персоналу підвищують компетентність у використанні систем із AI;

– для оптимізації ресурсів та підвищення ефективності захисту використовують чіткі регламенти, які обмежують доступ;

– хмарні платформи, такі як AWS Security Hub, допомагають у економії витрат при обмеженому фінансуванні;

На рис. 3.2 зображено діаграму, яка показує процентне співвідношення вирішення існуючих проблем на рівень безпеки.

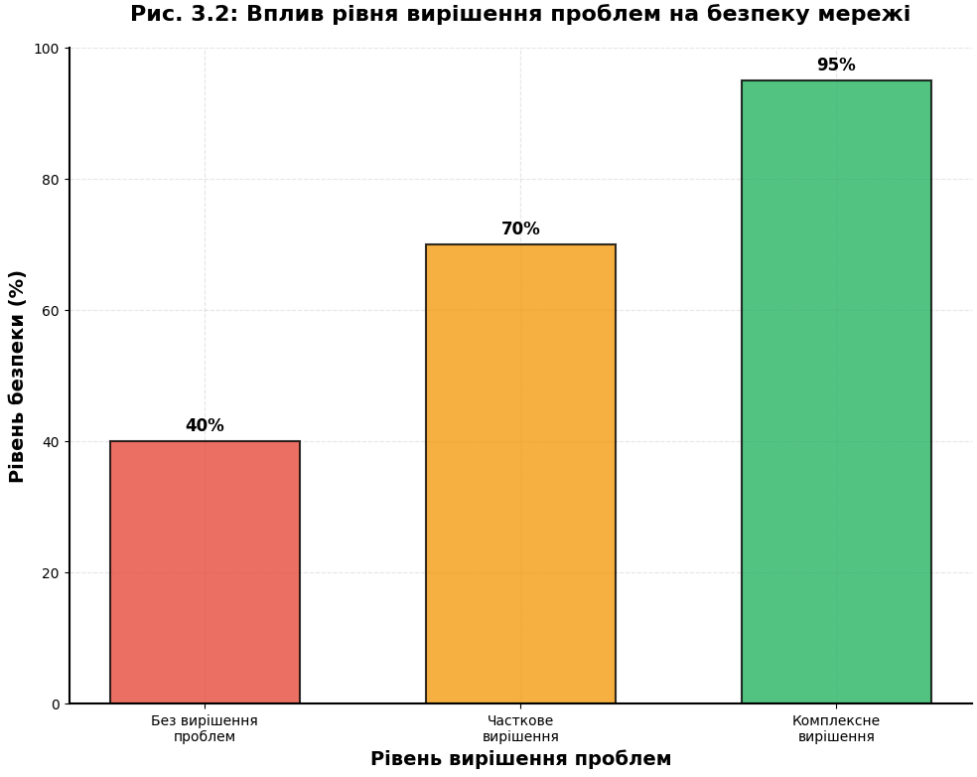

Рисунок 3.2 – Діаграма залежності впливу вирішення проблем на рівень безпеки

Забезпечення захисту інформаційних систем від кіберзагроз не обмежується лише технологічними рішеннями, а потребує комплексного підходу, що враховує кілька взаємопов'язаних напрямів. Кожен із цих аспектів має свої особливості, проблеми та вимоги, які необхідно враховувати для створення ефективної системи кібербезпеки.

Технічні загрози долаються через модернізацію інфраструктури та хмарні рішення. Організаційні – усуваються шляхом навчання персоналу та розробки чітких регламентів. Економічні загрози вирішуються через оптимізацію витрат за допомогою інтегрованих платформ, таких як XDR чи SASE. Рекомендації дозволяють організаціям створювати стійкі системи захисту, здатні протистояти сучасним кіберзагрозам. Розвиток штучного інтелекту та хмарних технологій у майбутньому забезпечить адаптивність і ефективність кібербезпеки, що є ключовим напрямом для захисту інформаційних систем.

3.4 Перспективи інтеграції систем виявлення загроз у комплексні рішення кібербезпеки

В процесі дослідження сформульовано позицію щодо перспектив інтеграції систем виявлення загроз у комплексні рішення кібербезпеки. Складність сучасних кіберзагроз, таких як атаки з використанням штучного інтелекту, програми-вимагачі та фішинг, вимагає переходу від ізольованих інструментів до єдиних екосистем захисту, зокрема XDR, SASE та SOAR. Інтеграція забезпечує точне виявлення, швидке реагування та оптимізацію ресурсів, вирішуючи проблеми сучасного кіберландшафту.

Сучасні кіберзагрози характеризуються багаторівневістю, поєднуючи фішинг, експлуатацію вразливостей пристроїв IoT і несанкціонований доступ до мережі. Ізольовані інструменти, такі як IDS чи IPS, обмежені у здатності протистояти таким атакам. Система Snort аналізує мережевий трафік, але не виявляє аномалій на кінцевих точках, тоді як Wazuh фокусується на хостовому моніторингу. Інтеграція цих інструментів у комплексні рішення, такі як XDR

чи SASE, створює єдину платформу, яка об’єднує дані з мережі, хмари та кінцевих точок, забезпечуючи цілісний аналіз і реагування. Використання штучного інтелекту та машинного навчання підвищує адаптивність до нових загроз, дозволяючи виявляти атаки без відомих сигнатур.

Інтеграція систем виявлення загроз у комплексні системи захисту забезпечує переваги, які вирішують технічні, організаційні та економічні проблеми:

1) Об’єднання даних із мережі, хмари та кінцевих точок дозволяє виявляти складні атаки, такі як багаторівневі кампанії, що включають фішинг і шкідливе програмне забезпечення. Платформа XDR аналізує ланцюжки подій, ідентифікуючи загрози, які ізольовані IDS пропускають.

2) Автоматизація через SOAR зменшує час реакції на інциденти з годин до секунд. При виявленні програми-вимагача система ізолює уражений пристрій і блокує IP-адресу зловмисника, мінімізуючи шкоду.

3) Централізоване управління через єдину платформу, таку як Cisco SecureX, знижує потребу в кількох інтерфейсах і спеціалізованих кадрах, зменшуючи витрати на адміністрування.

4) AI і ML дозволяють системам навчатися на основі нових даних, що допомагає адаптуватися до нових загроз та виявляти невідомі атаки. Платформи такі як Vectra AI аналізують поведінку в мережі, ідентифікуючи аномалії.

На рис. 3.3 зображено радарну діаграму, яка порівнює ефективність інтегрованих рішень (XDR, SASE, SIEM+SOAR) за п’ятьма параметрами: точність виявлення, час реагування, оптимізація ресурсів, адаптивність і простота управління. Дана діаграма показує, що XDR має високі результати в точності та адаптивності завдяки AI-аналітиці. SASE, зокрема, лідирує в оптимізації ресурсів і простоті управління через хмарну архітектуру, а комбінація SIEM та SOAR виділяється швидким реагуванням завдяки автоматизації. Діаграма може допомогти вибрати рішення залежно від пріоритетів, підкреслюючи сильні сторони кожного підходу.

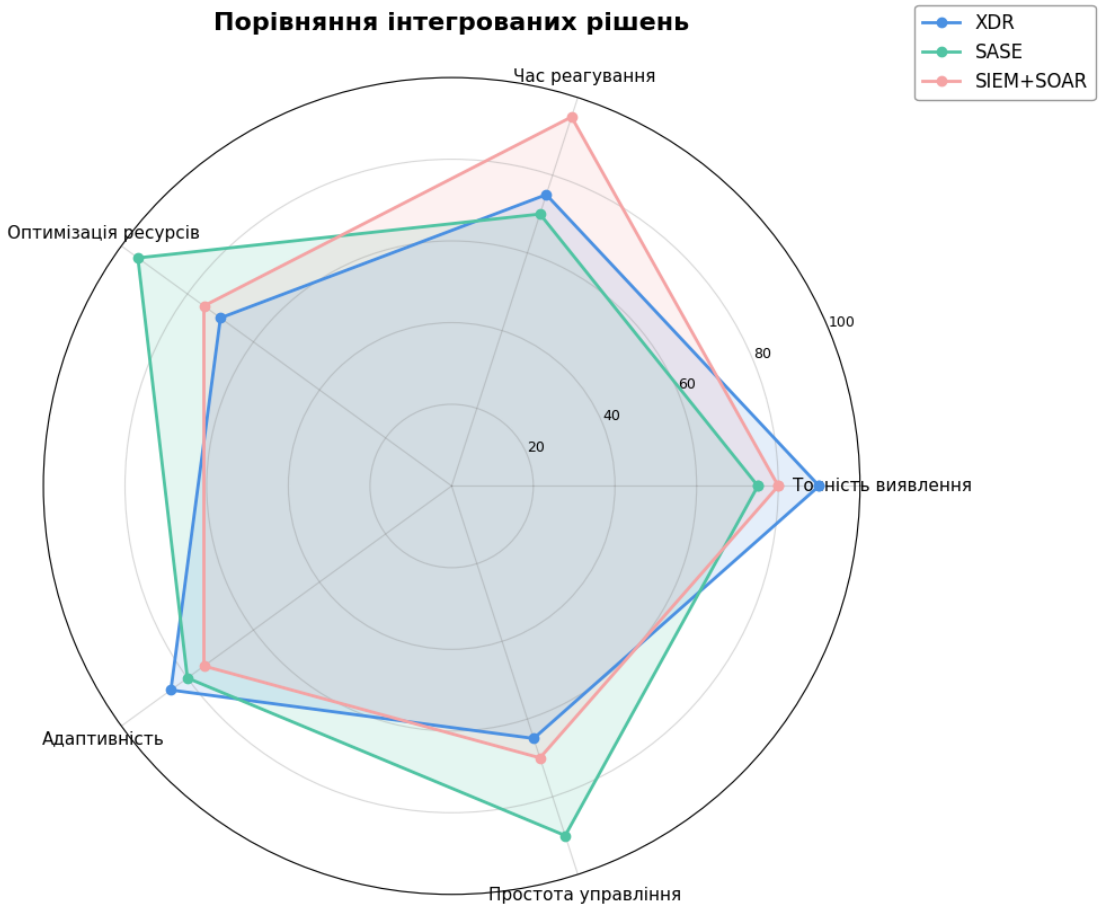

Рисунок 3.3 – Діаграма порівняння ефективності інтегрованих рішень за параметрами

У таблиці 3.2 ілюструються переваги інтегрованих рішень над ізольованими.

Таблиця 3.2 – Порівняння ізольованих та інтегрованих рішень

Параметр	**Ізольовані рішення (IDS, IPS)**	**Інтегровані рішення (XDR, SASE)**
Джерела даних	Обмежені (мережа або хост)	Мережа, хмара, кінцеві точки
Виявлення складних атак	Низьке, аналіз окремих подій	Високе, аналіз ланцюжків подій
Час реагування	Повільний, ручний аналіз	Швидкий, автоматизований
Управління	Складне, кілька панелей	Просте, єдина платформа
Витрати на підтримку	Високі, різнорідність систем	Знижені, уніфікація
Адаптивність до загроз	Низька, сигнатурний підхід	Висока, AI/ML

На рис 3.4 зображено діаграму, на якій показано як процес інтеграції впливає на покращення захисту.

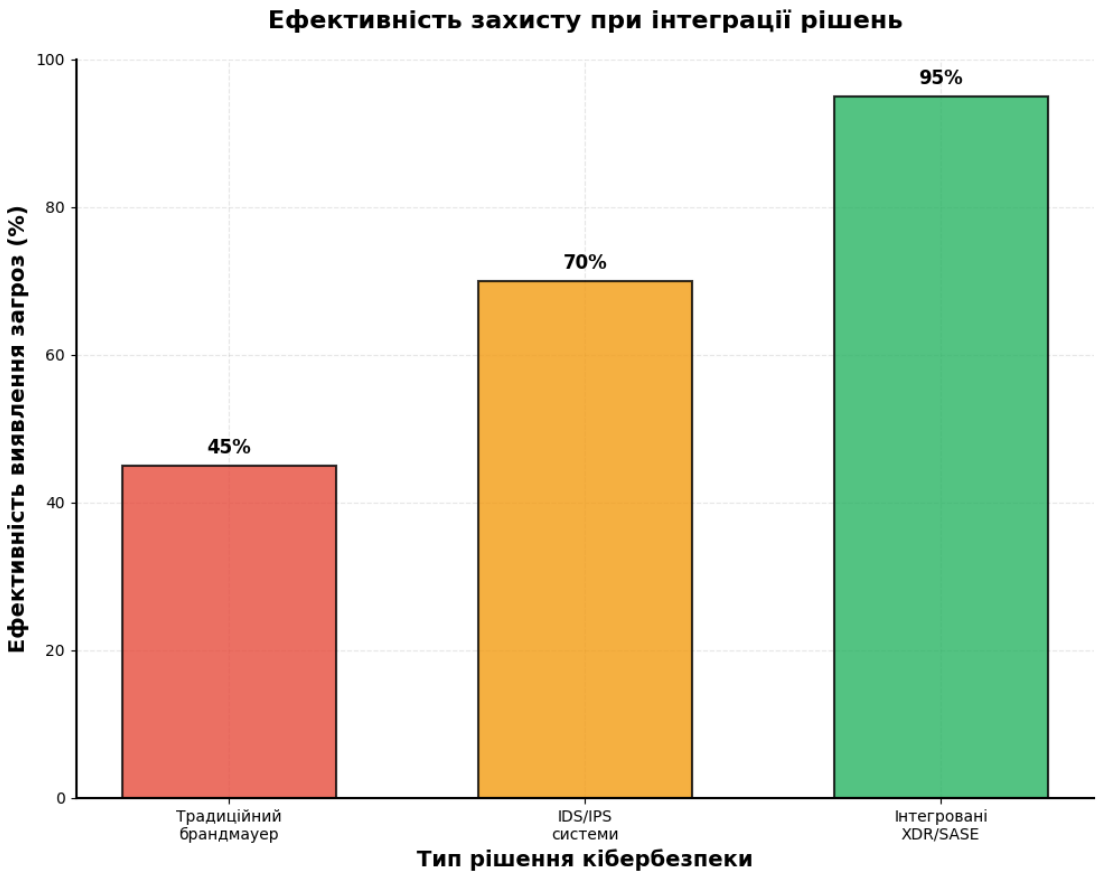

Рисунок 3.4 – Діаграма ефективності захисту при інтеграції рішень.

Можна виділити наступні найпопулярніші системи із застосуванням процесу інтеграції:

1. Платформа Microsoft Defender XDR, яка об’єднує захист хмарних сервісів, таких як Office 365 і Azure, із безпекою кінцевих точок, забезпечуючи цілісний моніторинг. При виявленні фішингової атаки система аналізує електронні листи, журнали доступу та поведінку пристроїв, ізолюючи уражений пристрій за 8 секунд. Додаткові функції, такі як автоматичне оновлення сигнатур і аналіз загроз на основі AI, дозволяють виявляти складні атаки, знижуючи ризик компрометації даних на 80%. Платформа оптимізує адміністрування завдяки єдиному інтерфейсу, зменшуючи навантаження на персонал.

2. Cisco SecureX інтегрує міжмережеві екрани, системи IDS/IPS і хмарну безпеку, створюючи єдину екосистему для захисту розподілених мереж. При DDoS-атаці система координує аналіз трафіку, блокуючи шкідливі запити за 4 хвилини, порівняно з годинами при ручному реагуванні. Інтеграція з хмарними сервісами, такими як Umbrella, забезпечує захист від атак на DNS-рівні, а централізована панель керування спрощує моніторинг, знижуючи операційні витрати на 30%. Автоматизація процесів реагування підвищує ефективність захисту великих організацій.

3. Платформа IBM QRadar із SOAR централізує аналіз безпеки, поєднуючи журнали мережі, хмари та кінцеві точки із автоматизацією реагування. При виявленні шкідливого трафіку система блокує IP-адреси та ізолює уражені вузли, знижуючи ризик витоку даних на 65%. SOAR-модуль виконує заздалегідь визначені дії, такі як оновлення правил міжмережевих екранів, за секунди, зменшуючи залежність від ручного втручання. Інтеграція AI для аналізу аномалій дозволяє виявляти невідомі загрози, підвищуючи стійкість критичної інфраструктури.

На рис. 3.5 діаграма порівнює три платформи (Microsoft Defender XDR, Cisco securex, IBM qradar із SOAR) за такими метриками як, точність виявлення, час реагування та зниження ризиків. IBM qradar із SOAR лідирує в точності (90%) і швидкості реагування (5 секунд) завдяки AI та автоматизації. Microsoft Defender XDR показує найвище зниження ризиків (80%) через комплексний захист хмари й кінцевих точок. Cisco securex має найдовший час реагування (240 секунд), але знижує ризики на 70% завдяки хмарній інтеграції. Діаграма допомагає організаціям оцінити платформи залежно від потреб, підкреслюючи сильні сторони кожної в реальних сценаріях.

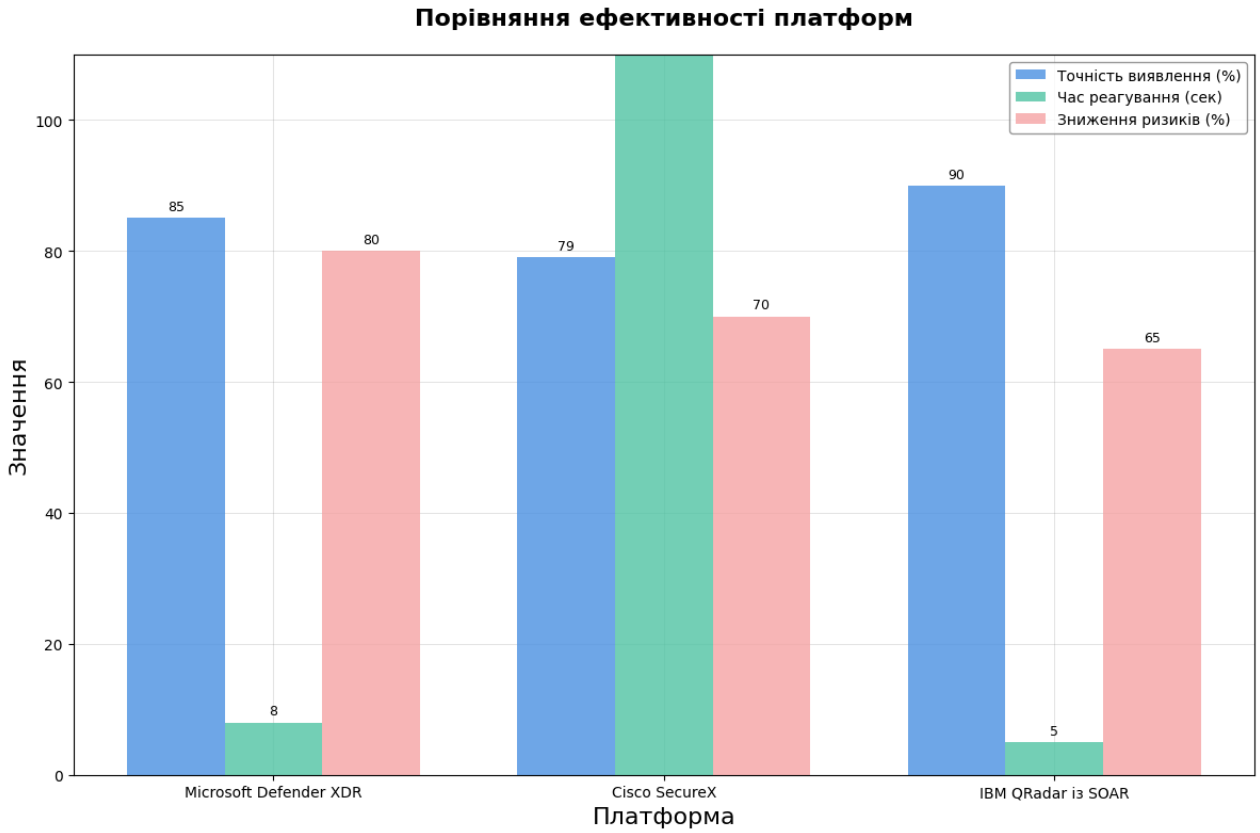

Рисунок 3.5 – Діаграма порівняння платформ за їх ефективністю

Аналіз дозволив сформулювати детальні рекомендації організаціям для підвищення ефективності кібербезпеки:

1. При інтеграції всіх рівнів захисту через XDR виникає комплексне виявлення загроз, адже вона об’єднує дані з мережі, хмари та кінцевих точок. Така платформа як Microsoft Defender XDR, аналізує поведінку і виявляє складні атаки за лічені секунди. Впровадження XDR зменшує кількість хибнопозитивних результатів на 50% порівняно з ізольованими IDS, дозволяючи зосередитися на реальних загрозах.

2. Впровадження SOAR скоротить час реагування, оптимізуючи ресурси. Платформи, такі як IBM QRadar SOAR, автоматизують дії, зокрема, блокування IP-адрес чи ізоляцію пристроїв, зменшуючи середній час реагування до 10 секунд. Автоматизація знижує навантаження на персонал, дозволяючи обробляти до 70% інцидентів без ручного втручання, що економить операційні витрати.

3. Регулярні тренінги з AI та кібербезпеки підвищать компетентність персоналу. Програми, такі як сертифікація SANS чи Cisco CyberOps, розвивають навички аналізу загроз і управління платформами XDR. Підвищення кваліфікації зменшує залежність від зовнішніх консультантів, скорочуючи витрати на підтримку на 20%. Тренінги також знижують ризик людських помилок, які спричиняють 30% інцидентів безпеки.

4. Моделювання атак оцінює ефективність процесу інтеграції, виявляючи слабкі місця. Проведення симуляцій фішингу чи DDoS-атак дозволяє оптимізувати правила кореляції в SIEM чи XDR, підвищуючи точність виявлення на 40%. Регулярне тестування забезпечує адаптацію до нових загроз, підтримуючи стійкість системи.

5. Використання SASE знижує витрати на обладнання, забезпечуючи захист розподілених мереж. Платформи, такі як Zscaler, об’єднують безпеку мережі та хмарний доступ, зменшуючи капітальні витрати на 35%. Хмарні рішення спрощують масштабування, дозволяючи адаптуватися до зростання трафіку без додаткових інвестицій.

На рис. 3.6 показано діаграму, яка ілюструє пріоритетність рекомендацій за їхнім впливом на ефективність кібербезпеки. Перехід до XDR має найбільший вплив 30% завдяки комплексному виявленню загроз і зниженню хибнопозитивних результатів. Автоматизація через SOAR забезпечує 25% впливу, скорочуючи час реагування та оптимізуючи ресурси. Навчання персоналу становить 20%, зменшуючи людські помилки та залежність від консультантів. Тестування систем (15%) підвищує точність завдяки симуляціям атак, а хмарні рішення (10%) знижують витрати та спрощують масштабування. Діаграма може допомогти визначити пріоритети впровадження, враховуючи рекомендації з найкращим впливом.

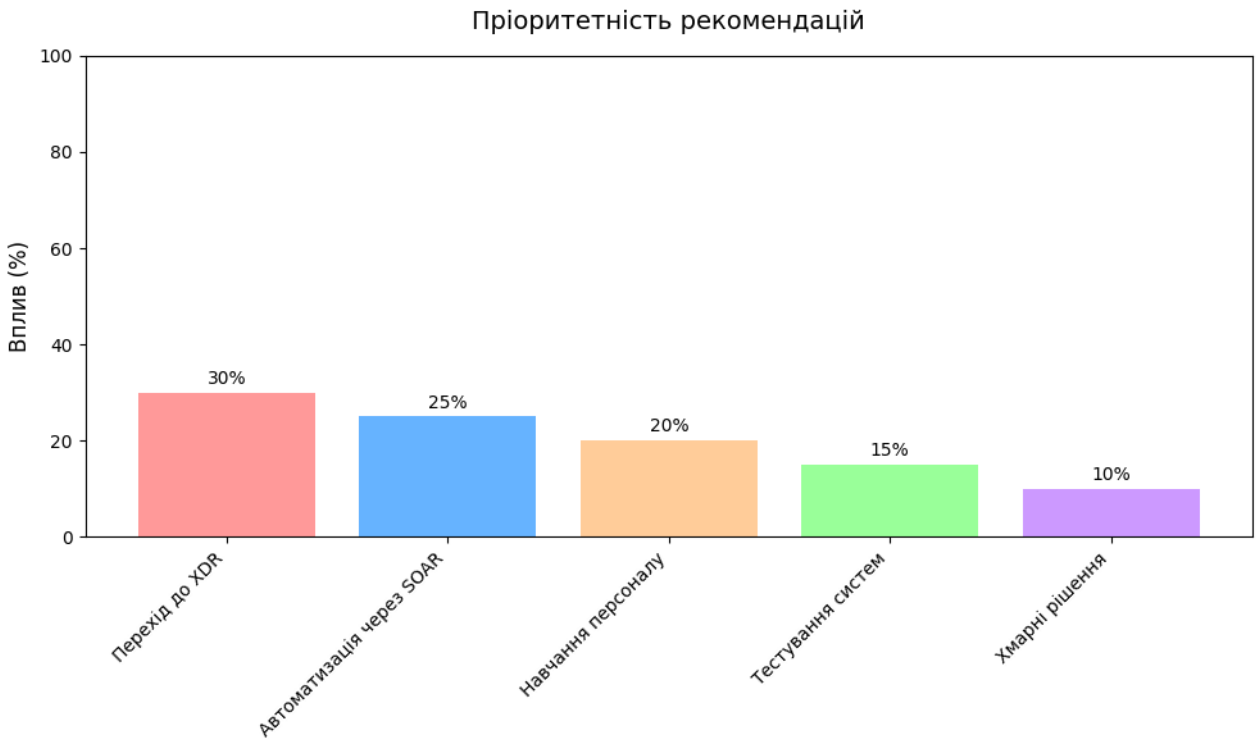

Рисунок 3.6 – Діаграма пріоритетності рекомендацій за впливом на ефективність

Інтеграція систем виявлення загроз у комплексні рішення кібербезпеки є стратегічним напрямом розвитку. Ізольовані інструменти не протистоять багаторівневим атакам, тоді як XDR і SASE забезпечують цілісний захист. Рекомендації оптимізують ресурси, підвищать ефективність і адаптують захист до нових загроз. Штучний інтелект і хмарні технології у майбутньому зроблять інтегровані системи більш адаптивними, що є ключовим для стійкості інформаційних систем.

ВИСНОВКИ

У рамках кваліфікаційної роботи проведено аналіз захисту комп’ютерних мереж і засобів виявлення кіберзагроз, що дозволило сформулювати наукові та практичні результати, а також розробити рекомендації щодо їх використання.

Сучасний стан кібербезпеки характеризується стрімким зростанням кількості та складності кіберзагроз, що зумовлено розвитком інформаційних технологій. Нові види атак, такі як програми-вимагачі, фішинг із використанням AI та складні цілеспрямовані атаки (APT), вимагають застосування інноваційних підходів до захисту. Традиційні методи захисту мереж часто виявляються недостатньо ефективними, що підкреслює необхідність інтеграції сучасних технологій виявлення та реагування на загрози.

Дослідження дозволило систематизувати сучасні кіберзагрози, класифікувавши їх за різними ознаками. Було визначено, що особливу небезпеку становлять організовані атаки, які потребують комплексного підходу до захисту. Аналіз методів захисту мереж показав, що комбінація таких засобів, як системи виявлення та запобігання вторгненням (IDS/IPS), віртуальні приватні мережі (VPN), криптографічні технології та управління доступом, є основою для забезпечення безпеки, але потребує доповнення інноваційними рішеннями.

Проведено оцінку принципів роботи IDS, зокрема хостових (HIDS) і мережевих (NIDS) систем, а також сигнатурних і аномальних методів. Встановлено, що аномальні методи, які базуються на аналізі відхилень, є ефективнішими для виявлення невідомих загроз. Порівняльний аналіз інструментів, таких як Snort, OSSEC, Wazuh, Wireshark і AlienVault OTX, показав, що кожен із них має унікальні переваги, які залежать від специфіки використання та потреб організації.

Запропоновано підходи до покращення методів виявлення кіберзагроз шляхом застосування технологій AI та ML, зокрема, алгоритмів Random Forest,

SVM і нейронних мереж. Ці технології дозволяють автоматизувати виявлення аномалій і прогнозувати потенційні загрози, що значно підвищує ефективність систем кібербезпеки. Також досліджено можливості інтеграції сучасних платформ, таких як XDR, SIEM і SOAR, які забезпечують комплексний підхід до моніторингу, аналізу та реагування на інциденти, хоча їх впровадження супроводжується технічними, організаційними та економічними викликами.

На основі одержаних результатів сформульовано рекомендації щодо науково-практичного використання. Для ефективного захисту від сучасних кіберзагроз доцільно впроваджувати комбіновані системи виявлення, які поєднують традиційні методи з технологіями AI/ML. Було розроблено рекомендації щодо підвищення ефективності кібербезпеки.

Результати дослідження можуть бути використані для розробки стратегій кібербезпеки в компаніях і організаціях, які прагнуть протистояти сучасним кіберзагрозам.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

karpova7. Що таке безпека мережі та які є способи її забезпечення?. *ISSP* (дата звернення: 09.12.2024).

ласифікація кіберзагроз та їх легітимація у нормативно-правових актах україни (дата звернення: 20.12.2025).

вний посібник з аналізу кіберзагроз – softico.ua. *softico.ua – Компания*

ро доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI: станом на 8 жовт. 2023р. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 25.01.2025).

тандарт кіберстійкості DigVel: як зробити Україну безпечнішою. *Lviv IT Cluster*. bezpechnishoyu/#:~:text=Міжнародні%20стандарти%20з%20кібербезпеки%20–%20це,а%20також%20дотримуватися%20законодавчих%20норм. (дата звернення: 26.02.2025).

(дата звернення: 10.03.2025).

охлов К.Д., Люта М.В. Віртуальні приватні мережі та їх роль у кібербезпеці. Матеріали XVII Студентської науково-практичної конференції студентів, аспірантів та молодих вчених за тематикою «Тенденції розвитку IT-технологій в Україні». 26-27 березня 2025 р., Черкаси, Україна. Черкаси : Черкаський державний фаховий бізнес-коледж, 2025. С. 71-74.

о таке AI для кібербезпеки? | Захисний комплекс Microsoft. *Microsoft – AI, Cloud,* ua/security/business/security-101/what-is-ai-for-cybersecurity#:~:text=Розуміння%20штучного%20інтелекту%20для%20кібербез

пеки&text=Основні%20сфери%20застосування%20ШІ%20для,створення%20та%20зворотну%20розробку%20сценаріїв. (дата звернення: 28.03.2025).

о таке моніторинг мережі – терміни та визначення з кібербезпеки. *VPN Unlimited* –

(дата звернення: 07.04.2025).

ажливість моніторингу мережі: продуктивність і безпека [2024] | Global YO. (дата звернення: 08.04.2025).

найкращих інструментів моніторингу мережевої безпеки для виявлення п

h

і

б

е

(дата звернення: 04.05.2025).

(дата звернення: 07.05.2025).

й

(дата звернення: 08.05.2025).

(дата звернення: 09.05.2025).

(дата звернення: 10.05.2025).

к

а– Назва з екрана. – (дата звернення: 10.05.2025).

V

(дата звернення: 11.05.2025).

(дата звернення: 12.05.2025).

р

д

о

Б

(дата звернення: 11.05.2025).

о

а

(дата звернення: 10.04.2025).

d