Міністерство освіти і науки України
Криворізький національний університет
Факультет інформаційних технологій
Кафедра комп’ютерних систем та мереж

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА
за спеціальністю 123 «Комп’ютерна інженерія»

Тема наукової роботи: МОДЕЛЬ ЗАХИСТУ ФУНКЦІОНАЛЬНОЇ ОРГАНІЗАЦІЇ ТА КОНФІГУРАЦІЇ ФІЗИЧНИХ КОМПОНЕНТІВ КОМП’ЮТЕРНИХ МЕРЕЖ

Виконав _____ Д. І. Біневський

Керівник роботи _____ Ю. О. Кумченко

Нормоконтроль _____ Д. І. Кузнєцов

Завідувач кафедри _____ А. І. Купін

Кривий Ріг
2024

Криворізький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерних систем та мереж

Ступінь вищої освіти магістр
Спеціальність 123 «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ
Завідувач кафедри, голова циклової комісії

_____ А. І. Купін

"____" _____ 20__ року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

_____
(прізвище, ім'я, по батькові)

1. Тема роботи _____
_____
_____

керівник роботи _____,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від "___"_____ 20__року №_

2. Строк подання студентом роботи _____

3. Вихідні дані до роботи _____
_____
_____
_____
_____

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)_____
_____
_____
_____
_____
_____

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)_____
_____
_____
_____
_____

6. Консультанти розділів роботи

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

7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Огляд літератури за тематикою та збір даних		
2	Проведення аналізу мереж на предмет захищеності системи та безпеки		
3	Підготовка та аналіз матеріалів першого розділу		
4	Розробка математичної моделі захисту та конфігурації фізичних компонентів мережі.		
5	Проведення соціологічного досліджування рівня знань щодо кібербезпеки		
6	Підготовка та аналіз матеріалів другого розділу		
7	Підготовка та аналіз матеріалів третього розділу		
8	Оформлення пояснювальної записки		

Студент _____ _____
(підпис) (прізвище та ініціали)

Керівник роботи _____ _____
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка: 106 сторінки, 50 рисунків, 8 таблиць, 2 додатка, 21 використаних джерел.

Об’єкт дослідження – функціональна організація та конфігурація фізичних компонентів комп'ютерних мереж, а також методи та засоби їх захисту. Аналіз потенційних загроз, що можуть впливати на структуру мережі, розробка моделі захисту, здатної забезпечити стійкість та надійність функціонування комп'ютерної мережі в умовах кіберзагроз.

Робота складається з трьох розділів.

Перший розділ присвячено аналізу фізичних компонентів мереж, огляду сучасних методів захисту та обґрунтуванню актуальності розробки нової моделі. Другий розділ розкриває питання моделювання, включаючи розробку математичної моделі захисту. У третьому розділі виконано практичну реалізацію, тестування та оцінку запропонованої моделі.

Ключові слова: КОМП’ЮТЕРНА МЕРЕЖА, БЕЗПЕКА, ЗАХИСТ, ФІЗИЧНІ КОМПОНЕНТИ МЕРЕЖІ, МАРШРУТИЗАТОР, КОМУТАТОР, СЕРВЕР, КІБЕРБЕЗПКА, КІБЕРЗАГРОЗИ.

Master’s work: 106 pages, 50 figures, 8 tables, 2 additions, 21 used sources.

Object of research – functional organization and configuration of physical components of computer networks, as well as methods and means of their protection. Analysis of potential threats that may affect the structure of the network, development of a protection model capable of ensuring the stability and reliability of the computer network in the face of cyber threats.

The paper consists of three sections.

The first section is devoted to the analysis of physical components of networks, a review of current protection methods and a justification of the relevance of developing a new model. The second section covers modelling issues, including the development of a mathematical model of protection. The third section describes the practical implementation, testing and evaluation of the proposed model.

Keywords: COMPUTER NETWORK, SECURITY, PROTECTION, PHYSICAL NETWORK COMPONENTS, ROUTER, SWITCH, SERVER, CYBER SECURITY, CYBER THREATS.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ 8
ВСТУП 9
1 ОПИС ФІЗИЧНИХ КОМПОНЕНТІВ КОМП'ЮТЕРНИХ МЕРЕЖ, ВИДИ ЗАГРОЗ ТА ЗАСОБИ ЇХ ПОМ'ЯКШЕННЯ.....13
1.1 Моделі захисту комп’ютерних мереж 13
1.1.1 Сегментація мережі 15
1.1.2 Брандмауер 17
1.1.3 Пісочниця (Sandbox).....18
1.2 Види загроз, кіберзагроз види сучасних способів атак та принцип їх роботи 18
1.2.1 Фішинг 20
1.2.2 Шкідливе програмне забезпечення.....21
1.2.3 Розподілені атаки на відмову в обслуговуванні (DDoS) 22
1.2.4 Захоплення корпоративного рахунку (CATO).....23
1.3 Активне мережеве обладнання.....23
1.4 Пасивне мереже обладнання.....25
Висновок до розділу 1 31
2 АЛГОРИТМИ ТА МЕТОДИ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ ДЛЯ ОЦІНКИ РІВНЯ ЗНАНЬ У СФЕРІ КІБЕРБЕЗПЕКИ". 32
2.1. Докладний опис методики проведених досліджень.....32
2.2. Вибір методів математичного моделювання для оцінки рівня знань у сфері кібербезпеки 34
2.3. Алгоритми класифікації користувачів за рівнем кібербезпеки 41
2.5. Аналіз результатів моделювання та їх вплив на рекомендації щодо підвищення кібербезпеки 44
2.6 Способи виявлення та передбачення загроз на основі штучного інтелекту 46
Висновок до розділу 2 51

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ЗАХИСТУ ФІЗИЧНИХ КОМПОНЕНТІВ КОМП'ЮТЕРНИХ МЕРЕЖ 52
3.1 Способи класифікації атак із позиції побудови систем їх виявлення 52
3.2 Моделювання методів побудови DMZ в Cisco Packet Tracer.....54
3.3 Налаштування політик безпеки 62
3.4 Створення DMZ через налаштування ACL на маршрутизаторі 63
Основні функції мережі.....65
3.5 Використання VPN-тунельних з'єднань для захисту локальних мереж: PPTP, L2TP та інші протоколи.....69
3.6 Безпека бездротових мереж: ключ до захисту ваших даних.....71
Висновок до розділу 3 94
ВИСНОВОК.....95
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....96

ПЕРЕЛІК СКОРОЧЕНЬ

1. **DMZ (Demilitarized Zone)** – сегмент комп'ютерної мережі, який відокремлює внутрішню мережу організації від публічної або незахищеної мережі (наприклад, Інтернет).
2. **LAN (Local Area Network)** – мережа, що покриває обмежену територію, наприклад, офіс або будівлю, і дозволяє пристроям обмінюватися даними на високій швидкості.
3. **WAN (Wide Area Network)** – мережа, що охоплює великі географічні області, часто з'єднуючи віддалені офіси або інші організації через публічні канали зв'язку.
4. **IP (Internet Protocol)** – протокол Інтернету, що використовується для маршрутизації та адресації даних у мережах.
5. **MITM (Man-In-The-Middle)** – атака, коли зловмисник перехоплює та змінює комунікацію між двома сторонами.
6. **DDoS (Distributed Denial of Service)** – атака, що перевантажує сервер або мережу великою кількістю запитів, унеможливлюючи доступ для легітимних користувачів.
7. **SQL (Structured Query Language)** – мова для взаємодії з базами даних. SQL-ін'єкція – вразливість, при якій зловмисник вводить шкідливий код для доступу до бази даних.
8. **SSL/TLS (Secure Sockets Layer / Transport Layer Security)** – протоколи для захищених з’єднань через Інтернет.
9. **RSA (Rivest–Shamir–Adleman)** – алгоритм асиметричного шифрування, що використовує пару ключів для забезпечення безпеки інформації.
10. **VPN (Virtual Private Network)** – віртуальна приватна мережа, яка забезпечує безпечне підключення через зашифровані тунелі.
11. **SaaS (Software as a Service)** – модель надання програмного забезпечення як сервісу через Інтернет.
12. **PCI DSS (Payment Card Industry Data Security Standard)** – стандарт безпеки для платіжних систем.

ВСТУП

Необережне поводження користувача може призвести до зараження комп'ютера вірусним, троянським або іншим шкідливим програмним забезпеченням, яке може пошкодити техніку або викрасти особисту інформацію. Неправильне користування Інтернетом робить користувача більш уразливим до фішингу. Необережне розголошення особистої інформації в Інтернеті може призвести до її неправомірного використання зловмисниками або до порушення конфіденційності даних.

Багато досліджень [1] присвячено цій актуальній темі: розглядалися приклади забезпечення безпеки власної локальної мережі, проблеми доступних ресурсів та сервісів, описувалися правила, яких слід дотримуватися. Отже, аналізуючи накопичену інформацію, можна розробити певний метод захисту та навчити користувачів його використовувати.

Перше з чого варто почати це уникати використання невідомих зовнішніх пристроїв для зберігання даних, таких як зовнішні *HDD/SSD/USB Flash Drive* накопичувачі, карти пам'яті, оптичні диски (*CD, DVD, Blu-ray*) тощо. Використання цих пристроїв може призвести до зараження комп'ютера вірусами або іншим шкідливим програмним забезпеченням.

Також підозрілі файли теж можуть задати значну шкоду вашому пристрою. Не відкривайте файли, електронні вкладення або архіви від недовірених джерел. Усе, що надходить від незнайомців, слід вважати потенційно небезпечним. Рекомендовано перенаправляти такі електронні листи в спам. Якщо ви знайомі з відправником, але не очікували від нього кореспонденції або файлів, зверніться до нього через інший комунікаційний канал для підтвердження. Це необхідно для виявлення можливого компрометування його акаунту. Наприклад, якщо ви отримали офіс документ через електронну пошту, зв'яжіться з відправником телефоном або через месенджер, щоб уточнити, чи дійсно він відправив вам цей файл [2].

Найбільш ризиковані типи файлів:

1) виконувані файли: *EXE, COM, CMD, BAT, PS1, ELF;*
2) скрипти та код: *JS, VBS, PY, PHP, SH;*
3) офісні документи з макросами: *DOCM, XLSM, PPTM;*
4) PDF з активним вмістом: *PDF;*
5) файли векторної графіки з вбудованим кодом: *SVG;*
6) архіви, особливо з авто-виконанням або захищені паролем: *ZIP, RAR, 7Z* [3].

Автор роботи брав участь у науковій конференції "XVII Всеукраїнська науково-практична WEB конференція аспірантів, студентів та молодих вчених «Комп’ютерні інтелектуальні системи та мережі» (26–28 березня 2024 р.) з темою "Захист функціональної організації та конфігурації фізичних компонентів комп’ютерних мереж" (Біневський Д. І., Кумченко Ю. О.). У цьому контексті важливим є питання безпеки користувачів Інтернету, адже необережне поводження може призвести до зараження комп’ютера вірусним, троянським або іншим шкідливим програмним забезпеченням. Неправильне користування Інтернетом робить користувача більш уразливим до фішингу, а необережне розголошення особистої інформації — до її неправомірного використання зловмисниками або до порушення конфіденційності даних.

Багато досліджень присвячено цій актуальній темі: розглядалися приклади забезпечення безпеки власної локальної мережі, проблеми доступних ресурсів та сервісів, описувалися правила, яких слід дотримуватися.

Отже, аналізуючи накопичену інформацію, можна розробити певний метод захисту та навчити користувачів його використовувати.

Актуальність досліджень. Сучасні комп’ютерні мережі є основою для функціонування різних організацій та інфраструктур, забезпечуючи передачу даних, управління процесами та доступ до інформаційних ресурсів. Разом із зростанням їх складності збільшується необхідність у надійному захисті, особливо фізичних компонентів, що становлять основу мережевої архітектури. Відтак, розробка ефективної моделі захисту функціональної організації та конфігурації фізичних компонентів є актуальним дослідженням, що сприятиме підвищенню безпеки і стійкості мережевих інфраструктур у сучасних умовах.

Мета і завдання дослідження. Метою цієї кваліфікаційної роботи є розробка моделі захисту функціональної організації та конфігурації фізичних компонентів комп'ютерних мереж, що дозволить зменшити ризики несанкціонованого доступу, збоїв у роботі мережевих компонентів та інших можливих загроз, а також побудова математичної моделі для оцінки рівня знань з кібербезпеки. Для досягнення поставленої мети необхідно виконати наступні завдання:

1. Провести аналіз існуючих методів і моделей захисту фізичних компонентів комп'ютерних мереж.
2. Розробити власну модель захисту функціональної організації мережевих компонентів та оцінити її ефективність.

Об'єкт дослідження. Об'єктом дослідження є комп'ютерні мережі з їх фізичними компонентами, що відповідають за забезпечення передачі даних, комунікацію та збереження інформації.

Предмет дослідження. Предметом дослідження є методи і моделі захисту функціональної організації та конфігурації фізичних компонентів комп'ютерних мереж, а також модель для оцінки рівня знань у сфері кібербезпеки

Методи досліджень. У роботі використані наступні методи досліджень: аналіз літературних джерел з метою вивчення існуючих моделей захисту; методи моделювання для побудови власної захисної моделі.

Наукова новизна одержаних результатів. Наукова новизна полягає у створенні нової моделі захисту функціональної організації та конфігурації фізичних компонентів комп'ютерних мереж, що враховує сучасні виклики інформаційної безпеки та спрямована на підвищення стійкості мережевої інфраструктури до зовнішніх загроз. Окремо важливим є використання штучного інтелекту для аналізу результатів опитування, що дає можливість отримати точніші висновки для покращення безпеки мережевих систем.

Практичне значення отриманих результатів. Розроблена модель захисту та модель тестування працівників може бути впроваджена в компанії та підприємства різної складності для зниження ризику несанкціонованого доступу до фізичних компонентів мережі, що дозволить забезпечити безперервність їх функціонування та захистити мережеву інфраструктуру від можливих атак та збоїв.

Апробація роботи. Біневський Д. І., Кумченко Ю. О. Захист функціональної організації та конфігурації фізичних компонентів комп’ютерних мереж. XVII Всеукраїнська науково-практична WEB конференція аспірантів, студентів та молодих вчених «Комп’ютерні інтелектуальні системи та мережі» : 26–28 березня 2024 р. : матер. Кривий Ріг, 2024. С. 41–46.

1 ОПИС ФІЗИЧНИХ КОМПОНЕНТІВ КОМП'ЮТЕРНИХ МЕРЕЖ, ВИДИ ЗАГРОЗ ТА ЗАСОБИ ЇХ ПОМ'ЯКШЕННЯ

1.1 Моделі захисту комп’ютерних мереж

Мережева безпека - це спосіб забезпечення безпеки інформаційно-технологічної системи, включаючи всю мережеву активність. Вона охоплює як комп'ютери, так і сервери. Доступ до Інтернету контролюється ефективним мережевим захистом, який виявляє і зупиняє різноманітні небезпеки, що поширюються в системі або отримують доступ до неї.

Різні рівні безпеки в системі, а також на рівні з'єднання об'єднуються, щоб сформувати мережеву безпеку. У кожному протоколі мережевої безпеки реалізовані стандарти та правила. Люди мають доступ до систем, в той час як хакери не можуть здійснювати атаки та використовувати вразливості.

Завдяки мережевій безпеці несанкціоновані особи не мають доступу до мережі та пов'язаних з нею пристроїв. Підозріла діяльність, збої в роботі, зловживання, руйнування, неналежне використання та зміна основної комунікаційної мережі захищені апаратними та програмними процедурами безпеки [1].

Мережева безпека забезпечує надійну основу для додатків, клієнтів і пристроїв, які можуть виконувати свої обов'язки в безпечному середовищі. Мережева інфраструктура підтримує довіру до бізнесу, захищаючи приватну інформацію від атак.

Небезпечно зосереджуватися на одному конкретному рівні захисту. Досвідчений зловмисник може зрештою подолати навіть простий захисний механізм. Тому що технології захисту надають доступ до системи та її сервісів лише авторизованим користувачам, відповідно до багатьох рівнів безпеки, які забезпечують дотримання правил та управління.

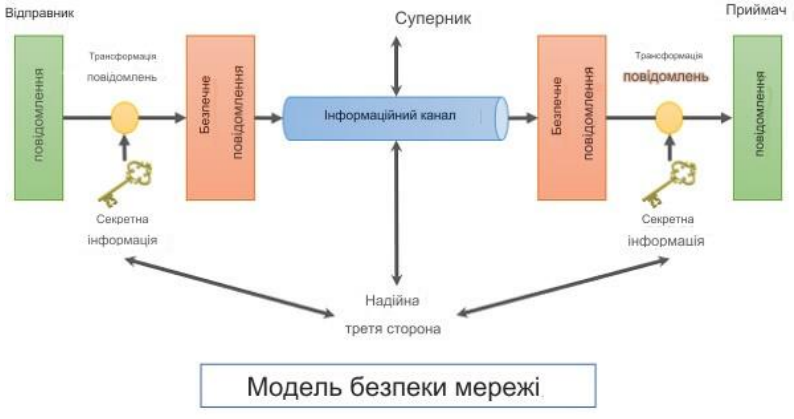


Рисунок 1.1 - Базова модель безпеки мережі

					КНУ.РМ.123.20.01.ВС		
Змн.	Арк.	№ документа	Підпис	Дата			
Розробив		Біневський			РОЗДІЛ 1	Літера	Аркуш	Аркушів
Перевірив		Кумченко						
						КІ-21м		
Н.контроль		Кузнєцов						
Затвердив		Купін						

Ефективна модель мережевої безпеки в комп'ютерних мережах має такі ключові аспекти:

1. Алгоритм шифрування кодує відкритий текст у зашифрований і декодує зашифрований текст назад у відкритий. Надійність алгоритму залежить від його здатності протистояти спробам злому зловмисниками.
2. Безпечна генерація, розповсюдження та використання секретного ключа, який передається виключно між сторонами, що спілкуються через комп'ютерну мережу. Довірена третя сторона сприяє обміну секретними ключами в моделі мережевої безпеки в CNS.
3. Комунікаційні протоколи дозволяють застосовувати вибране шифрування на основі секретного ключа для надання послуг безпеки, таких як конфіденційність, цілісність та автентифікація відправника.

Надійна модель мережевої безпеки складається з багаторівневих компонентів, які працюють разом для захисту конфіденційності, цілісності та доступності систем і даних. Ключові компоненти, які складають ефективну модель мережевої безпеки, включають в себе наступні: [2]

Таблиця 1.1 – Основні засоби безпеки

Засіб безпеки	Опис
Міжмережеві екрани (Firewall)	Міжмережеві екрани контролюють весь вхідний та вихідний трафік мережі і зупиняють віруси, хакерів та атаки DDoS відповідно до стандартів безпеки. Вони забезпечують периметрову безпеку через фільтрацію трафіку і блокують несанкціоновані спроби доступу.
Системи запобігання вторгнень (IPS)	IPS моніторять трафік для виявлення шкідливої активності, порушень політик, експлуатації вразливостей або загроз, які можуть пропустити міжмережеві екрани. Вони аналізують пакети даних і блокують атаки в режимі реального часу до заподіяння шкоди.
VPN (Віртуальні приватні мережі)	Віртуальні приватні мережі (VPN) забезпечують безпечні віддалені з'єднання для працівників та з'єднують розподілені сайти. Вони створюють зашифровані тунелі через публічні мережі, гарантуючи конфіденційність та цілісність даних.
Контроль доступу	Контроль доступу регулює доступ до мереж та систем через впровадження суворої аутентифікації, авторизації та обліку. Методи, такі як багатофакторна аутентифікація, доступ на основі ролей і контроль відповідності пристроїв, гарантують належний доступ до ресурсів.

Продовження таблиці 1.1

Шифрування даних	Шифрування даних захищає конфіденційну інформацію від несанкціонованого доступу або спроб модифікації. Дані зашифровуються за допомогою алгоритмів шифрування та ключів, забезпечуючи можливість їх прочитання лише для тих, хто має ключі для дешифрування.
Безпека кінцевих пристроїв	Захист кінцевих пристроїв за допомогою антивірусного програмного забезпечення, строгого контролю доступу та оновлення патчів допомагає запобігти зловмисним програмам, несанкціонованому доступу та атакам, спрямованим на кінцевих користувачів. Це запобігає загрозам проникати в мережі через кінцеві точки.
Моніторинг мережі	Постійний моніторинг за допомогою SIEM систем збирає та аналізує журнали активності мережі для швидкого виявлення можливих атак і аномальної поведінки, яка може свідчити про порушення. Це забезпечує видимість загроз.
Плани реагування на інциденти	Незважаючи на захист, порушення можуть статися, тому плани реагування на інциденти готують організації до належної реакції на події безпеки. Документи з описом ролей, відповідальності та дій є важливими для ефективного стримування порушень.

1.1.1 Сегментація мережі

Метод поділу комунікаційної мережі на різні підмережі з метою підвищення продуктивності та надійності відомий як сегментація мережі.

Сегментація мережі успішно усуває недоліки проектування і надзвичайно ускладнює зловмисникам завдання пошкодження всієї системи, розділяючи інфраструктуру на окремі обмежені частини.

Наприклад, якщо зловмисник отримує доступ до системи, він може спробувати переміщатися по ній, щоб отримати доступ до конфіденційних матеріалів і зловживати ними. Якщо структура є рівною, зловмисник може легко отримати контроль над усією мережею за допомогою простої точки доступу. Хоча пласка мережа забезпечує швидкий і надійний зв'язок, її латеральний доступ до компонентів робить їх надзвичайно вразливими в сучасному мережевому бізнесі [3].

1. Сегментація VLAN: Для поділу мереж зазвичай використовують віртуальні локальні мережі або підмережі. VLAN ділять мережу на кілька частин, які з'єднують сервери електронним способом. IP-адреси використовуються для поділу мережі на маски підмереж, які пов'язані між собою мережевими компонентами. Хоча ці методи ефективно розділяють систему, вони часто потребують значних зусиль і ними важче керувати.

2. Сегментація за допомогою брандмауерів: Системи безпеки, такі як брандмауери, є ще одним варіантом для забезпечення сегментації. У мережі брандмауери використовуються для створення локальних локацій, які відокремлюють різні відділи.

Підприємства, які прагнуть захистити складні мережі, звернулися до сегментації мережі як до найважливішої тактики.

Ось кілька переваг:

1. Покращений захист. Забезпечуючи перехресні недоліки безпеки, які перешкоджають латеральним кібератакам, сегментація мережі зменшує загрози. Як наслідок, якщо хакери проникають за вашу початкову лінію безпеки, вони обмежуються сегментом мережі, до якого намагаються отримати доступ.
2. Покращене управління мережею. Легше ізолювати проблеми і негайно виявляти небезпеки, коли ваша мережа розділена на впорядковані частини.
3. Підвищена ефективність роботи. Залежно від попиту, трафік обмежується певними зонами. Це зменшує загальну кількість адрес і клієнтів у певній підмережі, зменшуючи перевантаження та підвищуючи поточну ефективність.

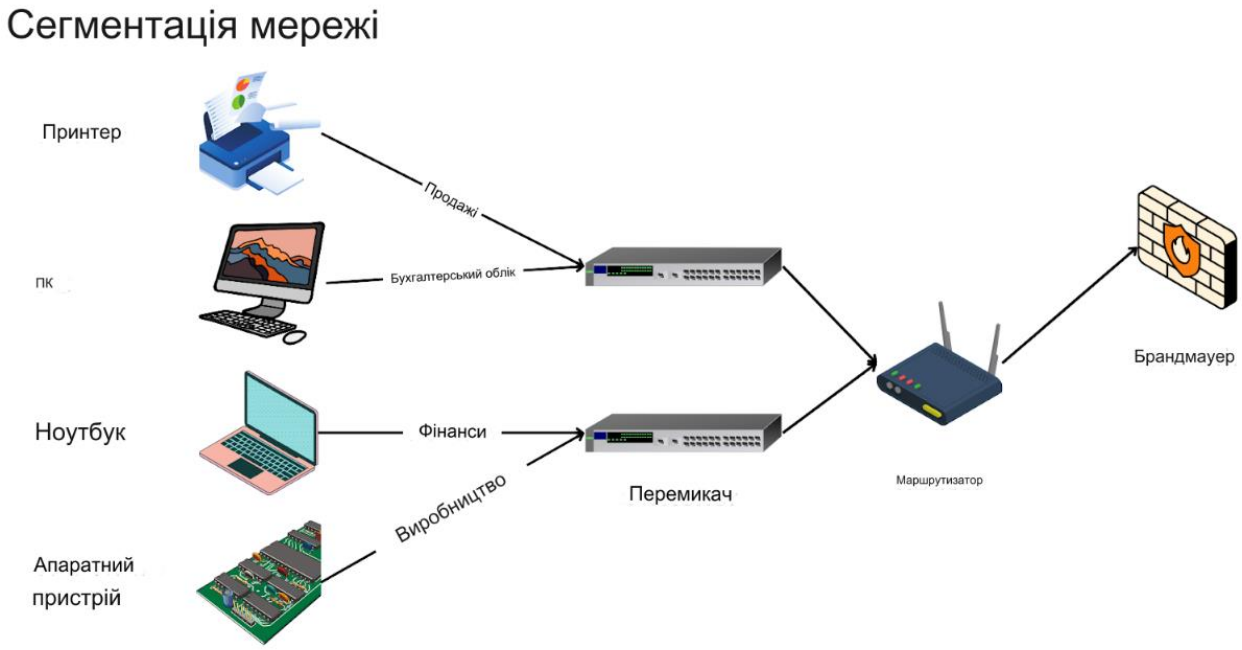


Рисунок 1.2 - Схема прикладу сегментації мережі

1.1.2 Брандмауер

Люди та організації повинні захищати свої дані, оскільки кількість кіберзлочинів зростає з кожним днем. Проте, для цього необхідно подолати кілька перешкод. Брандмауер - це архетип функції безпеки, яка може допомогти вам захистити вашу систему та пристрої від хакерів.

Брандмауери аналізують вхідний і вихідний трафік комп'ютера, шукаючи будь-які ознаки шкідливої поведінки. Якщо він відчує щось підозріле, він негайно зупинить його, не даючи наблизитися до своєї мети [4].

Брандмауери необхідні для мережевих і пакетних аналізаторів, які дозволяють або обмежують вхідний трафік, орієнтуючись на крихітний набір заздалегідь визначених критеріїв, коли вони були встановлені на початковому етапі. Їх досить просто обійти.

Брандмауери перетворилися на складні фрагменти коду, які набагато ефективніше запобігають небажаним вторгненням, і зараз вони є обов'язковим компонентом технології для всіх систем.

Брандмауери класифікуються відповідно до того, як вони працюють, і кожен тип може бути налаштований як програма або як апаратний пристрій. Існує шість основних типів брандмауерів, кожен з яких має власну операційну модель.

1. Брандмауери з фільтрацією пакетів
2. Проксі-сервери
3. Брандмауери нового покоління
4. NGFW, орієнтовані на загрози
5. Брандмауери з перевіркою стану
6. Шлюзи канального рівня
7. Брандмауери з уніфікованим управлінням загрозами (UTM)

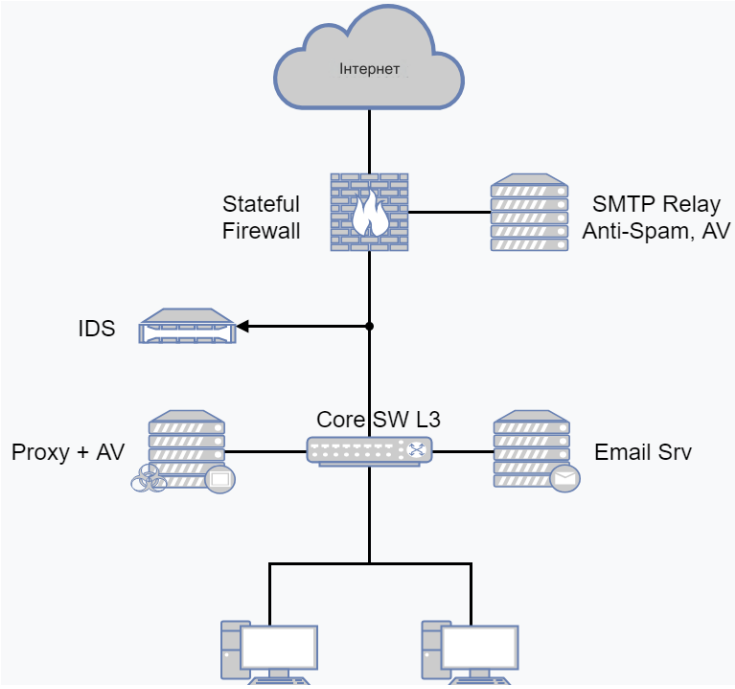


Рисунок 1.3 - Приклад NGFW

1.1.3 Пісочниця (Sandbox)

Пісочниця - це віртуальне представлення системи без мережевого підключення. Вона ізолює певну систему в іншій атмосфері. Середовище працює у своїх налаштуваннях, імітуючи комп'ютер. У разі витоку даних це захищає вашу систему та з'єднання.

Однак це процес симуляції всієї операційної системи. Він буде отримувати та запускати програми, щоб визначити свою мету. Можна продовжувати працювати з програмним забезпеченням у середовищі, якщо це ризиковано. Проте, завдяки ізоляції, воно не зможе вплинути на системи або будь-які інші типи обладнання в мережі.

Пісочниця може мати різні форми. Оскільки деякі компанії використовують пісочницю лише для моніторингу, вона також є чудовим ресурсом для багатьох інших цілей. Співпраця з програмами - це одна з таких цілей. Інтеграція багатьох збірок або елементів програми може бути складною.

Нижче наведено переваги пісочниці:

1. Пісочниця дозволяє протестувати додаток на придатність і переконатися, що він побудований належним чином.
2. Пісочниця є одним з найефективніших методів захисту бізнесу від хакерів, які намагаються отримати доступ до мережі або пошкодити її.
3. Пісочниця, незалежно від того, виконується вона в мережі чи на пристрої, забезпечує критично важливу безпеку. Деякі атаки, наприклад, можуть навіть не знищити комп'ютер або не мати очевидних наслідків, але вони можуть поступово знизити ефективність всієї системи зв'язку, затримуючи процедури і витрачаючи важливий час співробітників. Такі небезпеки можна запобігти, використовуючи пісочницю, яка дозволяє системі працювати точно за призначенням.

1.2 Види загроз, кіберзагроз види сучасних способів атак та принцип їх роботи

Кіберзагрози змінюються швидкими темпами. Тактика і методи атак змінюються і вдосконалюються щодня.

Кіберзлочинці отримують доступ до комп'ютера або мережевого сервера, щоб завдати шкоди, використовуючи кілька шляхів. Це також називається вектором атаки.

Найпоширеніші способи отримати доступ до комп'ютера або мережі включають:

1. Знімні носії, такі як флешки
2. Атака грубою силою з використанням методу спроб і помилок для розшифрування зашифрованих даних
3. Атаки через Інтернет або електронну пошту
4. Несанкціоноване використання системних привілеїв вашої організації

Типи кіберзагроз можуть бути наступні:

Таблиця 1.2 – Найпопулярніші типи кіберзагроз

Назва кіберзагрози	Опис	Частота зустрічі загрози (1-10)
Фішинг	Спосіб атаки, при якому шахраї намагаються отримати конфіденційну інформацію (логіни, паролі, номери карток) через підроблені вебсайти або електронні листи.	9
DDoS-атака (Розподілена відмова в обслуговуванні)	Нападники перевантажують сервер або мережу великою кількістю запитів, що призводить до неможливості обслуговування легітимних користувачів.	8
Шкідливе ПЗ (Malware)	Програми, які виконують зловмисні дії на пристроях жертви, такі як крадіжка даних або порушення роботи систем. Приклади: віруси, трояни, шпигунські програми.	9
Вимагачі (Ransomware)	Віруси, які блокують доступ до файлів або системи, вимагаючи викуп за їх розблокування.	7
Соціальна інженерія	Маніпуляції з метою обману користувачів для отримання доступу до конфіденційної інформації або систем без використання технічних засобів.	8
SQL-ін'єкція	Атака, яка полягає у введенні шкідливого SQL-коду в вебдодаток з метою отримання доступу до бази даних або її зміни.	6
MITM (Атака "людина посередині")	Атака, при якій зловмисник перехоплює та змінює комунікацію між двома сторонами без їхнього відома.	5
Кейлогери	Програми, що записують натискання клавіш на клавіатурі, щоб зловмисники могли отримати доступ до паролів та іншої конфіденційної інформації.	4
Злом паролів (Brute Force)	Спосіб атаки, при якому зловмисники намагаються зламати паролі шляхом послідовного підбору різних комбінацій.	6
Шахрайство з SIM-картами (SIM Swapping)	Заміна SIM-карти користувача, щоб отримати контроль над його обліковими записами через телефонні сервіси.	5

1.2.1 Фішинг

Фішинг — це одна з найпоширеніших та найбільш успішних кіберзагроз, метою якої є обман користувача для отримання його конфіденційної інформації (логіни, паролі, номери банківських карт, персональні дані тощо). Зловмисники маскуються під легітимні організації або відомі сервіси, надсилаючи підроблені електронні листи, повідомлення або створюючи фальшиві вебсайти, які візуально майже не відрізняються від справжніх [5].

Основні види фішингу:

1. **Email-фішинг.** Найпоширеніший метод, коли зловмисники надсилають електронні листи, що імітують повідомлення від банків, платіжних систем, поштових сервісів або соцмереж, із проханням ввести свої облікові дані.
2. **Spear-фішинг.** Цей вид спрямований на конкретних осіб або організації. Зловмисники ретельно вивчають жертву та надсилають персоналізовані повідомлення, що підвищує шанси на успішну атаку.
3. **Голосовий фішинг.** Зловмисники використовують телефонні дзвінки, щоб виманити конфіденційну інформацію, видаючи себе за представників служб підтримки або банків.
4. **SMS-фішинг.** Атака через текстові повідомлення, що містять посилання на фальшиві вебсайти або спонукають користувачів до дзвінка на шахрайські номери.
5. **Clone-фішинг.** Зловмисник копіює легітимний лист або повідомлення, змінює лише посилання або вкладення, щоб перенаправити користувача на шкідливий ресурс.

Фішинг працює через обман користувачів, коли зловмисники надсилають підроблені електронні листи, повідомлення або створюють фальшиві вебсайти, що нагадують справжні сервіси (банки, соцмережі тощо). Метою є змусити користувача ввести свої дані, такі як логіни, паролі чи банківські реквізити. Після цього зловмисники використовують отриману інформацію для крадіжки грошей, доступу до акаунтів або інших зловмисних дій.

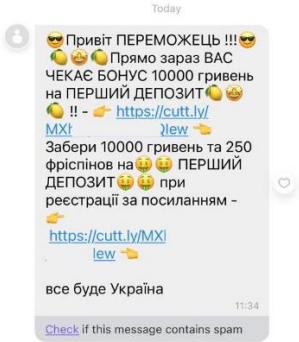


Рисунок 1.4 - Приклад фішингового повідомлення

1.2.2 Шкідливе програмне забезпечення

Шкідливе програмне забезпечення - це програма, яка вставляється в систему, щоб порушити конфіденційність, цілісність або доступність даних. Це робиться таємно і може вплинути на дані, програми або операційну систему. Шкідливе програмне забезпечення стало однією з найбільш значущих зовнішніх загроз для систем. Шкідливе програмне забезпечення може спричинити широкомасштабну шкоду і збої в роботі, і вимагає величезних зусиль в більшості організацій.

Шпигунське програмне забезпечення, призначене для порушення конфіденційності, також стало серйозною проблемою для організацій. Хоча шкідливе програмне забезпечення, що порушує конфіденційність, використовується вже багато років, останнім часом воно стало набагато більш поширеним. Шпигунські програми проникають у багато систем, щоб відстежувати особисту діяльність і здійснювати фінансові махінації.

Організації також стикаються зі схожими загрозами від декількох форм загроз, не пов'язаних зі шкідливим програмним забезпеченням. Ці форми кіберзагроз часто асоціюються зі шкідливим програмним забезпеченням. Більш поширеною формою є фішинг. Фішинг полягає в тому, щоб обманом змусити людей розкрити конфіденційну або особисту інформацію.

Кілька прикладів відомого шкідливого програмного забезпечення:

1. **WannaCry**

Це вірус-вимагач (ransomware), який поширювався у 2017 році та атакував комп'ютери з операційною системою Windows. Він шифрував дані користувачів і вимагав викуп за розшифровку. WannaCry використовував вразливість у системі Windows під назвою EternalBlue.

2. **NotPetya**

Спочатку виглядав як вірус-вимагач, але виявилося, що його основна мета — знищення даних. Атака NotPetya була спрямована на компанії, і найбільше постраждали підприємства в Україні у 2017 році. Вірус поширювався через оновлення бухгалтерської програми.

3. **Zeus**

Це троянський вірус, який використовувався для крадіжки банківських даних через зараження комп'ютера жертви. Він поширювався через шкідливі електронні листи і вебсайти. Після інфікування Zeus записував дані, які вводилися в браузері, включаючи паролі та інформацію про кредитні картки.

Рисунок 1.5 - Вірус WannaCry

1.2.3 Розподілені атаки на відмову в обслуговуванні (DDoS)

DDoS-атаки роблять онлайн-сервіс недоступним, перевантажуючи його надмірним трафіком з багатьох місць і джерел. Час відгуку веб-сайту сповільнюється, що унеможливлює доступ до нього під час DDoS-атаки. Кіберзлочинці створюють великі мережі заражених комп'ютерів, так звані ботнети, шляхом розповсюдження шкідливого програмного забезпечення. DDoS-атака може не бути основним кіберзлочином. Атаки часто створюють відволікаючий маневр, в той час як здійснюються інші види шахрайства та кібервторгнення.

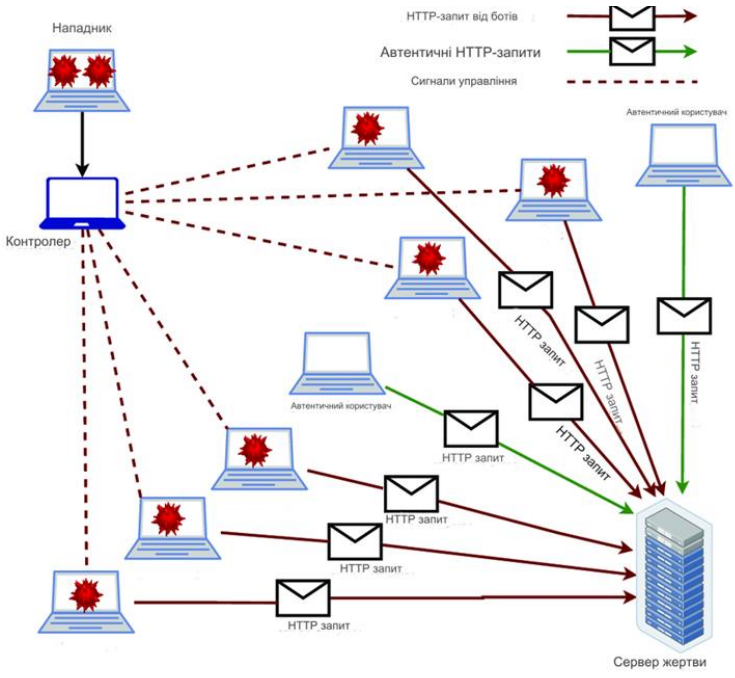


Рисунок 1.6 - Приклад типової DDoS атаки

1.2.4 Захоплення корпоративного рахунку (CATO)

CATO - це крадіжка бізнес-суб'єктів, коли кіберзлодії видають себе за компанію та надсилають несанкціоновані банківські перекази та ACH-транзакції. Несанкціоновані кошти надсилаються на рахунки, контрольовані кіберзлочинцем.

Багато підприємств є вразливими до атак CATO. Установи зі слабким комп'ютерним захистом і мінімальним контролем над системами онлайн-банкінгу є легкою мішенню. Ця форма кіберзлочинності може призвести до великих збитків. Кіберзлочинці використовують шкідливе програмне забезпечення для зараження комп'ютера через електронну пошту, веб-сайти або шкідливе програмне забезпечення, замасковане під програмне забезпечення. [6]

1.3 Активне мережеве обладнання

Активне мережеве обладнання — це група пристроїв, які виконують низку інтелектуальних функцій, таких як прийом, передача, розподіл і перенаправлення сигналів. Важливою особливістю таких пристроїв є те, що вони працюють від електричної мережі.

Такі пристрої також здатні створювати канали передачі даних і ефективно розподіляти навантаження між елементами мережі. Саме тому правильний вибір активного мережевого обладнання є ключовим для забезпечення безперебійної та надійної роботи всієї мережевої інфраструктури.

Активне мережеве обладнання включає такі типи пристроїв:

1. Маршрутизатори (роутери);
2. Комутатори (switch);
3. Точки доступу (Access Points);
4. Модеми;
5. Сервери;
6. VoIP.

Маршрутизатори (роутери) — це мережеве обладнання, яке забезпечує обмін даними між різними мережами, визначаючи найкращі шляхи для їх передачі. Вони аналізують дані, що надходять, і використовують таблиці маршрутизації для визначення оптимального маршруту до цільового пристрою. Маршрутизатори також можуть виконувати інші функції, такі як управління трафіком, забезпечення безпеки (через брандмауери), надання доступу до Інтернету і підтримка різних протоколів маршрутизації.

Комутатори (switch**)** — це мережеве обладнання, яке використовується для з'єднання пристроїв у межах локальної мережі (LAN). Вони забезпечують передачу даних між пристроями на основі їх MAC-адрес. Комутатори приймають вхідні дані, аналізують MAC-адресу відправника та отримувача, і надсилають дані тільки на порт, до якого підключено пристрій з відповідною MAC-адресою. Це дозволяє зменшити мережеве навантаження та підвищити ефективність передачі даних у локальній мережі. Комутатори також можуть підтримувати функції VLAN (віртуальні локальні мережі), забезпечуючи логічну сегментацію мережі.

Точки доступу (Access Points) — це пристрої, які забезпечують бездротове підключення до мережі для пристроїв через Wi-Fi. Вони функціонують як міст між бездротовими і дротовими мережами, дозволяючи бездротовим пристроям (ноутбукам, смартфонам, планшетам тощо) підключатися до локальної мережі (LAN) або Інтернету. Точки доступу передають та приймають дані через радіохвилі і можуть підтримувати різні стандарти Wi-Fi (таких як 802.11a/b/g/n/ac/ax), що визначають швидкість і діапазон бездротового з'єднання. Вони також можуть забезпечувати функції безпеки, такі як шифрування даних (WEP, WPA, WPA2) і контроль доступу.

Брандмауери (Firewall) — це мережеве обладнання або програмне забезпечення, яке контролює доступ до мережі та захищає її від зовнішніх загроз. Брандмауери аналізують вхідний і вихідний мережевий трафік на основі налаштованих правил безпеки, що дозволяє блокувати або дозволяти трафік відповідно до політик безпеки. Вони можуть забезпечувати захист від небажаних підключень, атак з мережі, вірусів та іншого шкідливого ПЗ. Брандмауери можуть бути розгорнуті на різних рівнях: на прикладі, як в мережевих маршрутизаторах (апаратні брандмауери), або як частина програмного забезпечення на окремих комп'ютерах (програмні брандмауери).

Модеми — це пристрої, які перетворюють сигнали з однієї форми (аналогової) на іншу (цифрову) і навпаки, для забезпечення підключення до Інтернет-провайдера. Модеми виконують функцію модуляції (перетворення цифрових сигналів комп'ютера в аналогові сигнали для передачі по телефонних лініях або інших аналогових каналах) і демодуляції (перетворення отриманих аналогових сигналів назад у цифрові сигнали). Це дозволяє передавати дані між пристроєм і провайдером через телефонні лінії, кабельні канали, оптоволоконні лінії або інші види з'єднань. Сучасні модеми можуть підтримувати різні технології та стандарти, такі як DSL, кабельні модеми, оптоволоконні модеми та мобільні модеми. Вони можуть також включати додаткові функції, такі як маршрутизація та бездротовий зв'язок, вбудовані в один пристрій.

Сервер — це спеціалізований комп’ютер або програма, що обробляє запити і передає дані іншим пристроям через мережу. Основні функції серверів включають:

1. Зберігання даних: зберігання файлів і баз даних.
2. Обробка веб-сторінок: перегляд і взаємодія з веб-контентом.
3. Управління електронною поштою: обробка та пересилання електронних листів.
4. Управління доменами: переклад доменних імен в IP-адреси.
5. Підтримка програм і додатків: надання ресурсів для онлайн-сервісів і програм.

VoIP-обладнання — це пристрої або програмне забезпечення, які використовуються для передачі голосових даних через IP-мережі, такі як Інтернет або локальні мережі. VoIP (Voice over Internet Protocol) дозволяє здійснювати голосові дзвінки, використовуючи протоколи IP для передачі голосу в цифровій формі, що може знижувати витрати на зв'язок і покращувати якість звуку в порівнянні з традиційними телефонними системами.

Медіаконвертери — це пристрої, які використовуються для перетворення типу мережевих з'єднань між різними середовищами передачі даних. Вони забезпечують можливість підключення мережевих пристроїв, що використовують різні типи фізичних медіа (наприклад, мідні кабелі і оптичні волокна).

Мережевий трансивер або **SFP (Small Form-Factor Pluggable) модуль** — це компактний, знімний компонент, який використовується для підключення мережевих пристроїв, таких як комутатори або маршрутизатори, до різних типів оптичних або мідних кабелів.

1.4 Пасивне мереже обладнання

Пасивне мережеве обладнання, на відміну від активного, не споживає електроенергію і виконує функції передачі даних безпосередньо через кабелі та оптичні волокна. Це обладнання є ключовим елементом мережевої інфраструктури, забезпечуючи фізичне з'єднання між пристроями. Правильний вибір пасивного обладнання допомагає підвищити надійність мережі, знизити ризик поломок і оптимізувати витрати на встановлення та експлуатацію активного обладнання. В результаті мережа стає більш стабільною і довговічною.

До пасивного обладнання належать різні компоненти, що забезпечують фізичну організацію та підключення мережевих пристроїв. Серед них:

1. Оптичні патч-панелі
2. Кабельні організатори
3. Оптичні муфти
4. Інформаційні розетки
5. Мідні та оптичні патч-корди
6. Оптичні бокси та сплайс-касети
7. Монтажні та телекомунікаційні шафи і стійки

Монтажні шафи поділяються на типові, спеціалізовані та антивандальні, а також за типом монтажу – на настінні та долівкові.

Комутаційні шафи, як правило, збірного типу, призначені для організації кабельної розводки. Вони використовуються для монтажу кабельних збірок, оптоволоконних систем, кросів, спліттерів та іншого пасивного обладнання.

Серверні шафи призначені для підключення активного обладнання, зокрема роутерів, патч-панелей, комутаторів, маршрутизаторів та станцій зв'язку. Їх основна функція — розміщення і захист мережевого обладнання в умовах підвищеного ризику пошкодження.

Рисунок 1.7 - Hypernet

Витий кабель (Twisted pair) – вид кабелю, що складається з однієї або декількох пар провідників, які звиті один з одним. Провідники скручуються з метою мінімізації зовнішнього електромагнітного впливу [7].

Рисунок 1.8 - Витий кабель UTP Cat.5e виробник одескабель

Він буває:

1. **Екранованим STP (Shielded Twisted Pair)** – використовується у середовищах з високим рівнем електромагнітних завад
2. **Неекранованим UTP (Unshielded Twisted Pair)** – підходить для умов з низьким рівнем завад, наприклад, у офісах або житлових приміщеннях.
3. **Кабель з екраном і фольгою SFTP (Shielded Foiled Twisted Pair)** – поєднує екранування кожної пари фольгою (Foiled) і загальний екран для всього кабелю (Shielded). Використовується в умовах із високим рівнем електромагнітних завад, забезпечуючи максимальний захист сигналу.

Мідні кабелі поділяються на вуличні **(Outdoor)** і для приміщень **(Indoor)**, залежно від місця прокладання. Вони відрізняються, зокрема, товщиною зовнішньої оболонки, що впливає на їх стійкість до зовнішніх умов.

За швидкістю передач інформації витий кабель ділиться на наступні категорії:

1. **CAT 1, CAT 2, CAT 3**: кабелі цих категорій мають низьку пропускну здатність і використовуються переважно для телефонії. Вони підтримують передачу голосу та даних на невеликих швидкостях, не перевищуючи 10 Мбіт/с.
2. **CAT 4**: пропускна здатність до 16 Мбіт/с. Ця категорія раніше використовувалася в мережах Token Ring, але на сьогодні втратила актуальність через низьку швидкість і застарілість технології.
3. **CAT 5** забезпечує передачу даних зі швидкістю до 100 Мбіт/с при використанні двох пар провідників.
4. **CAT 5e** (Enhanced) – удосконалена версія CAT 5, підтримує швидкість до 1000 Мбіт/с (1 Гбіт/с) при використанні чотирьох пар провідників. Ця категорія широко використовується в сучасних локальних мережах, оскільки забезпечує стабільну та надійну передачу даних.
5. **CAT 6**: підтримує швидкість передачі від 1000 Мбіт/с до 10 Гбіт/с на коротких відстанях (до 50 м). Смуга пропускання — 250 МГц. Вона краще захищена від перешкод і сигналів затухання в порівнянні з CAT 5e.
6. **CAT 6a**: підтримує швидкість до 10 Гбіт/с на відстані до 100 метрів. Має смугу пропускання 500 МГц і зазвичай оснащується додатковим екраном, що зменшує вплив електромагнітних завад.
7. **CAT 7**: забезпечує швидкість до 10 Гбіт/с і має смугу пропускання 700 МГц. Характеризується наявністю загального екрану і додаткового захисту навколо кожної групи провідників, що робить його ще більш стійким до перешкод і сигналів затухання.

Мідний патч-корд використовується для з'єднання розподільних пристроїв у структурованих кабельних мережах. Зазвичай оснащений роз'ємами RJ-45 і забезпечує з'єднання між компонентами мережі.

Рисунок 1.9 - Оптоволоконний кабель

Волоконна оптика стала стандартом у телекомунікаційній індустрії, забезпечуючи високу ефективність і стабільність з'єднань через передачу даних за допомогою світлових сигналів. Це означає, що оптоволоконний інтернет працює за допомогою світла, а не електрики. Таке інноваційне рішення в галузі зв'язку забезпечує високу ефективність та стабільність інтернет-з'єднань.

Оптичний патчкорд – це важлива складова сучасних структурованих кабельних систем. Зовні він представляє собою відрізок оптичного кабелю довжиною від 50 сантиметрів до 100 метрів, обтиснений з обох кінців конекторами стандарту LC, SC, ST, або MTP/MPO (Multi-fiber Push On/Multi-fiber Push Off). Ці конектори забезпечують з'єднання між оптичними пристроями, такими як комутатори, маршрутизатори, або оптичні розподільчі панелі.

Рисунок 1.10 - Оптичний патчкорд

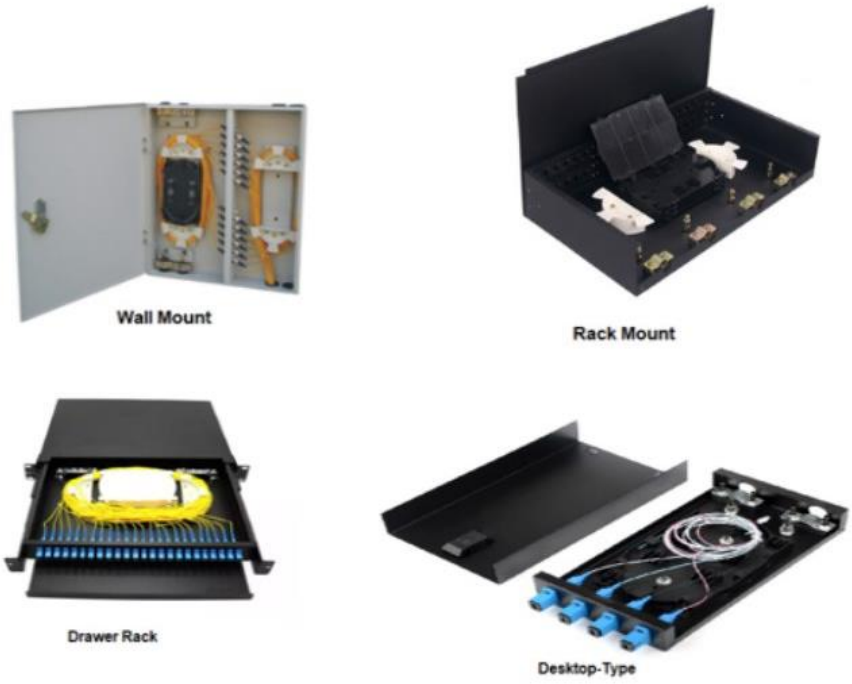


Рисунок 1.11 - Оптичний бокс

Рисунок 1.12 - Оптоволоконна коробка

Кабельний організатор – важливий елемент для впорядкування і зберігання зайвих патч-кордів. Він допомагає зменшити вигини кабелів під час укладки і знижує навантаження на місця підключення, рівномірно розподіляючи вагу через свою конструкцію.

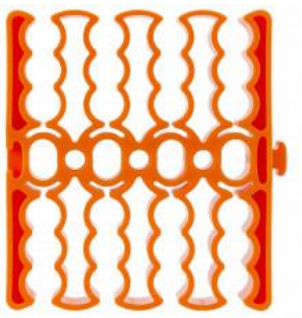


Рисунок 1.13 - Організатор кабелю

Патч-панель організовує кабелі в структурованій кабельній інфраструктурі. Зазвичай це стандартна стійкова панель шириною 19 дюймів із серією роз'ємів RJ-45, яка служить точкою з'єднання для мережевих кабелів, що виходять з комутаційної шафи та прокладаються горизонтально до настінних панелей у робочих зонах. Патч-панелі використовуються для підключення кабелів від окремих кінцевих пристроїв, таких як комп'ютери та сервери, доцентрального вузла, де їх можна під'єднати до іншого обладнання за допомогою патч-кабелів

Рисунок 1.14 - Патч панель

Рисунок 1.15 - Оптична патч панель

Оптичні патч-панелі також є пристроями для організації та комутації оптичних волокон у мережах. Вони надають зручний спосіб підключати та з'єднувати оптичні кабелі, що дозволяє централізовано керувати великою кількістю волокон.

Висновок до розділу 1

Під час науково-дослідної практики були отримані навички аналізу фізичних компонентів комп'ютерних мереж, їхньої побудови та функціонування. Вивчені сучасні моделі захисту комп'ютерних мереж, такі як сегментація мережі, що використовується для поділу мереж на ізольовані сегменти з метою зменшення ризиків, брандмауери для контролю та фільтрації трафіку, а також пісочниці (Sandbox), які забезпечують безпечне середовище для аналізу потенційно шкідливих програм.

Окремо були досліджені види кіберзагроз та принципи їхньої роботи. Серед них фішинг, який спрямований на викрадення конфіденційних даних через обманні методи, шкідливе програмне забезпечення, що завдає шкоди системам, розподілені атаки на відмову в обслуговуванні (DDoS), які перевантажують мережеві ресурси, та захоплення корпоративних рахунків (CATO), що може спричинити суттєві збитки для компаній.

Також були отримані практичні знання щодо компонентів побудови локальних мереж. Досліджено активне мережеве обладнання, таке як маршрутизатори, комутатори та точки доступу, що відповідають за передачу даних та управління трафіком. Окрім того, вивчено пасивне мережеве обладнання, включаючи кабелі, роз'єми та патч-панелі, які забезпечують фізичну інфраструктуру для передачі сигналів.

Завдяки науково-дослідній практиці було значно поглиблено розуміння технологій побудови та захисту комп'ютерних мереж, що є ключовими елементами забезпечення стабільності та безпеки інформаційних систем.

2 АЛГОРИТМИ ТА МЕТОДИ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ ДЛЯ ОЦІНКИ РІВНЯ ЗНАНЬ У СФЕРІ КІБЕРБЕЗПЕКИ".

2.1. Докладний опис методики проведених досліджень

Для оцінки рівня знань у сфері кібербезпеки серед респондентів було проведено соціальне опитування, що дозволило зібрати дані від 300 учасників. Методика дослідження була розроблена з урахуванням цілей, завдань та специфіки досліджуваної теми. Дослідження включало кілька етапів [8].

Основною метою дослідження було визначення рівня обізнаності респондентів про кібербезпеку та виявлення основних факторів, що впливають на їх знання. Завданнями дослідження стали:

1. Визначення структури запитань для опитування.
2. Збір даних за допомогою соціального опитування.
3. Аналіз отриманих даних та побудова математичної моделі для оцінки рівня знань.

Анкета була розроблена таким чином, щоб максимально охопити різні аспекти знань у сфері кібербезпеки. Вона складалася з трьох основних частин:

1. ***Загальна інформація.***
   Вік, стать.

2. ***Запитання про кібербезпеку.***
   Закриті запитання, які передбачали вибір однієї або декількох відповідей. Це включало питання про знання загроз (віруси, фішинг, шкідливе програмне забезпечення), методи захисту (антивіруси, брандмауери) та найкращі практики безпеки (управління паролями, безпечне користування Інтернетом).

3. ***Відкриті запитання.***
   Запитання, що дозволяли респондентам вільно висловлювати свої думки та рекомендації щодо покращення обізнаності в цій сфері.

Загальна інформація включала запитання про вік та стать респондентів, що дозволяло краще зрозуміти демографічні характеристики опитуваних. У рамках запитань про кібербезпеку було використано закриті питання, що передбачали вибір однієї або кількох відповідей. Респонденти мали можливість висловити своє знання про основні загрози, такі як віруси, фішинг і шкідливе програмне забезпечення, а також методи захисту, включаючи антивіруси, брандмауери та інші інструменти. Крім того, розглядалися найкращі практики безпеки, зокрема управління паролями та безпечне користування Інтернетом.

Опитування охопило респондентів з різних соціальних та професійних груп. Анкети були розповсюджені через онлайн-платформи, що забезпечило легкість доступу для учасників. Для залучення більшої кількості респондентів було використано соціальні мережі, електронні листи та фахові спільноти.

Для проведення соціального опитування було обрано платформу Google Форми, що забезпечило зручність та ефективність в організації збору даних. Google Форми дозволяють створювати адаптивні анкети, які легко заповнюються респондентами на будь-яких пристроях, таких як комп'ютери, планшети чи смартфони.

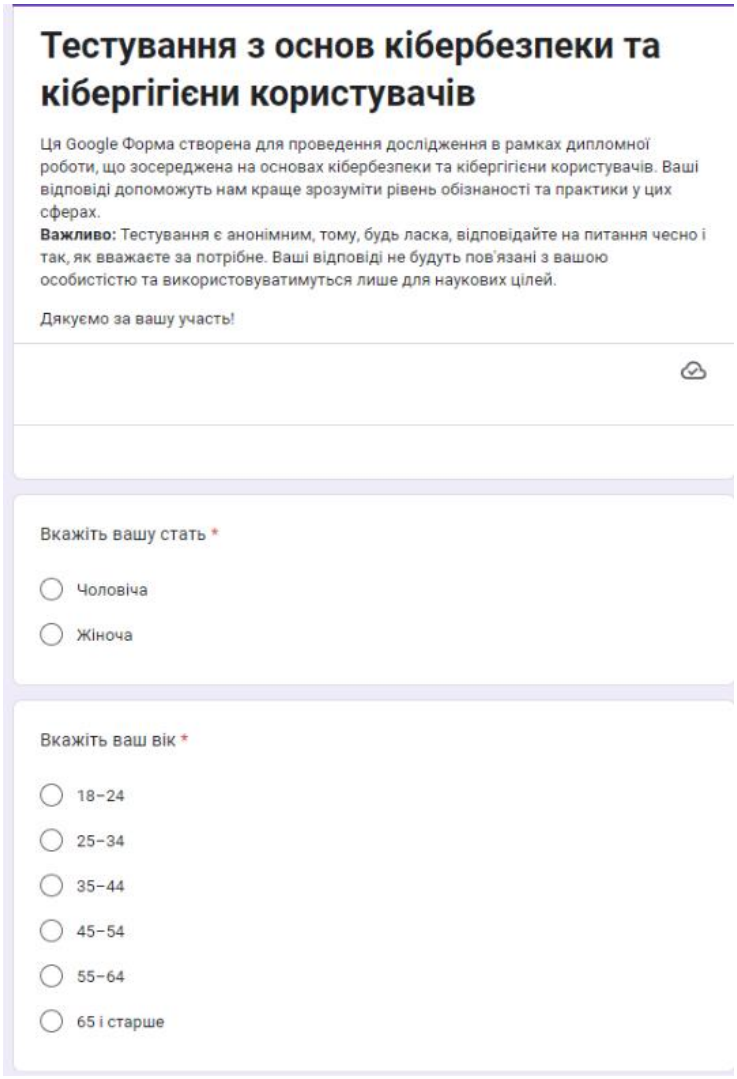


Рисунок 2.1 - Сторінка проведення тестування

Після завершення збору анкет, отримані дані були конвертовані у формат CSV для подальшої обробки. Весь обсяг даних було проаналізовано за допомогою статистичних інструментів.

Для цього були використані мови програмування, такі як Python, а також бібліотеки Pandas і NumPy, що дозволили здійснити описову статистику, виявити закономірності та підготувати дані для подальшого моделювання.

2.2. Вибір методів математичного моделювання для оцінки рівня знань у сфері кібербезпеки

Для оцінки рівня знань респондентів у сфері кібербезпеки було розроблено математичні моделі, що базуються на статистичних методах аналізу даних. Ці моделі дозволяють не лише визначити загальний рівень обізнаності, а й виявити закономірності, що впливають на знання респондентів.

Рівень знань респондента оцінюється за бальною системою, яка дозволяє визначити ступінь його обізнаності з питань, що стосуються кібербезпеки. Кожне запитання має свою вагу, і респонденти отримують бали за правильні відповіді або втрачають їх за неправильні. Такий підхід забезпечує більш точну оцінку, враховуючи як рівень знань, так і здатність респондента правильно розпізнавати загрози та використовувати методи захисту. Оцінка дозволяє також виявити, на яких аспектах кібербезпеки потрібно звернути більше уваги для покращення загальної обізнаності серед користувачів. Загальний бал знань Z для кожного респондента розраховується за формулою [9], що дозволяє автоматично оцінити рівень знань, спрощуючи процес аналізу та підготовки звітів. Цей підхід є корисним не лише для оцінки індивідуальних досягнень, а й для виявлення загальних тенденцій в обізнаності на груповому рівні.

$$Z_i = \sum_{j=1}^{n} x_{ij}$$

де:

1. Z_i— загальний рівень знань і-го респондента;
2. n — загальна кількість запитань;
3. x_{ij}— бали, отримані і-м респондентом за j-те запитання (можливі значення: +2, 0 або -2).

Після отримання балів знань для кожного респондента застосовується описова статистика, яка допомагає більш детально проаналізувати дані та отримати загальну картину обізнаності респондентів у сфері кібербезпеки. Описова статистика дозволяє виявити ключові тенденції, середні значення, варіації в рівнях знань, а також порівняти результати серед різних груп респондентів. Вона є важливим інструментом для представлення і структуризації отриманих даних у вигляді зрозумілих і наочних показників, що полегшує подальший аналіз і прийняття рішень. Основні статистичні показники, які використовуються в цьому процесі, включають:

Середнє значення (μ):

$$\mu = \frac{1}{N}\sum_{i=1}^{N} Z_i$$

Стандартне відхилення(σ):

$$\sigma = \frac{1}{N}\sum_{i=1}^{N}(Z_{i-}\mu)^2$$

Критерії нарахування балів наступні:

Таблиця 2.1 – Критерії нарахування балів за тестування.

Питання	**Варіанти відповідей**	**Бали**
Чи використовуєте ви пароль на своєму робочому місці?	Так	+3
	Hi, я не використовую.	-3
Якими електронними поштовими скриньками ви користуєтесь у повсякденному житті?	@gmail.com, @protonmail.com, @outlook.com, @aol.com, @mailfence.com	+2
	@ukr.net, @i.ua, @online.ua, @meta.ua, @bigmir.net	+2
	@rambler.ru, @yandex.ru, @mail.ru	-2
Який із наведених браузерів ви використовуєте?	Mozilla Firefox	+2
	Tor	+3
	Google Chrome	+2
	Brave	+3
	Opera	+2
	Internet Explorer	-1
	Microsoft Edge	+2
Чи використовуєте паролі, які відносяться до типу "змішаних" або "випадково згенерованих"?	Так	+2

Продовдження таблиці 2.1

	Ні	-1
Чи використовуєте один і той же пароль для різних сервісів?	Так, одного пароля достатньо та зручно.	-1
	Ні, у мене є декілька паролів у запасі.	+2
Визначте, які з повідомлень є коректними	Не вказано правильної відповіді	+2
Визначте, які з повідомлень є підозрілими.	Повідомлення 1, 2, 3, 4 (вказані окремо або в комбінаціях)	1-4 (залежно від кількості)
	Інакше	-2
Чи використовуєте ви двофакторну аутентифікацію?	Так	+2
	Ні	-1
	Я не знаю, що це	-1
Чи користуєтеся ви менеджерами паролів?	Так, я користуюся програмою KeePass.	+2
	Інакше	-1
Чи блокуєте ви комп'ютер та інші гаджети, якщо відходите від них?	Так, звичайно.	+2
	Ні	-1
Що ви зробите, якщо вам пише знайомий/колега у месенджері з проханням надати код підтвердження?	Нікому не надавайте цей код!	+2

Продовдження таблиці 2.1

	Інакше	-1
Що ви маєте пам'ятати, підключаючись до загальнодоступного Wi-Fi?	Небезпечно використовувати будь-які фінансові інтернет-сервіси із загальнодоступних мереж	+2
	Інакше	-1
Який із наведених нижче файлів, надісланий як додаток до електронного листа, скоріше за все є шкідливим програмним забезпеченням?	Річний_звіт_2024.doc.exe	+2
	Інакше	-2
У месенджері вам приходить повідомлення від знайомого, який просить вас проголосувати. Вкажіть алгоритм ваших дій.	Я часто зайнятий, мало вільного часу на дурниці.	+2
	Я послідовно виконав усі дії, але відмовився голосувати.	+1
	Я перейду за посиланням, проголосую, допоможу родині.	-3

```
ID: 1, Баллы: 17
ID: 2, Баллы: 19
ID: 3, Баллы: 25
ID: 4, Баллы: 6
ID: 5, Баллы: 15
ID: 6, Баллы: 19
ID: 7, Баллы: 8
ID: 8, Баллы: 21
ID: 9, Баллы: 18
ID: 10, Баллы: 12
ID: 11, Баллы: 11
ID: 12, Баллы: 11
ID: 13, Баллы: 6
ID: 14, Баллы: 24
ID: 15, Баллы: 19
ID: 16, Баллы: 18
ID: 17, Баллы: 13
ID: 18, Баллы: 12
ID: 19, Баллы: 0
ID: 20, Баллы: 2
```

Рисунок 2.2 - Перші 20 балів респондентів які пройшли тестування

Здійснивши аналіз результатів усіх записів, на рисунку 2.3 можна побачити що мінімальний бал – 0, максимальний бал – 28, більшість результатів – 15.

Середнє значення (μ): 15.19

Стандартне відхилення (σ): 4.79

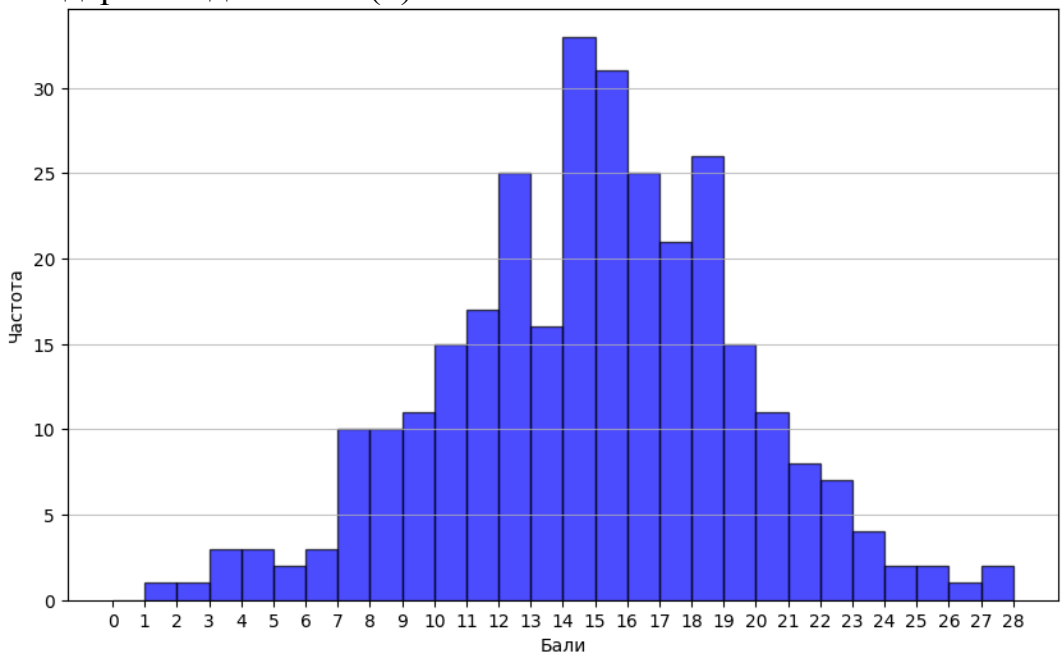


Рисунок 2.3 - Розподіл результатів проходження тестування

Можна зробити висновок, що рівень знань респондентів є досить однорідним, оскільки більшість з них продемонстрували приблизно однакові результати.

Однак варто зазначити, що існує невелика кількість респондентів, які отримали значно нижчі бали, ніж більшість. Це може свідчити про наявність певної кількості осіб із суттєвими прогалинами в знаннях.

Для виявлення взаємозв'язків між різними факторами (такими як вік, освіта, професійна діяльність) та рівнем знань у сфері кібербезпеки можна використовувати кореляційний аналіз.

Кореляційний коефіцієнт варіюється від -1 до +1. Значення +1 вказує на ідеальну позитивну кореляцію, тобто зростання однієї змінної призводить до зростання іншої. Значення -1 означає ідеальну негативну кореляцію, тобто зростання однієї змінної призводить до зниження іншої. Значення близько 0 вказує на відсутність зв'язку між змінними.

Для аналізу кореляцій обрані ключові фактори, які можуть впливати на рівень знань у сфері кібербезпеки, і проведено порівняння даних.

Почнемо аналіз датасету. Для початку виведемо графіки статистичних даних для кращого розуміння розподілу [10].

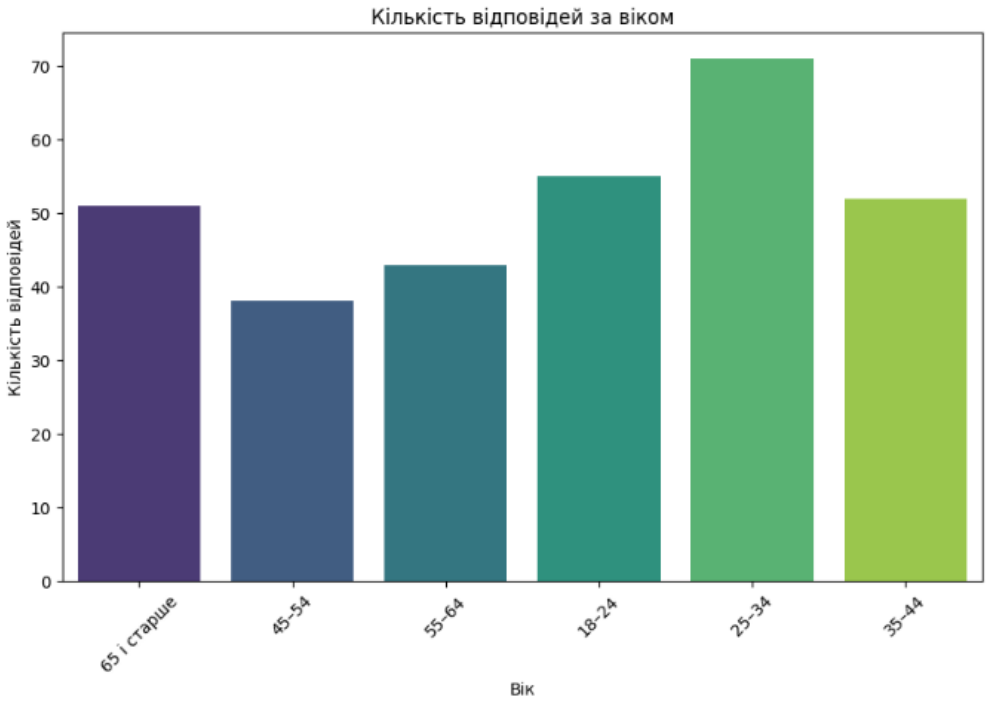


Рисунок 2.4 - Графік розподілу респондентів за віком

Як можна побачити на рисунку 2.2 більшість респондентів знаходяться у віці 25-34 роки, але в цілому дані є по всім віковим групам.

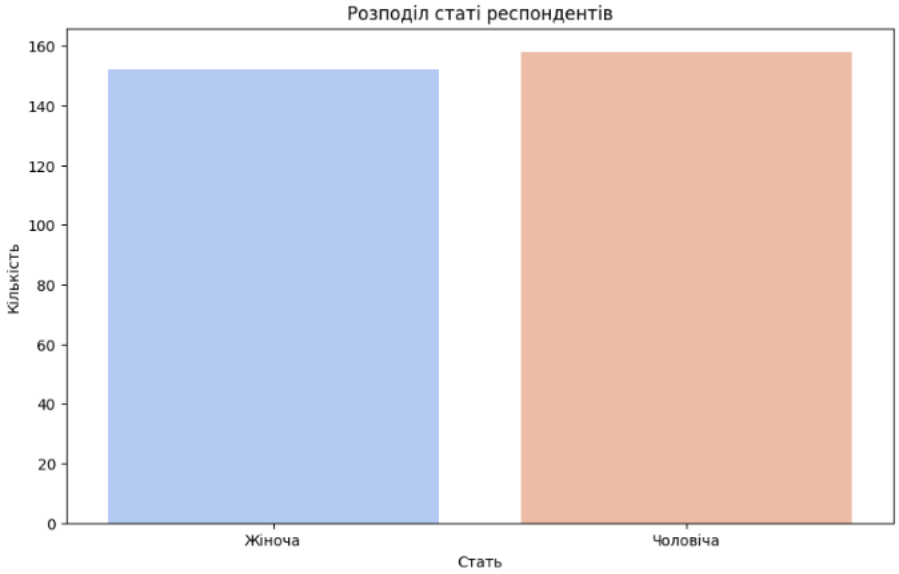


Рисунок 2.5 - Розподіл статі респондентів

Кількість жінок і чоловіків які проходили тестування майже однакове, але кількість чоловіків трохи більша.

На основі кореляційної матриці можна зробити висновок, що між вікомі статтю відсутні сильні лінійні зв'язки. Це означає, що вік, стать та бали респондентів є в основному незалежними один від одного.

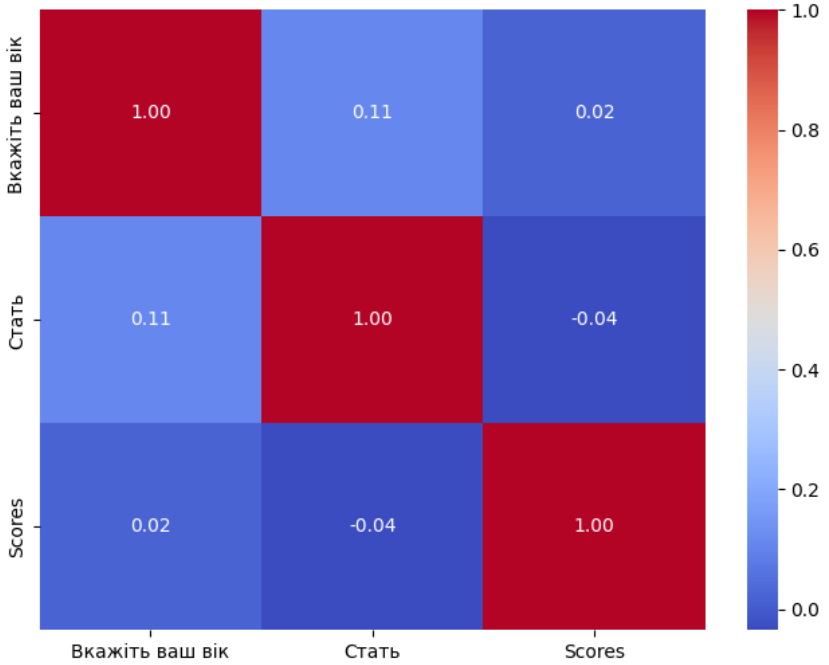


Рисунок 2.6 - Кореляція між статтю, віком та набраними балами

2.3. Алгоритми класифікації користувачів за рівнем кібербезпеки

Одним із ключових показників, який буде використано для подальшого аналізу та класифікації користувачів, є показник **Scores**. Цей показник варіюється від 0 до 28 балів і відображає рівень обізнаності користувачів щодо кібербезпеки.

Для класифікації користувачів за рівнем кібербезпеки було прийнято рішення поділити їх на три основні категорії:

1. **Високий рівень кібербезпеки** (показник Scores від 20 до 28 балів),
2. **Середній рівень кібербезпеки** (показник Scores від 10 до 19 балів),
3. **Низький рівень кібербезпеки** (показник Scores від 0 до 9 балів).

Для автоматизації процесу класифікації та побудови моделі, яка дозволить ефективно розподілити користувачів по відповідних категоріях, було використано алгоритм машинного навчання. Даний підхід дозволяє не тільки швидко класифікувати нові дані, але й оцінити точність моделі, що є важливим для верифікації результатів.

Після проведеного аналізу та вибору моделі було визначено кілька алгоритмів, які потенційно могли підходити для розв'язання поставленого завдання. Серед них розглядалися:

1. Логістична регресія,
2. Метод найближчих сусідів (K-NN),
3. Дерева рішень (Decision Trees).

Однак, враховуючи характер даних і необхідність зрозумілого та інтерпретованого поділу респондентів на групи, було обрано дерева рішень як основний алгоритм класифікації. Цей вибір був продиктований бажанням отримати чітку та інтуїтивно зрозумілу модель, що дозволяє ефективно класифікувати респондентів на основі їхніх балів знань.

Дерева рішень є одним із найбільш інтуїтивно зрозумілих алгоритмів класифікації, оскільки вони надають можливість візуалізувати процес прийняття рішень, що дозволяє не лише отримати результат, але й зрозуміти, як саме цей результат був отриманий. Цей алгоритм працює шляхом послідовного поділу набору даних на менші підгрупи, що відображають ключові характеристики — у нашому випадку це значення Scores.

Кожен крок поділу базується на логічних умовах, що відповідають найбільш значущим ознакам, які допомагають класифікувати респондентів. Завдяки цьому процесу дерево рішень дозволяє створити чітку і прозору модель, яку легко інтерпретувати. Переваги використання дерев рішень включають їхню простоту у використанні, можливість отримання наочних результатів у вигляді графічних діаграм, а також здатність працювати з великими обсягами даних, при цьому зберігаючи високу точність класифікації.

Переваги використання дерев рішень:

1. Модель легко візуалізується, і кожен розподіл користувачів може бути пояснений певними умовами (значеннями Scores).
2. Алгоритм не потребує нормалізації чи стандартизації вхідних даних.
3. Дерева рішень можуть працювати як із числовими, так і з категоріальними даними.

В результаті побудови моделі дерева рішень були визначені порогові значення для класифікації користувачів, що дозволило поділити їх на відповідні категорії за рівнем кібербезпеки. Точність моделі перевірялась на тестовій вибірці, де були отримані задовільні результати, що свідчить про надійність побудованої моделі [11].

Рисунок 2.7 - Співвідношення людей за рівнями кібербезпеки

```
Кількість людей у кожній категорії:
Category
Середній рівень    215
Високий рівень      55
Низький рівень      40
Name: count, dtype: int64

Середній бал у кожній категорії:
Category
Високий рівень     21.690909
Низький рівень      7.175000
Середній рівень    14.344186
Name: Scores, dtype: float64
```

Рисунок 2.8 - Отримані результати

Результати класифікації користувачів за рівнем кібербезпеки на основі їхніх балів дозволяють виокремити три основні категорії: **високий рівень, середній рівень** та **низький рівень**.

1. **Розподіл користувачів за рівнями**:

Найбільша кількість респондентів, 215 осіб, належить до категорії **середнього рівня** кібербезпеки, що становить переважну більшість.

До **високого рівня** належать 55 осіб, що вказує на те, що менша частина респондентів досягла високих показників за шкалою кібербезпеки.

Лише 40 осіб віднесені до **низького рівня**, що свідчить про відносно незначну кількість користувачів з низькими знаннями або навичками в галузі кібербезпеки.

2. **Середній бал у кожній категорії**:

Високий рівень: середній бал становить 21.69, що вказує на високі показники знань та практичних навичок у сфері кібербезпеки серед цих респондентів.

Це свідчить про те, що більшість з цих осіб мають добре розвинені навички захисту своїх даних і обізнаність щодо основних загроз, таких як фішинг, шкідливе програмне забезпечення та інші кіберзагрози. Респонденти цієї групи зазвичай мають чітке розуміння використання антивірусних програм, брандмауерів та інших засобів захисту.

Середній рівень: середній бал 14.34 свідчить про задовільний рівень кібербезпеки, хоча й із простором для вдосконалення.

Це означає, що респонденти цієї категорії мають основні знання, але їм не вистачає глибших навичок або свідомості щодо деяких аспектів захисту своїх даних. Їм ще потрібно вдосконалити свої навички у розпізнаванні загроз та впровадженні ефективних методів захисту.

Низький рівень: середній бал лише 7.17 вказує на значні прогалини у знаннях та практичних навичках у сфері кібербезпеки серед цієї групи. Респонденти цієї категорії, ймовірно, мають обмежене розуміння основних загроз та методів захисту, що підвищує ризики для їхніх особистих даних та онлайн-безпеки.

Це свідчить про потребу в додатковому навчанні та покращенні загальної обізнаності щодо важливості кібербезпеки.

2.5. Аналіз результатів моделювання та їх вплив на рекомендації щодо підвищення кібербезпеки

Моделювання рівнів кібербезпеки користувачів на основі їхніх балів дозволяє зробити кілька важливих висновків, що безпосередньо впливають на формування рекомендацій для підвищення рівня кібербезпеки.

1. Домінування середнього рівня кібербезпеки

Аналіз даних показує, що 215 респондентів, або близько 71% від загальної кількості, належать до категорії середнього рівня кібербезпеки. Це свідчить про наявність базових знань і розуміння принципів кібербезпеки, але також вказує на недостатність практичних навичок або глибшого розуміння певних аспектів, що впливають на захищеність користувачів в онлайн-середовищі.

Рекомендації:

Необхідно зосередити зусилля на поглибленні знань у сфері кібербезпеки для цієї категорії користувачів. Це можуть бути спеціальні тренінги з акцентом на практичні навички, такі як:

1. Навчання з ідентифікації фішингових атак;
2. Розуміння основ безпечного користування паролями;
3. Використання двофакторної автентифікації.

Організація практичних занять та реальних кейсів для відпрацювання кіберзагроз допоможе респондентам із середнім рівнем кібербезпеки піднятися до високого рівня. Такий підхід дозволить користувачам набути більш глибоких практичних навичок у розпізнаванні та нейтралізації кіберзагроз, що стане важливим кроком до покращення їх здатності реагувати на реальні ситуації. Включення сценаріїв з реальними атаками, такими як фішинг, шкідливе програмне забезпечення або соціальна інженерія, дозволить учасникам ефективніше застосовувати свої знання на практиці, покращуючи здатність приймати правильні рішення у критичних ситуаціях.

2. Мала кількість респондентів із високим рівнем кібербезпеки

Лише 55 респондентів (18%) досягли високого рівня кібербезпеки, що свідчить про значний дефіцит глибоких знань у цій сфері серед користувачів. Ця група показала середній бал 21.69, що демонструє високу обізнаність про кіберзагрози та відповідні заходи захисту.

Вони, ймовірно, мають добрі практичні навички у використанні антивірусних програм, брандмауерів та інших інструментів захисту, а також розуміють важливість правильного управління паролями та безпеки в Інтернеті.

Рекомендації:

Для користувачів з високим рівнем доцільно проводити більш спеціалізоване навчання, наприклад:

1. Поглиблені курси з криптографії та мережевої безпеки;
2. Практичне застосування технологій захисту даних і моніторингу систем безпеки;
3. Участь у сертифікованих програмах з кібербезпеки для подальшого підвищення кваліфікації.

3. Наявність користувачів із низьким рівнем кібербезпеки

Незначна, але важлива група з 40 респондентів (11%) має низький рівень кібербезпеки з середнім балом 7.17. Це свідчить про серйозну вразливість до кіберзагроз та брак елементарних навичок захисту. Користувачі цієї групи, ймовірно, не мають достатньої обізнаності про основні загрози та методи захисту, що підвищує їх ризик ставати жертвами фішингу, шкідливого програмного забезпечення чи інших кіберзлочинів.

Відсутність належних заходів захисту, таких як надійні паролі, антивірусні програми чи налаштування безпеки на пристроях, робить їх особливо уразливими. Ця група потребує термінового навчання та підвищення обізнаності для зниження ризику кібератак і покращення загальної безпеки в Інтернеті.

Рекомендації:

Для цієї групи необхідно провести базові курси з кібербезпеки, які охоплюють фундаментальні аспекти:

1. Розпізнавання загроз;
2. Основи захисту інформації в інтернеті;
3. Правила безпечного користування електронною поштою та соціальними мережами.

Необхідно підвищити загальну обізнаність про кіберризики через освітні програми та інформаційні кампанії. Це дозволить мінімізувати кількість користувачів, які є найбільш вразливими до атак, і створити більш захищене середовище для обміну інформацією в мережі.

Освітні ініціативи можуть включати інтерактивні семінари, вебінари, а також розповсюдження матеріалів, що висвітлюють актуальні загрози та методи захисту. Зокрема, важливо акцентувати увагу на розпізнаванні фішингових атак, збереженні конфіденційності в Інтернеті та правильному використанні паролів. Ці заходи сприятимуть не тільки зниженню рівня вразливості користувачів, а й загальному покращенню безпеки в Інтернеті.

В кінцевому рахунку, це допоможе створити безпечніший онлайн-простір, зменшуючи ймовірність успішних атак на недосвідчених користувачів та підвищуючи загальний рівень захисту [12].

2.6 Способи виявлення та передбачення загроз на основі штучного інтелекту

На сучасному етапі розвитку інформаційної безпеки ШІ та машинне навчання (ML) стали важливими інструментами для аналізу великих обсягів даних і своєчасного виявлення загроз, які раніше могли залишатися непоміченими через складність або обсяг інформації.

Основні методи виявлення загроз в наш час є наступні:

1. Методи машинного навчання (ML).

Багато сучасних рішень для забезпечення кібербезпеки базуються на використанні алгоритмів машинного навчання, таких як методи класифікації (напр., SVM, Decision Trees) та кластеризації (напр., K-means).

2. Глибоке навчання (DL).

Завдяки глибоким нейронним мережам можливо проводити аналіз складних патернів у поведінці мережевого трафіку, що допомагає виявляти складні кіберзагрози. Наприклад, рекурентні нейронні мережі (RNN) добре підходять для роботи з часовими рядами, що робить їх ефективними для виявлення аномалій у послідовності подій.

3. Мережі для виявлення аномалій (Anomaly Detection Networks).

Цей підхід дозволяє розпізнавати потенційно небезпечні дії, які відрізняються від нормальних поведінкових шаблонів. Використання таких мереж дозволяє зменшити кількість хибнопозитивних спрацьовувань.

Методи передбачення загроз в свою чергу наступні:

1. Прогностичне моделювання.

Використання методів регресії та прогнозування ризиків дозволяє на основі поточних даних передбачати ймовірність виникнення майбутніх загроз. Це дозволяє виявити потенційні проблеми на ранніх етапах і вжити відповідних заходів для їх мінімізації. Для таких прогнозувань широко використовуються моделі на основі часових рядів, зокрема ARIMA (AutoRegressive Integrated Moving Average) та LSTM (Long Short-Term Memory).

Моделі ARIMA дозволяють ефективно аналізувати та прогнозувати змінні, що залежать від часу, враховуючи їхню сезонність та тренди. LSTM, в свою чергу, є частиною глибинного навчання і здатний працювати з великими обсягами даних, вивчаючи складні патерни для точніших прогнозів, зокрема в умовах нестабільності та змінності. Ці підходи значно покращують здатність до своєчасного реагування на кіберзагрози та забезпечують кращу готовність до майбутніх викликів.

2. Інтеграція з великими даними (Big Data).

Обробка великих масивів даних дозволяє штучному інтелекту знаходити приховані закономірності й залежності, що можуть сигналізувати про можливі загрози. Використання Big Data з ML-моделями сприяє побудові прогностичних моделей, що ефективно працюють з постійно змінними даними.

3. Методи на основі графових моделей.

Використання графових нейронних мереж для аналізу зв'язків між подіями дозволяє передбачати можливі вектори атак та оцінювати ризики розповсюдження кіберзагроз.

Для виявлення та вирішення кіберзагроз можна, на приклад, використати метод Isolation Forest, який є одним із популярних інструментів для виявлення аномалій у великих наборах даних. Цей метод базується на концепції відокремлення аномальних точок даних, які мають значну відмінність від основного обсягу інформації, що представляє нормальний стан системи.

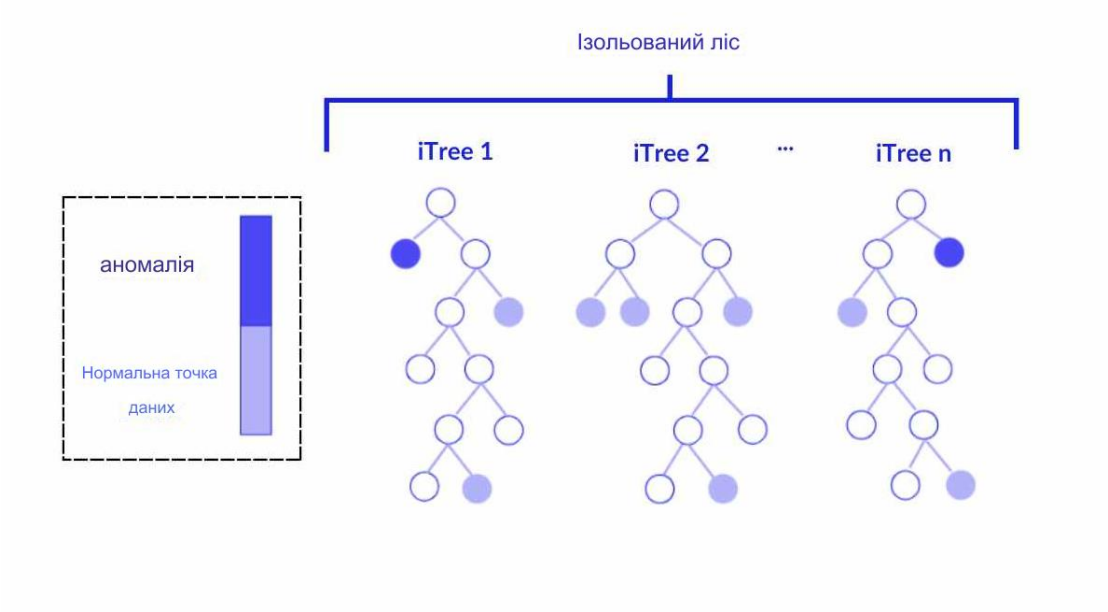


Рисунок 2.9 - Концепція роботи ізольованого лісу

Isolation Forest працює ізолюючи аномалії через поділ вхідних даних (трафіку) на менші підмножини. Аномалії, наприклад, підозрілі підключення або потоки даних з незвично високою інтенсивністю, зазвичай потребують меншої кількості розділень для ізоляції порівняно з нормальним трафіком. Це дозволяє швидко виявити потенційні загрози, такі як атаки DDoS, вторгнення або сканування портів.

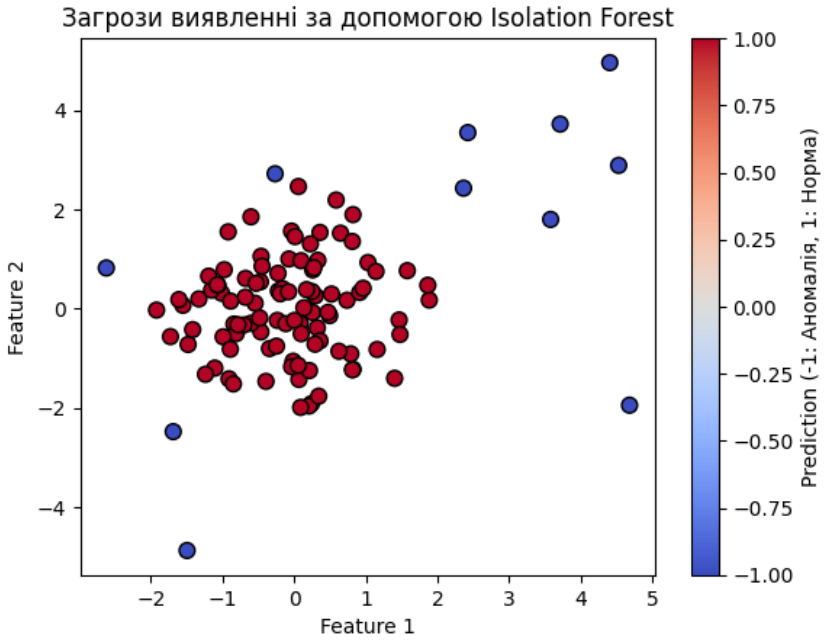


Рисунок 2.10 - Приклад роботи Isolation Forest

Для прикладу, реалізуємо емуляцію атаки на сервер, зокрема розподілену атаку на відмову в обслуговуванні (DDoS). У цій симуляції налаштовуємо параметри, щоб відтворити поведінку нормального мережевого трафіку та інтенсивного потоку запитів, що характерний для DDoS-атаки.

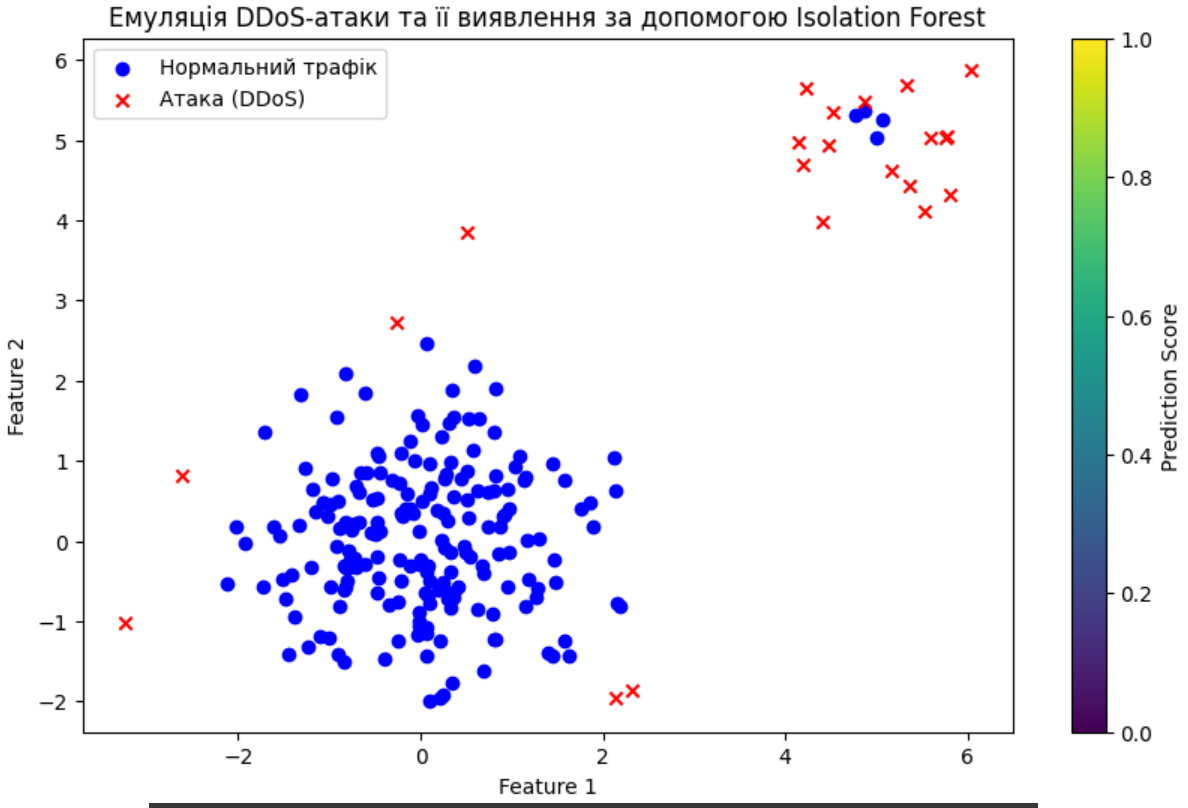
Нормальний трафік:

1. 200 запитів, які відповідають звичайному навантаженню сервера.
2. Дані генеруються на основі нормального розподілу із середнім значенням 0 і стандартним відхиленням 1, що імітує випадковий мережевий трафік із помірною варіабельністю.
3. Нормальні запити знаходяться близько до центру координат (0,0), що відповідає нормальному трафіку із середньою інтенсивністю.

DDoS-атака:

1. 20 запитів, які значно відрізняються від нормального трафіку та є інтенсивнішими.
2. Для цих запитів обрано інший розподіл із середнім значенням 5 і малим відхиленням 0.5. Це відображає концентровану хвилю трафіку, яка, ймовірно, перевантажить сервер. [13]

Під час DDoS-атаки трафік зосереджений навколо певного рівня інтенсивності, що робить його віддаленим від середнього значення звичайного трафіку, тим самим полегшуючи його виявлення як аномалії.




```
Кількість дерев у лісі: 100
Відсоток аномальних зразків: 0.1
Розмір підвибірки для кожного дерева: auto
Кількість суттєвих аномалій: 0
Суттєві аномалії: []
```

Рисунок 2.11 - Емуляція DDoS атаки та виявлення її за допомогою Isolation Forest

Як можна побачити, Isolation Forest досить добре виділяє аномальний трафік, що виникає під час DDoS-атак. Завдяки своїй здатності виявляти нехарактерні патерни в даних, ця модель ефективно ідентифікує запити, які суттєво відрізняються від нормального рівня трафіку.

Але окрім Isolation Forest є також багато інших ефективних методів для виявлення кіберзагроз.

Таблиця 2.2 – Найбільш ефективні методи машинного навчання для виявлення та усунення кіберзагроз

Метод	Опис	Приклад застосування
Autoencoders	Нейронна мережа для зменшення розмірності даних і пошуку аномалій через значне відхилення від норми.	Виявлення аномальної поведінки користувачів у мережі, яке може вказувати на потенційні загрози.
K-means кластеризація	Метод, що класифікує дані в групи (кластери) за схожими характеристиками, дозволяючи виявляти аномалії.	Визначення незвичних моделей трафіку, що відрізняються від типових патернів у певних кластерах.
Рекурентні нейронні мережі (RNN)	Аналізує часові ряди, щоб виявити послідовності подій, що можуть призвести до загроз.	Прогнозування загроз на основі історичного аналізу даних, наприклад, для виявлення аномальної активності в логах.
Support Vector Machine (SVM)	Класифікаційний метод, що розділяє дані на категорії та допомагає визначати аномальні випадки.	Виявлення підозрілих мережевих запитів на основі класифікації поведінки користувачів.
Graph Neural Networks (GNN)	Моделі, що аналізують зв'язки між об'єктами, дозволяючи виявляти складні патерни в мережевій структурі.	Визначення потенційних шляхів поширення атаки по мережі, аналізуючи зв'язки між вузлами та з'єднаннями.

Продовження таблиці 2.2

Long Short-Term Memory (LSTM)	Вид RNN для прогнозування загроз у часових рядах, запам'ятовуючи попередню інформацію.	Прогнозування аномальної активності у трафіку з урахуванням попередніх зразків, що часто використовують для виявлення атак.

Способи виявлення та передбачення загроз на основі штучного інтелекту, такі як методи Isolation Forest, демонструють високу ефективність у ідентифікації аномалій у мережевому трафіку. Ці технології дозволяють виявляти потенційні кіберзагрози, зокрема DDoS-атаки, завдяки здатності аналізувати великі обсяги даних і виявляти нетипові патерни.

Використання штучного інтелекту суттєво підвищує рівень безпеки інформаційних систем, дозволяючи організаціям своєчасно реагувати на загрози і запобігати можливим втратам. Це створює більш стійкі до атак мережі, що є критично важливим у сучасному цифровому середовищі.

Висновок до розділу 2

Проведене дослідження та математичне моделювання рівня знань у сфері кібербезпеки серед респондентів дозволили отримати детальну картину обізнаності в цій важливій області. Зібрані дані за допомогою соціального опитування дали змогу оцінити рівень знань, виявити основні слабкі місця та встановити закономірності, що впливають на обізнаність респондентів. Використання бальної системи оцінки знань, а також описової статистики забезпечило точний та ефективний аналіз отриманих результатів.

Результати дослідження вказують на те, що більшість респондентів має базове розуміння основ кібербезпеки, але все ще є значний потенціал для покращення знань, зокрема в питаннях захисту даних та використання найбільш ефективних інструментів безпеки. Аналіз показав, що деякі групи респондентів мають недостатній рівень обізнаності щодо загроз і методів захисту, що вимагає додаткових освітніх заходів та впровадження більш ефективних програм навчання.

Загалом, результати цього дослідження можуть бути корисними для розробки нових стратегій підвищення обізнаності в сфері кібербезпеки та для створення освітніх програм, спрямованих на усунення виявлених прогалин у знаннях.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ ЗАХИСТУ ФІЗИЧНИХ КОМПОНЕНТІВ КОМП'ЮТЕРНИХ МЕРЕЖ

3.1 Способи класифікації атак із позиції побудови систем їх виявлення

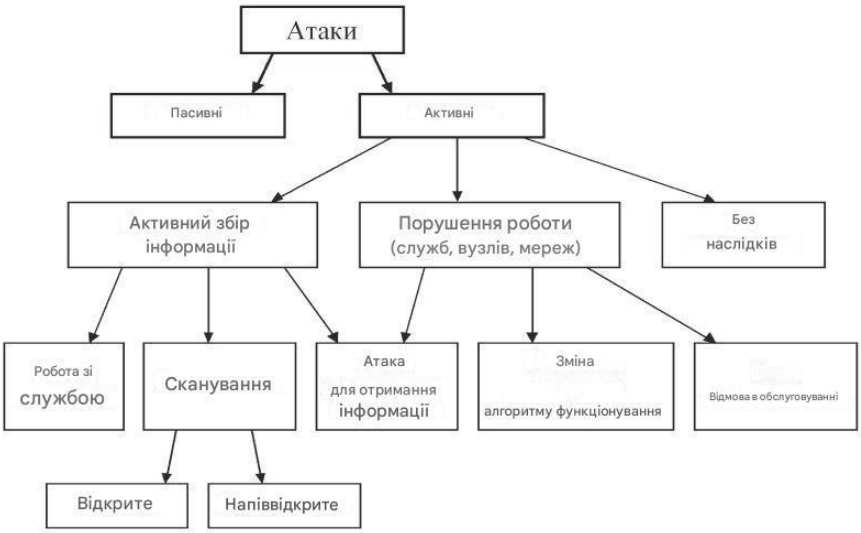


Рисунок 3.2 - Класифікація атак

Актуальність проблеми класифікації атак у контексті побудови систем їх виявлення (СВА) обумовлена необхідністю забезпечення ефективного протистояння різним типам загроз у мережевих системах. Класифікація атак має важливе значення для ідентифікації потенційних ризиків і розробки відповідних засобів протидії. Існують різні підходи до класифікації атак, які включають поділ на активні та пасивні, зовнішні й внутрішні, умисні та ненавмисні. Водночас деталізація класифікації не завжди корисна для СВА, оскільки часто виділяються класи, які мають мінімальне практичне значення для їх виявлення [14].

Найбільш доцільною з позиції СВА є класифікація, яка дозволяє об’єднувати атаки у групи, що легко піддаються аналізу та ідентифікації. До таких груп належать наступні категорії атак:

1. **Віддалене проникнення** (remote penetration) включає атаки, які дозволяють отримати несанкціонований доступ до віддалених комп’ютерів через мережу. Такі атаки часто реалізуються за допомогою програм, як-от NetBus або Back Orifice.
2. **Локальне проникнення** (local penetration) передбачає отримання несанкціонованого доступу до локального вузла або підвищення прав користувача. До прикладів належать експлойти для уразливостей операційних систем.
3. **Віддалений відмову в обслуговуванні** (remote DoS) – це атаки, спрямовані на порушення роботи системи або її перезавантаження шляхом використання віддалених дій. До таких атак належать, наприклад, trinoo та teardrop.

4. **Локальний відмову в обслуговуванні** (local DoS) включає атаки, що порушують функціонування системи на локальному рівні, наприклад, шляхом перевантаження процесора.

5. **Мережеві сканери** (network scanners) аналізують топологію мережі для виявлення доступних сервісів. Типовими прикладами є програми nmap.

6. **Сканери уразливостей** (vulnerability scanners) спрямовані на пошук вразливих точок у мережах. Відомими прикладами є SATAN, XSpider.

7. **Програми для зламу паролів** (password crackers) застосовуються для підбору паролів користувачів, як, наприклад, L0pht Crack.

8. **Сніфери** (sniffers) перехоплюють мережевий трафік із метою вилучення чутливої інформації, зокрема ідентифікаторів та паролів. Прикладом таких засобів є tcpdump.

Важливим аспектом класифікації є те, що атаки можуть належати до кількох класів одночасно. Це зумовлено різноманіттям шляхів досягнення кінцевих цілей, наприклад, використанням віддаленого проникнення для ініціювання DoS-атаки.

З позиції СВА не рекомендується класифікувати атаки за типами загроз, такими як порушення конфіденційності, цілісності чи доступності, оскільки ці категорії є занадто загальними й не враховують специфіку способів реалізації загроз. Натомість орієнтація на реальні сценарії атак дозволяє розробляти більш ефективні підходи до їх ідентифікації та протидії.

Особливу увагу слід приділити пасивним та активним атакам, які суттєво відрізняються за своєю природою. Пасивні атаки спрямовані на збір інформації без прямого втручання в роботу системи, тоді як активні атаки включають дії, спрямовані на порушення функціонування системи або отримання доступу до її ресурсів.

Для боротьби з пасивними атаками доцільно використовувати методи шифрування трафіку, що унеможливлює вилучення інформації навіть у разі її перехоплення. У разі активних атак важливими є засоби моніторингу та блокування підозрілих дій, зокрема виявлення аномальної активності на ранніх етапах.

Висновок: класифікація атак із позиції СВА є ключовим інструментом для розробки ефективних методів їх виявлення. Використання такої класифікації дозволяє не лише вчасно виявляти загрози, але й адаптувати системи захисту до нових викликів у сфері інформаційної безпеки.

3.2 Моделювання методів побудови DMZ в Cisco Packet Tracer

У цій роботі використовується програма **Cisco Packet Tracer** — ефективний інструмент для моделювання та аналізу мережевої інфраструктури. Вона дозволяє створювати складні топології, налаштовувати мережеве обладнання, тестувати його роботу та аналізувати мережевий трафік. Основна увага зосереджена на конфігурації пристроїв для забезпечення безпеки та ефективності роботи мережі.

Однак через обмежений функціонал **Cisco Packet Tracer** не вдається повністю розкрити весь потенціал обладнання Cisco. Деякі функції, такі як просунуті можливості безпеки, підтримка певних протоколів або специфічні сценарії реального використання, не можуть бути відтворені в рамках цієї програми. Це слід враховувати під час оцінки результатів, оскільки повний спектр функціональності Cisco доступний лише на фізичному обладнанні або за допомогою більш просунутих інструментів, таких як Cisco VIRL або GNS3.

Незважаючи на ці обмеження, **Cisco Packet Tracer** залишається одним із найзручніших інструментів для навчання та тестування базових і середніх сценаріїв роботи мережі. Він широко використовується у навчальних закладах для ознайомлення з базовими принципами налаштування маршрутизаторів, комутаторів, брандмауерів та інших мережевих пристроїв. Його інтуїтивно зрозумілий інтерфейс та можливості візуалізації значно спрощують вивчення складних мережевих концепцій.

Одним із ключових завдань цієї роботи є налаштування та моделювання роботи **Cisco ASA** (Adaptive Security Appliance), пристрою для забезпечення мережевої безпеки. ASA поєднує функціональність маршрутизаторів і брандмауерів, забезпечуючи надійний захист мережі. Вона підтримує функції, такі як **Stateful Packet Inspection**, VPN, NAT, динамічна маршрутизація та фільтрація трафіку. Основна увага зосереджена на налаштуванні безпечних рівнів довіри між внутрішньою, зовнішньою та демілітаризованою зонами мережі (DMZ).

Для цього в роботі виконуються наступні кроки: [15]

1. Налаштування VLAN-інтерфейсів з різними рівнями безпеки.
2. Впровадження механізмів NAT для трансляції адрес.
3. Реалізація функцій Stateful Packet Inspection для контролю сесійного трафіку.
4. Тестування доступності між зонами мережі.

Важливим аспектом є дотримання принципу «найменшого довіреного рівня», що полягає в налаштуванні мінімального рівня довіри для зовнішніх інтерфейсів та максимального — для внутрішніх. Наприклад, зовнішній інтерфейс (security-level 0) отримує найнижчий рівень довіри, тоді як внутрішній інтерфейс (security-level 100) — найвищий. Це дозволяє ефективно захищати внутрішню мережу від загроз ззовні.

Таким чином, хоча **Cisco Packet Tracer** має певні обмеження, він дозволяє розв'язувати багато завдань з налаштування мережевих пристроїв, що є важливим етапом у вивченні основ мережевої безпеки та інфраструктури.

Таблиця 3.1 – Функції Cisco ASA

Загальні функції з маршрутизаторами	**Основні функції Cisco ASA**	**Функції, доступні тільки на маршрутизаторах**
Динамічна маршрутизація – дозволяє автоматично оновлювати таблиці маршрутизації.	**Stateful Packet Inspection** – перевірка стану сесій для забезпечення безпеки трафіку.	**BGP** – протокол маршрутизації для великих мереж, наприклад, інтернету.
NAT – трансляція мережевих адрес для економії IP-адрес та захисту мережі.	**IDFW** – виявлення внутрішніх загроз у мережі.	**MPLS** – технологія маршрутизації для передачі трафіку різних типів.
Фільтрація трафіку (Access Lists) – контроль доступу за певними критеріями.	**TrustSec** – підвищення безпеки через розподіл рівнів довіри.	**DMVPN** – динамічне створення VPN між декількома точками.
VPN (site-to-site, RA VPN) – створення безпечних тунелів для передачі даних.	**Покращений VPN** – розширені функції для безпечної передачі даних через тунелі.	**GRE** – протокол для інкапсуляції трафіку в тунелях.
-	**IPS** – система запобігання вторгненням, що захищає від атак.	**WLAN Controller** – централізоване управління бездротовими мережами.

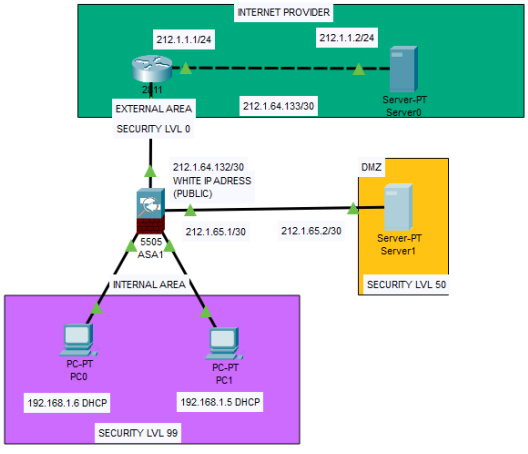


Рисунок 3.3 – Схема захисту мережі

На схемі зображено мережеву інфраструктуру з використанням міжмережевого екрана ASA5505 та розділенням мережі на три зони безпеки:

EXTERNAL AREA (зовнішня зона, рівень безпеки 0):

1. Підключення до Інтернет-провайдера.
2. Вказані IP-адреси для маршрутизатора зовнішньої зони (212.1.1.1/24) і сервера провайдера (212.1.1.2/24).
3. Використовується IP-адреса 212.1.64.132/30 як публічна адреса для підключення до ASA.

INTERNAL AREA (внутрішня зона, рівень безпеки 99):
Локальна мережа з двома клієнтськими комп'ютерами (PC0 та PC1), які отримують IP-адреси через DHCP:

PC0: 192.168.1.6
PC1: 192.168.1.5
Ця зона є найбільш захищеною.

DMZ (Demilitarized Zone) (демілітаризована зона, рівень безпеки 50):
Сервер (Server1) у цій зоні має IP-адресу 212.1.65.2/30.
Ця зона призначена для розміщення серверів, які мають доступ із зовнішньої мережі.

Основні елементи:

ASA5505:

Використовується як міжмережевий екран для управління доступом між зонами безпеки.
Розділяє мережу на зовнішню, внутрішню та DMZ.

Підключення:

Зовнішня зона підключається до публічної IP-адреси ASA.
DMZ з'єднана з ASA для розміщення публічного сервера.
Внутрішня зона має доступ до локальної мережі через ASA.

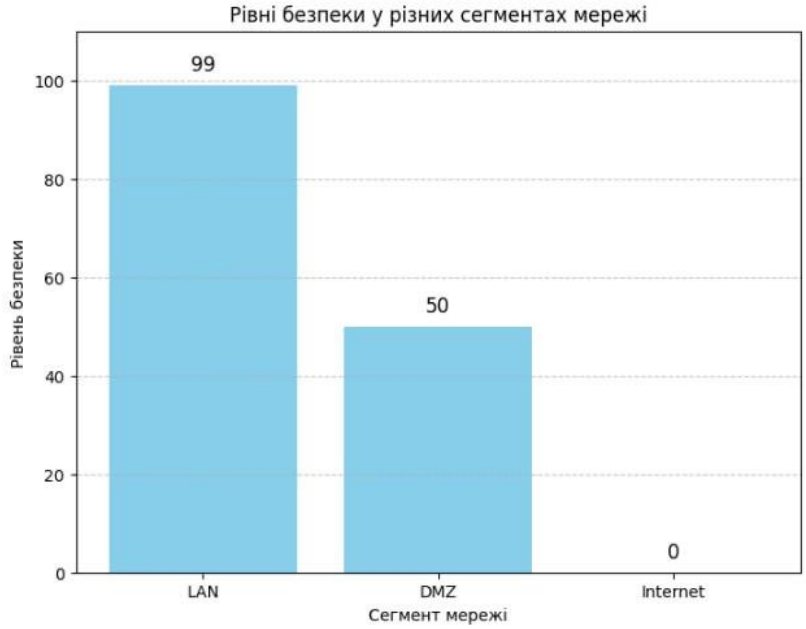


Рисунок 4.3 - Рівні безпеки у сегментах мережі

Налаштування Cisco ASA:

1. Початкова конфігурація ASA

ASA за замовчуванням використовує DHCP-сервер для внутрішніх пристроїв з пулом IP-адрес: 192.168.1.5–192.168.1.36.

```
ciscoasa>enable
ciscoasa#configure terminal
ciscoasa(config)#interface Vlan1
ciscoasa(config-if)#nameif inside
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#ip address 192.168.1.1 255.255.255.0
ciscoasa(config)#interface Vlan2
ciscoasa(config-if)#nameif outside
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#ip address dhcp
```

2. Налаштування доступу через SSH

Дозволяємо підключення по SSH для внутрішньої мережі:

```
ciscoasa(config)#username admin password c6s2u7MA
ciscoasa(config)#ssh 192.168.1.0 255.255.255.0 inside
ciscoasa(config)#aaa authentication ssh console local
```

3. Налаштування NAT Створюємо об'єкт для NAT:

```
ciscoasa(config)#object network nat
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0
ciscoasa(config-network-object)#nat (inside,outside) dynamic interface
```

4. Налаштування Stateful Packet Inspection

Додаємо перевірку ICMP та HTTP:

```
ciscoasa(config)#class-map inspection_default
ciscoasa(config-cmap)#match default-inspection-traffic
ciscoasa(config-cmap)#exit
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#inspect icmp
ciscoasa(config-pmap-c)#inspect http
ciscoasa(config)#service-policy global_policy global
```

Налаштування маршрутизатора (Router R0)

1. Призначаємо IP-адреси для інтерфейсів:

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 212.1.64.133 255.255.255.252
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 212.1.1.1 255.255.255.0
```

2. Створюємо маршрут:

```
Router(config)#ip route 192.168.1.0 255.255.255.0 212.1.64.132
```

Демонстрація роботи

Коли користувач надсилає ICMP-пакет із внутрішньої мережі, ASA аналізує цей трафік і запам'ятовує сесію у своїй динамічній таблиці станів. При цьому пристрій інспектує пакет, перевіряючи кілька параметрів: відповідність джерела, адресата, портів, а також номера пакета. Якщо всі ці параметри відповідають умовам активної сесії, яка була ініційована з більш довіреного інтерфейсу (з вищим рівнем безпеки), то ASA пропускає відповідний пакет.

Коли відповідний ICMP-пакет повертається через зовнішній інтерфейс, ASA перевіряє таблицю станів. Якщо запис про цю сесію існує і всі параметри збігаються, пакет пропускається. У разі ж, якщо пакет надходить із зовнішнього інтерфейсу, але сесія не була ініційована внутрішньою мережею, ASA проінспектує цей трафік і не знайде його у своїй таблиці. У такому випадку пакет буде відхилено, адже це порушує правила безпеки.

Таким чином, інспектування трафіку на ASA забезпечує, що тільки трафік, ініційований з більш довіреного інтерфейсу, може отримати зворотній доступ. Всі пакети з невідомих сесій або ті, що не відповідають записам у таблиці станів, блокуються, забезпечуючи захист мережі від несанкціонованого трафіку. [16]

Рисунок 3.5 - Конфігурація системи

На зображенні представлено блок-схему, яка описує процес обробки ICMP-пакетів міжмережевим екраном Cisco ASA. Ось детальний опис кожного етапу:

1. **Користувач надсилає ICMP-пакет з внутрішньої мережі**:
   На цьому етапі користувач (або пристрій) з внутрішньої локальної мережі відправляє ICMP-пакет (наприклад, пінг) у зовнішню мережу (інтернет або іншу мережу).
2. **ASA отримує ICMP-пакет**:
   Міжмережевий екран ASA приймає цей ICMP-пакет на одному зі своїх інтерфейсів, зазвичай на внутрішньому інтерфейсі (inside interface).
3. **ASA аналізує трафік та запам'ятовує сесію**:
   ASA перевіряє структуру пакета, його IP-адресу джерела, адресу призначення, тип пакета (ICMP) та іншу інформацію.
   На основі цієї інформації ASA створює запис у таблиці сесій (state table), щоб дозволити зворотний трафік від адресата.
4. **Пакет повертається через зовнішній інтерфейс**:
   Після проходження через зовнішній інтерфейс (outside interface), ICMP-пакет потрапляє у зовнішню мережу, наприклад, до сервера, до якого був адресований.

Ця схема демонструє роботу механізму перевірки стану (stateful inspection) міжмережевого екрану Cisco ASA, який дозволяє пропускати лише відповідний трафік і блокує небажаний.

DMZ

Організація **DMZ-зони** в Cisco Packet Tracer для розміщення публічних сервісів в окремому сегменті мережі. Оскільки ці сервіси є загальнодоступними і до них відкритий доступ з Інтернету, ризик їх злому досить високий. У випадку проникнення на один із серверів, наша локальна мережа залишається захищеною, оскільки знаходиться в іншому сегменті. Таким чином, ми мінімізуємо потенційну шкоду від можливого взлому публічного сервера.

Принцип роботи DMZ

Сервери, розташовані в DMZ, зазвичай мають публічні ("білі") IP-адреси. Хоча можна обійтися і приватними адресами, використовуючи функції статичного NAT. Головна умова — це виділений сегмент для серверів, яким потрібен доступ з зовнішньої мережі.

Для повноцінної реалізації DMZ мережеве обладнання повинно підтримувати функції **Stateful Firewall**, тобто можливість запам'ятовувати сесії. Використовуючи інспектування трафіку, ми можемо заборонити серверам у DMZ ініціювати з'єднання з локальною мережею, тим самим захищаючи користувачів від зловмисників, які, можливо, зламали один із публічних серверів. При цьому для самих користувачів сервери DMZ залишаються доступними. Якщо використовувати лише звичайні Access Lists, це може залишити дири для можливого проникнення або взагалі не дозволити налаштувати необхідний рівень безпеки [17].

Реалізація DMZ

DMZ можна організувати на міжмережевому екрані за допомогою **security-level**, а також реалізувати на маршрутизаторі, використовуючи **Zone-Based Firewall** або старішу технологію **CBAC** (Context-Based Access Control). Оскільки вся робота виконується в емуляторі Cisco Packet Tracer, можливості якого обмежені, будемо використовувати CBAC.

Структура мережі

Зазвичай у корпоративній мережі є три сегменти:

1. **Внутрішня мережа (Inside)** — локальна мережа організації.
2. **Зовнішня мережа (Outside)** — мережа Інтернет.
3. **DMZ-зона** — сегмент для публічних серверів.

У нашій роботі будуть реалізовані три політики доступу:

1. **З локальної мережі в Інтернет**.
2. **З локальної мережі в сегмент DMZ**.
3. **З мережі Інтернет в сегмент DMZ**.

Додавання сервера в DMZ-зону

До схеми додаємо новий сервер, який буде розташований в DMZ-зоні. Він підключений до Cisco ASA через інтерфейс Ethernet0/2 з IP-адресою 212.1.65.1/30. Сервер має IP-адресу 212.1.65.2/30. Сервер буде виконувати функцію, наприклад, веб-сервера або поштового шлюзу, і забезпечить доступ з інтернету через зовнішній інтерфейс ASA. Для налаштування доступу та безпеки між інтерфейсами ASA буде використовуватися NAT та відповідні правила доступу.

Також необхідно налаштувати відповідні маршрути та ACL (списки контролю доступу) для управління трафіком між інтерфейсами DMZ, Inside та Outside. Крім того, для забезпечення належного захисту серверу в DMZ-зоні, рекомендується застосувати фільтрацію трафіку через ASA та застосування політик для обмеження несанкціонованого доступу з інших мереж.

Налаштування маршрутизатора провайдера (R0)

На маршрутизаторі R0 необхідно прописати маршрут до сервера в зоні DMZ через інтерфейс ASA:

R0(config)# ip route 212.1.65.0 255.255.255.252 212.1.64.132

Налаштування Cisco ASA

1. **Налаштування інтерфейсу для DMZ**

ciscoasa(config)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 3
ciscoasa(config-if)# exit
ciscoasa(config)# interface vlan 3
ciscoasa(config-if)# nameif dmz

Примітка: з'явилася помилка

ERROR: This license does not allow configuring more than 2 interfaces with nameif and without a "no forward" command on this interface or on 1 interface(s) with nameif already configured.

Це пов'язано з обмеженнями ліцензії в Cisco Packet Tracer. Щоб обійти цю проблему, потрібно виконати:

ciscoasa(config-if)# no forward interface vlan 1
ciscoasa(config-if)# nameif dmz
INFO: Security level for "dmz" set to 0 by default.
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 212.1.65.1 255.255.255.252

3.3 Налаштування політик безпеки

На даний момент у нас така ситуація:

Внутрішня мережа (VLAN 1) — security-level 99.

DMZ-зона (VLAN 3) — security-level 50.

Зовнішня мережа (VLAN 2) — security-level 0.

За замовчуванням, трафік з інтерфейсу з вищим рівнем безпеки може ініціювати з'єднання до інтерфейсу з нижчим рівнем безпеки, але не навпаки. Тому з Інтернету (security-level 0) трафік не може заходити в DMZ (security-level 50) без явного дозволу.

Дозвіл трафіку з Інтернету до DMZ

Щоб дозволити пінг та доступ до веб-сервера в DMZ з Інтернету, налаштовуємо ACL:

ciscoasa(config)# access-list FROM-OUTSIDE extended permit icmp any host 212.1.65.2

ciscoasa(config)# access-list FROM-OUTSIDE extended permit tcp any host 212.1.65.2 eq www

ciscoasa(config)# access-group FROM-OUTSIDE in interface outside

Проблеми та обмеження

Через обмеження Cisco Packet Tracer ми не можемо повністю реалізувати всі функціональні можливості обладнання Cisco. Наприклад, використання команди `no forward interface vlan 1` може призвести до того, що з приватної зони (внутрішньої мережі) ми не зможемо пінгувати сервер у DMZ. На реальному обладнанні ця проблема не виникає, оскільки там немає таких ліцензійних обмежень [18].

Підсумок

У результаті ми отримали мережу з трьома рівнями безпеки:

Security-level 99 (Inside): може ініціювати з'єднання до всіх інших зон.

Security-level 50 (DMZ): може ініціювати з'єднання лише до зон з нижчим рівнем безпеки (наприклад, до Інтернету).

Security-level 0 (Outside): не може ініціювати з'єднання до зон з вищим рівнем безпеки без явного дозволу в ACL.

Це означає, що:

1. Користувачі внутрішньої мережі можуть доступатися до серверів у DMZ та в Інтернеті.

2. Сервери в DMZ можуть доступатися до Інтернету, але не до внутрішньої мережі.

3. Зовнішні користувачі (з Інтернету) можуть доступатися лише до серверів у DMZ, якщо це дозволено в ACL.

Команди налаштування

Маршрутизатор R0:

R0(config)# ip route 212.1.65.0 255.255.255.252 212.1.64.132

Cisco ASA:

ciscoasa# configure terminal
ciscoasa(config)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 3
ciscoasa(config-if)# exit
ciscoasa(config)# interface vlan 3
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# no forward interface vlan 1
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 212.1.65.1 255.255.255.252
ciscoasa(config)# access-list FROM-OUTSIDE extended permit icmp any host 212.1.65.2
ciscoasa(config)# access-list FROM-OUTSIDE extended permit tcp any host 212.1.65.2 eq www
ciscoasa(config)# access-group FROM-OUTSIDE in interface outside

Висновок

Реалізація DMZ-зони дозволяє підвищити безпеку мережі, розділивши її на сегменти з різним рівнем довіри. Це мінімізує ризик для внутрішньої мережі у випадку компрометації публічних серверів. Хоча Cisco Packet Tracer має обмеження, які не дозволяють повністю розкрити потенціал обладнання Cisco, він все ж є корисним інструментом для моделювання базових мережевих сценаріїв та навчання.

3.4 Створення DMZ через налаштування ACL на маршрутизаторі

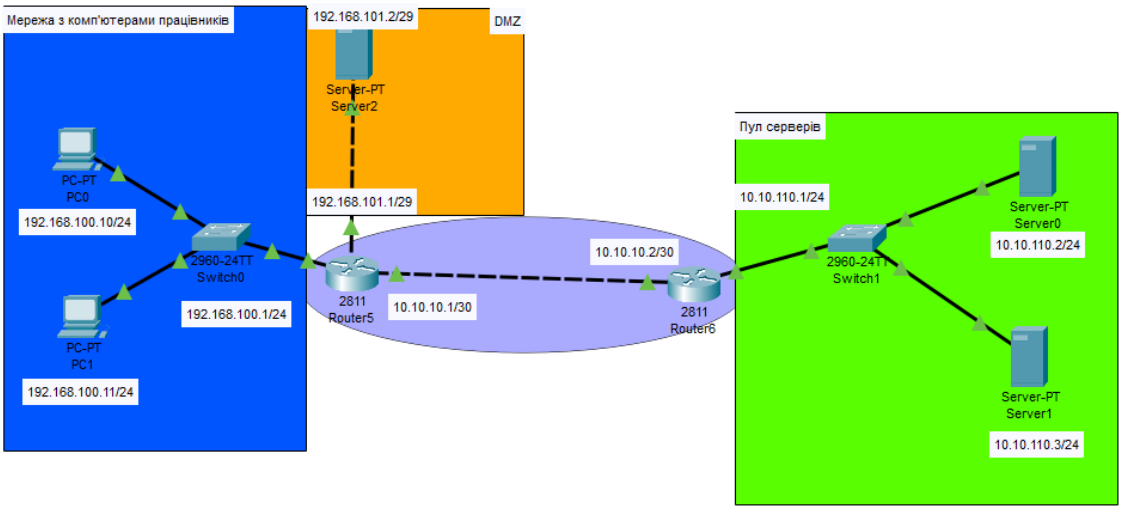


Рисунок 3.5 - Мережа з DMZ

На представленій схемі зображена локальна мережа, побудована для демонстрації налаштування зон мережі за допомогою списків контролю доступу (ACL). Мережа розбита на три основні зони: **Мережа з комп'ютерами працівників, DMZ-зона та зона пулу серверів.**

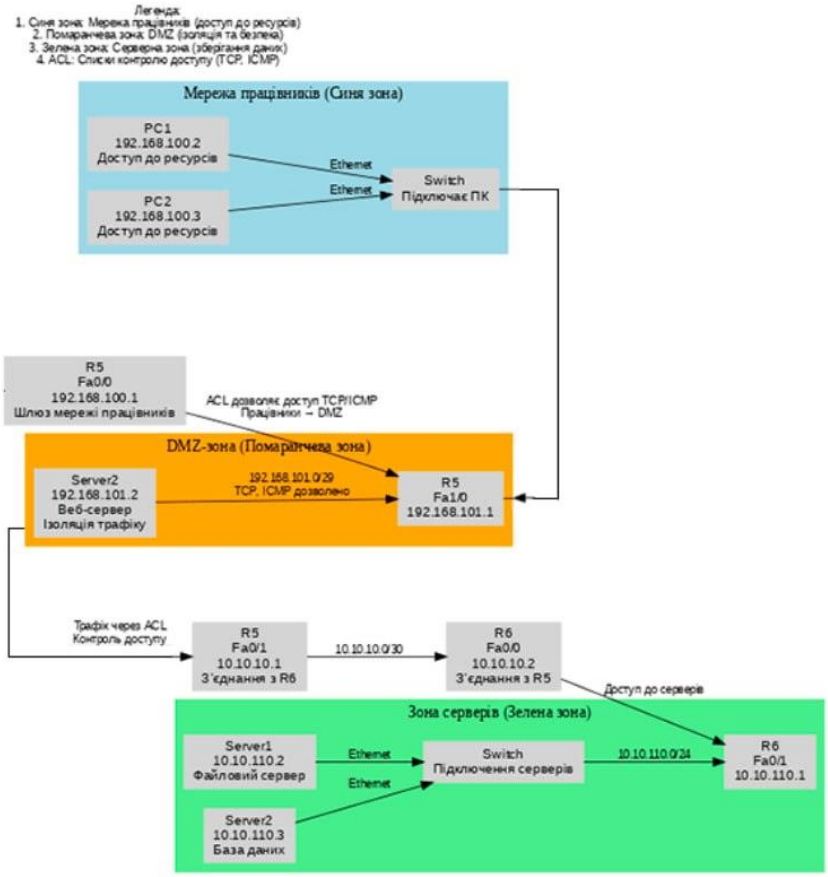


Рисунок 3.6 - Принцип роботи мережі

Мережа, зображена на рисунку 3.6 поділена на три основні зони для забезпечення сегментації та базової безпеки:

1. **Мережа працівників (синя зона):**

Ця зона включає два комп'ютери, підключені до комутатора.

Всі пристрої працюють у підмережі **192.168.100.0/24** зі шлюзом **192.168.100.1** (маршрутизатор R5).

Призначення зони — забезпечення доступу співробітників до внутрішніх ресурсів і зовнішніх мереж.

2. **DMZ-зона (помаранчева зона):**

Включає сервер (**Server2**) з IP-адресою **192.168.101.2**, ізольований від інших зон.

Трафік до цієї зони контролюється через ACL на маршрутизаторі R5, дозволяючи лише певний тип трафіку (TCP, ICMP).

Призначення зони — забезпечення безпеки для серверів, що обробляють зовнішні запити.

1. **Серверна зона (зелена зона):**

Складається з двох серверів (**Server1** та **Server2**) у підмережі **10.10.110.0/24**.

Сервери з'єднані через комутатор зі шлюзом **10.10.110.1** (маршрутизатор R6).

Призначення зони — зберігання даних та забезпечення доступу до серверних ресурсів.

2. **Міжзонова мережа:**

Зв’язує маршрутизатори R5 і R6 через підмережу **10.10.10.0/30** для обміну трафіком між зонами.

Таблиця 3.2 - Опис зон і компонентів

Зона	**Компоненти**	**IP-адреси**	**Призначення**
Мережа працівників	2 ПК, комутатор, маршрутизатор R5	192.168.100.0/24, шлюз 192.168.100.1	Доступ співробітників до ресурсів локальної та зовнішньої мережі.
DMZ-зона	Сервер (Server2), маршрутизатор R5	192.168.101.0/29, сервер 192.168.101.2	Ізоляція сервера для безпечного оброблення зовнішніх запитів.
Серверна зона	2 сервери (Server1, Server2), комутатор, маршрутизатор R6	10.10.110.0/24, шлюз 10.10.110.1	Зберігання даних і обробка запитів з інших зон.
Міжзонова мережа	З’єднання між маршрутизаторами R5 і R6	10.10.10.0/30	Обмін трафіком між зонами через маршрутизатори.

Основні функції мережі

1. **Сегментація трафіку:**

Зони ізольовані одна від одної для захисту від несанкціонованого доступу.

DMZ забезпечує проміжний рівень безпеки між зовнішньою та внутрішньою мережею.

1. **Контроль доступу:**

ACL на маршрутизаторі R5 обмежує доступ між зонами, дозволяючи лише потрібний тип трафіку.

Сервери в DMZ та серверній зоні захищені від прямого доступу з мережі працівників.

2. **Гнучкість:**

Мережа легко масштабується, додаючи нові сервери або підмережі.

3. **Простота адміністрування:**

ACL забезпечують централізоване управління доступом без складних рішень.

Ця схема і пояснення демонструють ефективний підхід до побудови безпечної мережі з DMZ для малого або середнього бізнесу.

Основні команди для налаштування:

Налаштування маршрутизатора R5:

```
Router>enable
Router#configure terminal
Router(config)#ip route 10.10.110.0 255.255.255.0 10.10.10.2
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 192.168.100.1 255.255.255.0
Router(config-if)#ip nat inside
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip address 10.10.10.1 255.255.255.252
Router(config-if)#ip nat outside
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fastEthernet 1/0
Router(config-if)#ip address 192.168.101.1 255.255.255.248
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#ip access-list standard PAT
Router(config-std-nacl)#permit 192.168.100.0 0.0.0.255
Router(config-std-nacl)#exit
Router(config)#ip nat inside source list PAT interface fastEthernet 0/1 overload
Router(config)#ip access-list extended DMZ
Router(config-ext-nacl)#deny ip host 192.168.101.2 192.168.100.0 0.0.0.255
Router(config-ext-nacl)#permit ip any any
```

```
Router(config-ext-nacl)#exit
Router(config)#interface fastEthernet 1/0
Router(config-if)#ip access-group DMZ in
Router(config-if)#exit
Router(config)#ip access-list extended outside
Router(config-ext-nacl)#permit icmp any host 192.168.101.2
Router(config-ext-nacl)#permit tcp any host 192.168.101.2
Router(config-ext-nacl)#deny ip any any
Router(config-ext-nacl)#exit
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip access-group outside in
Router(config-if)#exit
Router(config)#ip inspect name in-out http
Router(config)#ip inspect name in-out icmp
Router(config)#ip inspect name in-out tcp
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip inspect in-out in
Router(config-if)#exit
```

Налаштування маршрутизатора R6:

```
Router>enable
Router#configure terminal
Router(config)#ip route 192.168.100.0 255.255.255.0 10.10.10.1
Router(config)#ip route 192.168.101.0 255.255.255.248 10.10.10.1
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 10.10.10.2 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip address 10.10.110.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

Демонстрація налаштування DMZ через ACL:

Списки контролю доступу (ACL) на маршрутизаторі R5 використовуються для ізоляції DMZ-зони та контролю доступу до сервера 192.168.101.2. Дозволяється лише визначений тип трафіку (TCP, ICMP) до сервера в DMZ-зоні, а інший трафік блокується. ACL дозволяють обмежувати трафік між різними зонами мережі, зокрема між внутрішньою мережею працівників та серверною зоною.

Висновок

Дана мережа є прикладом ефективної сегментації локальної мережі для забезпечення базової безпеки та ізоляції зон з використанням списків контролю доступу (ACL). Вона складається з трьох ключових зон: мережі працівників, DMZ-зони та серверної зони. ACL на маршрутизаторі **R5** забезпечують розмежування трафіку між цими зонами, дозволяючи доступ лише до визначених ресурсів за чітко прописаними правилами.

Переваги мережі:

1. **Сегментація та контроль доступу:**

Кожна зона має свої чітко визначені функції, а доступ між ними контролюється за допомогою ACL. Це забезпечує захист внутрішніх ресурсів від несанкціонованого доступу.

2. **Простота реалізації:**

Використання ACL є відносно простим способом забезпечення базового захисту, особливо для невеликих або середніх мереж.

3. **Гнучкість налаштувань:**

ACL дозволяють детально налаштувати правила доступу, включаючи дозволи або заборони для конкретних типів трафіку.

Недоліки та обмеження:

1. **Обмежений рівень безпеки:**

ACL забезпечують лише базовий контроль доступу та не аналізують трафік на рівні додатків, що робить їх менш ефективними у випадку складних атак, таких як SQL-ін’єкції або DDoS.

2. **Складність масштабування:**

У великих мережах управління великими ACL-списками стає складним і неефективним, що може спричинити конфлікти правил або помилки в налаштуванні.

3. **Відсутність розширених функцій:**

Використання фаєрволу замість ACL дозволяє реалізувати більш глибокий аналіз трафіку, виявлення загроз і захист від атак на прикладному рівні.

3.5 Використання VPN-тунельних з'єднань для захисту локальних мереж: PPTP, L2TP та інші протоколи.

У сучасному цифровому світі захист даних у локальних мережах став невід'ємною частиною будь-якого бізнесу чи приватного користувача. Враховуючи зростаючу кількість кіберзагроз, зокрема хакерських атак, витоків інформації та несанкціонованого доступу до мереж, важливість надійного захисту комунікацій стала критичною.

Одним із найефективніших методів забезпечення безпеки є використання VPN-тунельних з'єднань, які створюють захищену «тунельну» оболонку для передачі даних між пристроями, що дозволяє запобігти перехопленню чи маніпуляціям з переданими даними.

Протоколи, такі як PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol), та інші, відіграють ключову роль у створенні таких захищених каналів зв'язку [19].

Принцип роботи VPN тунеля наступний:

VPN (Virtual Private Network) забезпечує створення зашифрованого тунелю між пристроями в мережі. Тунельне з'єднання дозволяє передавати дані через зашифровану сесію, захищаючи їх від несанкціонованого доступу та перехоплення. Протоколи, такі як PPTP і L2TP, виконують такі завдання:

1. **PPTP (Point-to-Point Tunneling Protocol):**

Використовує точку доступу для створення тунелю.

Простий у налаштуванні та сумісний з більшістю пристроїв.

PPTP — один із найстаріших і найбільш поширених протоколів для створення VPN-з'єднань. Він використовує метод тунелювання, який дозволяє обмінюватися даними між користувачем і віддаленим сервером, забезпечуючи певний рівень шифрування і автентифікації. Однією з основних переваг PPTP є простота налаштування і сумісність з більшістю операційних систем. Однак, незважаючи на свою популярність, PPTP має суттєві вразливості, зокрема слабке шифрування і відсутність підтримки сучасних стандартів безпеки. Це робить його менш надійним для захисту конфіденційних даних у порівнянні з новими протоколами.

2. **L2TP (Layer 2 Tunneling Protocol):**

Поєднує функціонал PPTP з додатковими рівнями безпеки.

Часто використовується разом із протоколом IPsec для покращення шифрування.

Більш стійкий до атак і забезпечує кращий захист для корпоративних даних.

3. **OpenVPN, IKEv2, WireGuard:**

Сучасні альтернативи, які забезпечують високий рівень захисту та оптимальну швидкість передачі даних.

VPN тунелі наступним чином захищають локальну мережу:

1. **Шифрування даних:** VPN-тунелі кодують дані, які передаються через мережу, роблячи їх недоступними для сторонніх осіб. Це особливо важливо у локальних мережах, де передається конфіденційна інформація, така як корпоративні документи чи фінансові звіти.
2. **Анонімність і приватність:** VPN приховує IP-адресу користувача, забезпечуючи анонімність у мережі. У локальних мережах це знижує ризик атак, спрямованих на конкретні пристрої.
3. **Захист від хакерів:** Завдяки тунельному шифруванню, навіть якщо зловмисник отримає доступ до мережевого трафіку, він не зможе прочитати або використати перехоплені дані.
4. **Захист від внутрішніх загроз:** VPN корисний не лише для захисту від зовнішніх атак, але й для забезпечення безпеки у випадку недобросовісних дій співробітників або ненавмисних витоків даних.

VPN тунелі в локальних мережах важливо використовувати по наступним причинам:

1. **Безпека даних у віддаленій роботі:** VPN дозволяє безпечно підключатися до локальної мережі підприємства, працюючи віддалено. Це особливо актуально для сучасних умов роботи, коли співробітники часто працюють із дому чи підключаються до мережі з публічних точок доступу.
2. **Відповідність нормативам:** У багатьох галузях, таких як фінанси чи медицина, використання VPN є вимогою законодавства для захисту даних клієнтів і дотримання стандартів кібербезпеки.
3. **Підвищення продуктивності:** За допомогою VPN можливо об'єднати кілька віддалених офісів в одну мережу, що спрощує обмін даними та співпрацю між відділами.
4. **Захист IoT-пристроїв:** У локальних мережах, що використовують розумні пристрої, VPN допомагає захистити ці пристрої від зовнішніх загроз.

Висновок

Використання VPN-тунельних з'єднань, таких як PPTP, L2TP та інших, є ефективним способом захисту локальних мереж. Ці технології забезпечують шифрування даних, захищають від атак і знижують ризики витоку інформації. Інвестування в налаштування VPN не лише забезпечує безпеку, але й підвищує довіру клієнтів, сприяє збереженню конфіденційності та дозволяє компаніям відповідати сучасним стандартам кібербезпеки. У сучасному світі, де дані є одним із найцінніших активів, використання VPN стає необхідністю, а не розкішшю.

3.6 Безпека бездротових мереж: ключ до захисту ваших даних

Безпека бездротових мереж є критично важливим аспектом у сучасному цифровому світі, де більшість пристроїв підключені до Wi-Fi. Ефективний захист забезпечує не лише конфіденційність даних, а й запобігає можливим загрозам. Розглянемо основні протоколи безпеки, типові загрози та значення шифрування трафіку у бездротових мережах.

Протоколи безпеки Wi-Fi: еволюція стандартів

1. **WEP (Wired Equivalent Privacy)**
   Перший протокол безпеки Wi-Fi, розроблений для забезпечення базового рівня захисту. Однак слабке шифрування (ключ 40 або 104 біт) робить його вразливим до зломів. На сьогодні WEP вважається застарілим і не рекомендується до використання.
2. **WPA (Wi-Fi Protected Access)**
   Створений для заміни WEP, WPA забезпечує покращене шифрування за допомогою протоколу TKIP (Temporal Key Integrity Protocol). Це стало значним покращенням, але залишилося певне вікно для атак.
3. **WPA2 (Wi-Fi Protected Access 2)**
   WPA2 впроваджує шифрування AES (Advanced Encryption Standard), що забезпечує високий рівень захисту. Він залишається основним стандартом безпеки Wi-Fi для багатьох пристроїв.
4. **WPA3**
   Остання версія протоколу, яка забезпечує ще вищий рівень захисту завдяки використанню SAE (Simultaneous Authentication of Equals). WPA3 стійкіший до атак словника і підтримує кращий захист у відкритих мережах

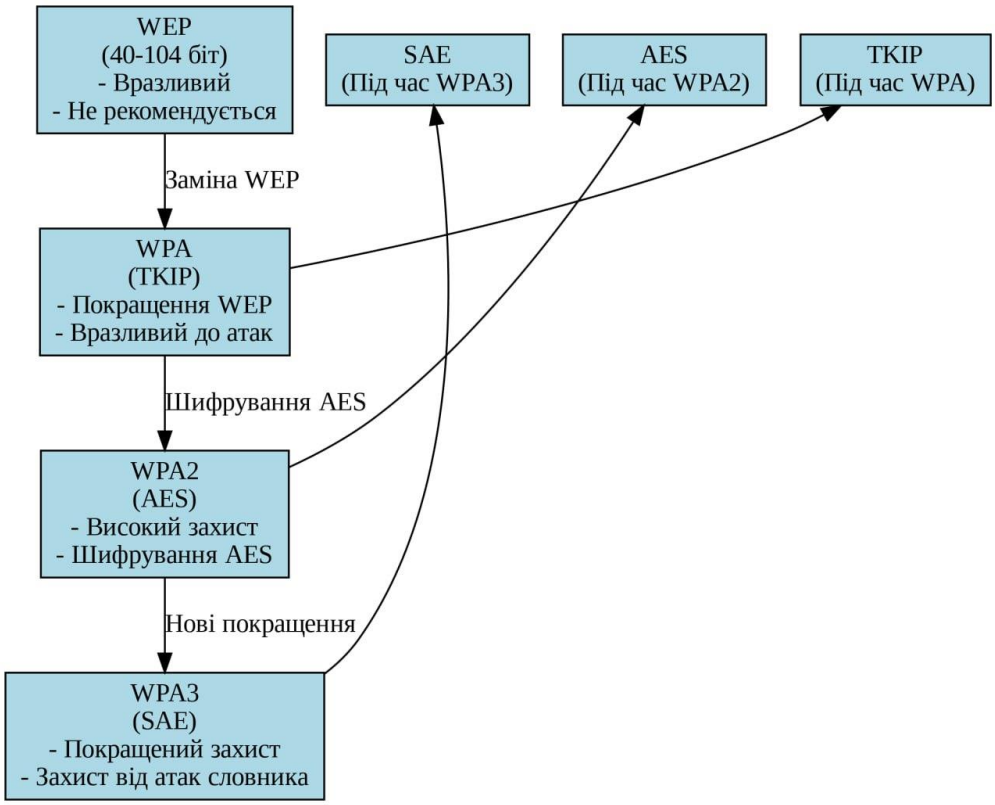


Рисунок 3.7 - Протоколи безпеки Wi-Fi

Загрози бездротових мереж: на що звертати увагу

1. **Evil Twin** Це атака, при якій зловмисник створює фальшиву точку доступу з ідентичним ім'ям (SSID), щоб обманом змусити користувачів підключитися до неї. Це дозволяє перехоплювати трафік і викрадати конфіденційну інформацію.

2. **Приховані точки доступу** Ці точки доступу не передають своє SSID, що робить їх важкими для виявлення. Вони можуть використовуватися зловмисниками для перехоплення даних або запуску атак на клієнтські пристрої.

Шифрування трафіку у бездротових мережах: захист у дії

Шифрування трафіку забезпечує перетворення даних у зашифрований формат, який неможливо прочитати без ключа. Це важливий крок для захисту інформації в локальній мережі. Ось чому шифрування є необхідністю:

Запобігання перехопленню: Зловмисники не зможуть отримати доступ до конфіденційної інформації навіть у разі перехоплення трафіку.

Захист від атак man-in-the-middle: Шифрування унеможливлює зміну або підробку переданих даних.

Забезпечення конфіденційності: Особиста інформація користувачів, паролі та дані карток залишаються недоступними для сторонніх осіб.

Сучасні стандарти, такі як WPA3, забезпечують більш ефективне шифрування і знижують ризик розкриття даних навіть у відкритих мережах.

Вибір надійного протоколу безпеки, як-от WPA2 або WPA3, і шифрування трафіку допомагає:

Забезпечити безпечний доступ до мережі.

Захистити дані від кіберзлочинців.

Запобігти несанкціонованому доступу до мережі.

Інтеграція цих технологій не лише підвищує рівень безпеки, а й створює довіру до використання бездротових мереж, що є важливим як для домашніх користувачів, так і для підприємств.

3.6 **Антивірусний захист у локальних мережах: огляд рішень Cisco Secure Endpoint та ESET**

Cisco Secure Endpoint (раніше відомий як AMP for Endpoints) — це комплексне рішення для захисту кінцевих точок, яке поєднує можливості виявлення та реагування на загрози (EDR) з розширеним виявленням та реагуванням (XDR). Це дозволяє організаціям ефективно виявляти, аналізувати та нейтралізувати загрози в реальному часі.

Основні можливості:

Виявлення та реагування на загрози (EDR): Забезпечує глибокий аналіз поведінки кінцевих точок для виявлення підозрілих дій та швидкого реагування на інциденти.

Розширене виявлення та реагування (XDR): Інтегрує дані з різних джерел безпеки, таких як мережеві пристрої та хмарні сервіси, для отримання повного огляду на загрози та їх контекст.

Хмарне управління: Дозволяє централізовано керувати політиками безпеки та отримувати оновлення в режимі реального часу через хмарну консоль.

Інтеграція з іншими рішеннями Cisco: Забезпечує спільну роботу з іншими продуктами безпеки Cisco, такими як SecureX, для покращення координації та автоматизації заходів безпеки.

Переваги використання Cisco Secure Endpoint:

Покращений захист: Забезпечує багаторівневий захист від сучасних загроз, включаючи шкідливе програмне забезпечення, фішинг та атаки нульового дня.

Підвищена ефективність операцій: Автоматизує процеси виявлення та реагування, зменшуючи навантаження на команди безпеки та скорочуючи час реагування на інциденти.

Масштабованість: Підходить для організацій будь-якого розміру, забезпечуючи гнучкість та адаптивність до змінних потреб бізнесу.

Рисунок 3.8 - Cisco Secure Endpoint

Cisco Secure Endpoint є високотехнологічним рішенням для комплексного захисту кінцевих пристроїв, яке чудово підходить для підприємств, що прагнуть отримати максимальний рівень безпеки. Це антивірусне програмне забезпечення використовує новітні хмарні технології, інтегрується з іншими продуктами Cisco та дозволяє контролювати мережу в реальному часі.

Основні можливості Cisco Secure Endpoint:

1. **Виявлення та блокування шкідливого ПЗ:** Cisco Secure Endpoint відстежує операції з файлами на кінцевих пристроях і використовує хмарні технології для автоматичного блокування шкідливих дій на основі політик безпеки. Це дозволяє швидко реагувати на загрози та запобігати їхньому поширенню мережею.
2. **Ретроспективний аналіз:** Рішення дозволяє виявляти невідомі раніше загрози шляхом аналізу їхньої поведінки. Такий підхід допомагає попередити повторні інциденти та забезпечити високий рівень безпеки в майбутньому.
3. **Контроль доступу та політик безпеки:** Адміністратори можуть створювати спеціальні політики для обмеження запуску нелегального або небезпечного програмного забезпечення, що знижує ризик зараження мережі.

Переваги Cisco Secure Endpoint:

Інтеграція з іншими системами Cisco для створення комплексного кіберзахисту.

Використання штучного інтелекту для адаптації до нових загроз.

Реагування на загрози в реальному часі завдяки хмарним технологіям.

Це рішення є ідеальним вибором для сучасних систем, які потребують не лише базового антивірусного захисту, а й детального аналізу та швидкого реагування.

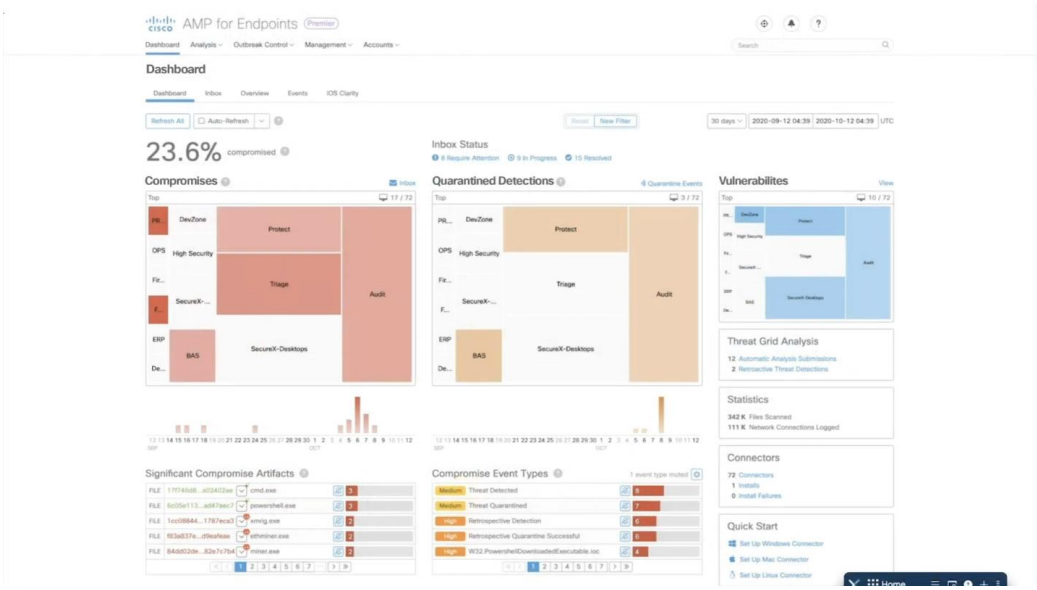


Рисунок 3.9 – Дашборд (Dashboard)

На зображенні представлена основна панель управління **Cisco Secure Endpoint**, яка забезпечує зручний та інтуїтивний огляд ключових показників безпеки системи. Панель демонструє відсоткове співвідношення компрометованих систем (у прикладі – 23.6%) та графічне представлення основних категорій компрометацій, таких як "Protect", "Triage" і "Audit".

Інформаційна панель надає короткий огляд поточного стану безпеки, включаючи компрометації (compromises), ізольовані загрози (quarantined detections) та вразливості (vulnerabilities). Окрім цього, вона містить детальний список значущих компрометаційних артефактів із назвами файлів, типами загроз і рівнем серйозності кожної події. Графічна візуалізація типів компрометаційних подій допомагає швидко оцінити природу загроз у середовищі.

Панель також забезпечує можливості для аналізу компрометованих систем. Це включає перегляд ключової інформації, такої як назва хоста, ім’я файлу, рівень серйозності та час виявлення. Таким чином, Cisco Secure Endpoint забезпечує прозорість у роботі системи безпеки, дозволяючи оперативно реагувати на загрози та забезпечувати високий рівень захисту інфраструктури.

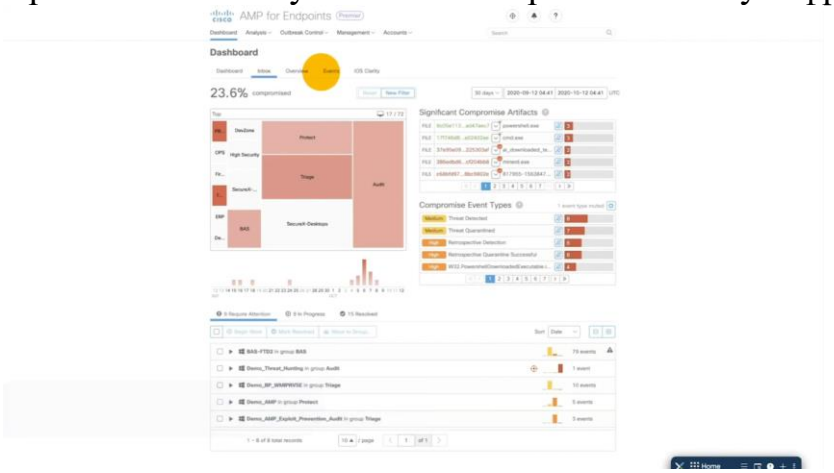


Рисунок 3.10 – Інбокс (Inbox)

Панель містить папку "Inbox", що дозволяє швидко вживати заходів проти компрометованих хостів, забезпечуючи ефективність і оперативність у роботі з інцидентами безпеки.

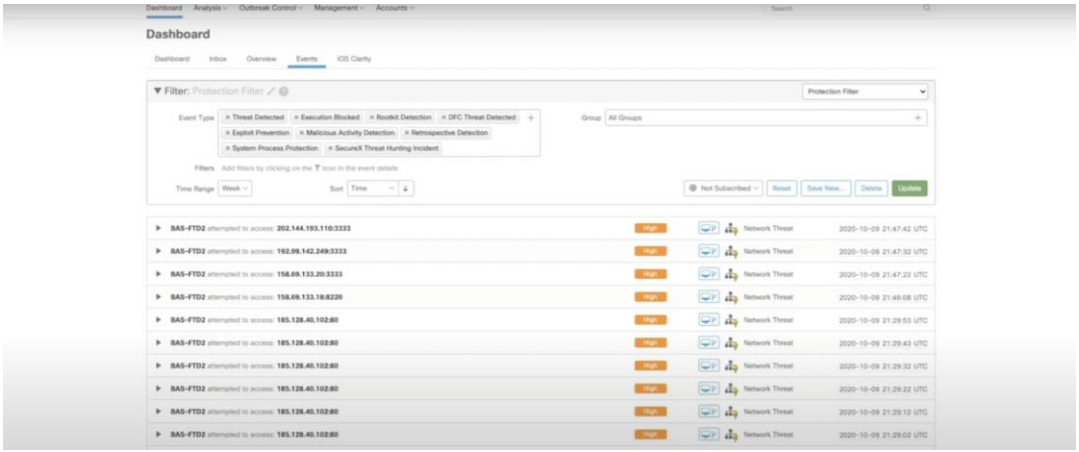


Рисунок 3.11 – Дашборд, евенти (Dashboard, Events)

На зображенні представлено розділ **Events** інформаційної панелі **Cisco Secure Endpoint**, який містить активний список подій у середовищі. Цей список забезпечує доступ до актуальної інформації про виявлені загрози, включаючи назви хостів, деталі інцидентів і час їхнього виявлення.

Панель також дозволяє фільтрувати події за різними категоріями, такими як **Threat Detected**, **Execution Blocked**, **Malicious Activity Detected**, та інші. Кожна подія супроводжується додатковими даними: типом загрози (наприклад, **Network Threat**), IP-адресою, рівнем серйозності й часом інциденту. Це дає змогу аналітикам швидко ідентифікувати джерело проблеми та вжити відповідних заходів.

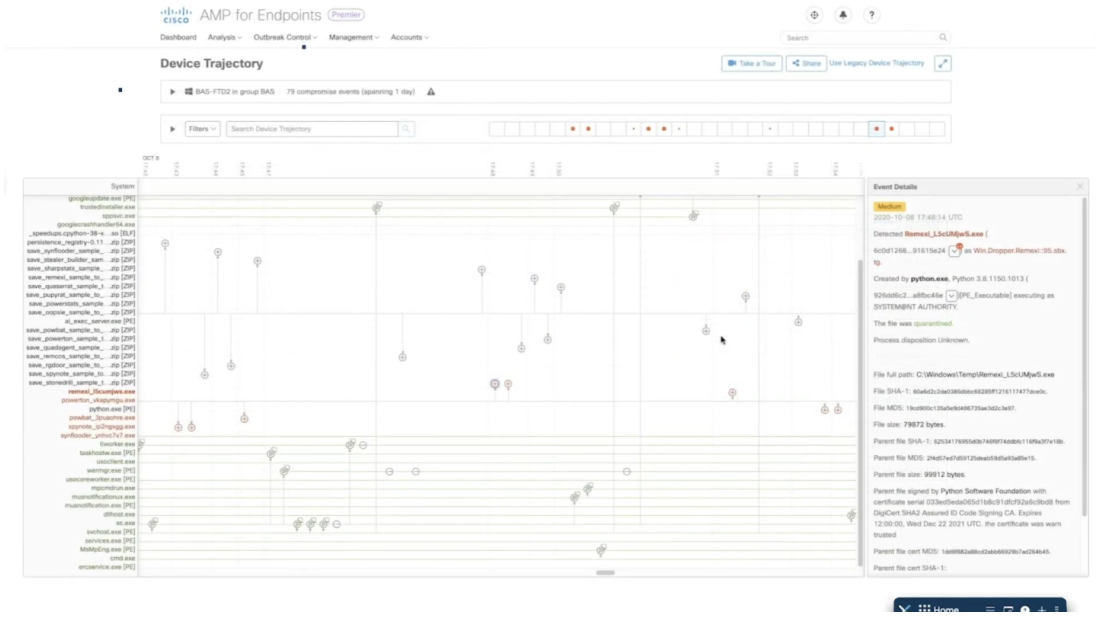


Рисунок 3.12 – Device Trajectory

На зображенні представлена секція **Device Trajectory** в інтерфейсі **Cisco Secure Endpoint**, яка забезпечує детальний огляд активності пристрою та історію подій, пов’язаних із виявленням загроз. Цей розділ дозволяє візуалізувати кожну подію, пов’язану з хостом, включаючи часову шкалу, що показує послідовність дій.

На траєкторії відображаються всі події, які здійснив пристрій, із позначками, що вказують на окремі точки інтересу. Користувачі можуть переглянути більш детальну інформацію про кожну подію, вибравши конкретну точку. Деталі включають:

1. Назву хоста та IP-адресу.
2. Тип події (наприклад, виявлення шкідливого програмного забезпечення чи поведінкової аномалії).
3. Час і контекст події.
4. Інформацію про відповідний файл чи процес (ім'я файлу, шлях до нього, хеш).

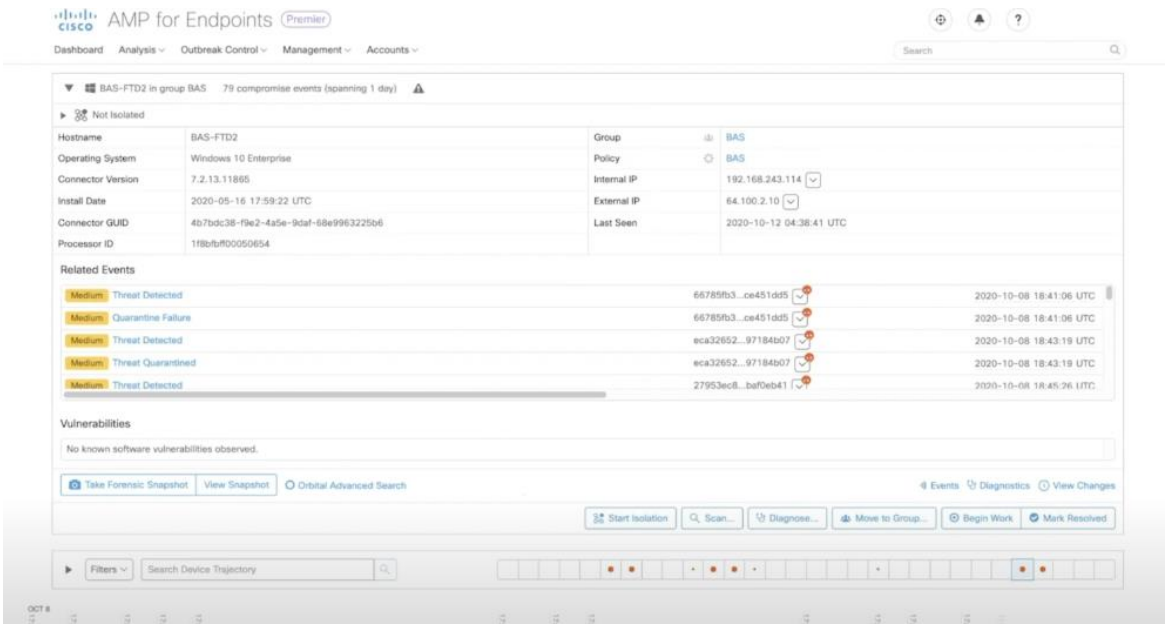


Рисунок 3.13 – Host Details

На зображенні представлено розділ **Host Details** в інтерфейсі **Cisco Secure Endpoint**, який надає ключову інформацію про пристрій та дозволяє оперативно реагувати на інциденти. У верхній частині показано короткий огляд системи, включаючи назву пристрою, операційну систему, IP-адреси та дату останнього виявлення.

Секція подій відображає пов’язані інциденти, такі як **Threat Detected** чи **Quarantine Failure**, із деталями про час, тип події та статус. Для швидкого реагування передбачена функція ізоляції пристрою від мережі, що мінімізує ризик поширення загроз.

Інструменти аналізу, такі як **Take Forensic Snapshot** та **Orbital Advanced Search**, дозволяють проводити глибокий аналіз інцидентів. Перша функція створює знімок системи, включаючи активні процеси, системні файли та заплановані завдання. Orbital Advanced Search забезпечує пошук у реальному часі з доступом до журналів активності та мережевих підключень.

Cisco Secure Endpoint також пропонує уніфікований аналіз шкідливих програм, який використовує статичний і динамічний підходи, зокрема пісочницю, для детального дослідження загроз. Контекстно-насичений інтелект дозволяє співвідносити результати з даними системи, забезпечуючи комплексний огляд інцидентів.

Для організацій, що прагнуть інтегрувати активне полювання на загрози, пакет **Premier** включає функції **Threat Hunting** за допомогою SecureX та команди експертів Cisco. Це забезпечує високу точність сповіщень і рекомендації для усунення загроз. Платформа SecureX дозволяє централізувати управління безпекою та інтегрувати всі можливості Cisco Secure Endpoint.

Рисунок 3.14 - Антивірус ESET

Якщо **Cisco Secure Endpoint** орієнтований переважно на сучасні системи, то **ESET** є оптимальним вибором для застарілих пристроїв, які все ще підключені до мережі Інтернет. Програма поєднує високу стабільність із простотою використання та мінімальними системними вимогами. Її багатофункціональний інтерфейс, як показано на ілюстрації, сприяє зрозумілому і ефективному управлінню захистом.

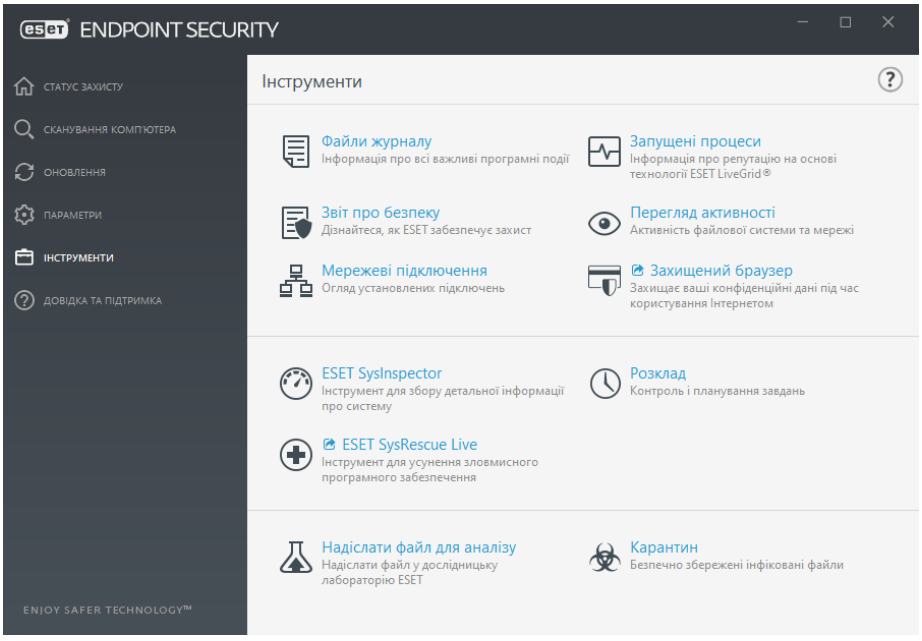


Рисунок 3.15 – Інтерфейс ESET Endpoint Security

На зображенні представлено функціонал розділу "Інструменти" програми **ESET Endpoint Security**, який включає набір засобів для моніторингу, діагностики та захисту системи. Інтерфейс організований логічно та інтуїтивно, зручно для користувачів із будь-яким рівнем технічної підготовки.

Таблиця, яка описує функціонал основних інструментів програми **ESET Endpoint Security**:

Таблиця 3.3 – Функціонал ESET Endpoint Security

Інструмент	Опис
Файли журналу	Забезпечують детальну інформацію про всі важливі події у програмі, дозволяючи аналізувати та відслідковувати стан системи.
Запущені процеси	Показують інформацію про активні процеси з використанням технології **ESET LiveGrid**, що оцінює їхню репутацію та потенційні загрози.
Звіт про безпеку	Надає повний огляд рівня безпеки системи, дозволяючи користувачеві швидко оцінити поточний стан захисту.
Перегляд активності	Відображає активність файлової системи та мережевих з'єднань, допомагаючи ідентифікувати підозрілі дії.
Мережеві підключення	Показують список активних підключень до мережі, що дозволяє виявляти небезпечні або підозрілі з'єднання.
Захищений браузер	Створює безпечне середовище для перегляду вебсайтів, забезпечуючи захист конфіденційних даних (паролів, банківських карт тощо).
ESET SysInspector	Інструмент для збору детальної інформації про систему, корисний для діагностики й виявлення проблем.
Розклад	Дозволяє налаштувати автоматизацію завдань, таких як регулярне сканування або оновлення програмного забезпечення.
ESET SysRescue Live	Призначений для видалення зловмисного програмного забезпечення, відновлення системи без загрози для важливих файлів.
Надіслати файл для аналізу	Забезпечує можливість відправлення підозрілих файлів до лабораторії **ESET** для детального дослідження.

Основні можливості ESET:

1. **Багаторівневий захист:** ESET використовує евристичний аналіз, сигнатурні бази даних та хмарний аналіз для виявлення як відомих, так і нових загроз.
2. **Мінімальне навантаження на систему:** Антивірус оптимізований для роботи на пристроях з обмеженими ресурсами, забезпечуючи швидке сканування без значного впливу на продуктивність системи.
3. **Захист від атак нульового дня:** Постійні оновлення хмарної бази дозволяють оперативно виявляти нові загрози, що важливо для старих комп'ютерів із високим ризиком вразливостей.
4. **Зручний інтерфейс:** Простий і зрозумілий інтерфейс дозволяє користувачам легко налаштовувати захист і запускати сканування без необхідності спеціальних технічних знань.

Переваги ESET:

Легкість у встановленні та використанні.

Низькі системні вимоги, що робить його ефективним навіть для старих пристроїв.

Додатковий захист від фішингових атак і небезпечних вебсайтів.

ESET забезпечує базовий рівень захисту без значного навантаження на систему, що дозволяє використовувати його на комп'ютерах із застарілим апаратним забезпеченням.

Висновок

Обираючи антивірусне рішення для локальної мережі, необхідно враховувати технічний стан пристроїв, вимоги до захисту та тип загроз, з якими вони можуть зіткнутися.

Cisco Secure Endpoint стане ідеальним вибором для сучасних систем із високими вимогами до безпеки, забезпечуючи ретроспективний аналіз і швидке реагування на загрози.

ESET підходить для старих пристроїв із обмеженими ресурсами, які потребують надійного захисту без значного впливу на продуктивність.

Поєднання цих двох рішень дозволяє створити оптимальну систему захисту, адаптовану до особливостей кожного пристрою в локальній мережі.

Криптографія в захисті мереж: сучасні рішення для забезпечення безпеки

Криптографія є ключовим інструментом у забезпеченні безпеки мереж, що дозволяє захистити конфіденційність, цілісність та автентичність даних. У сучасних умовах зростаючих кіберзагроз використання криптографічних методів стало невід'ємною частиною функціонування як великих підприємств, так і невеликих організацій.

Симетричне та асиметричне шифрування: різниця та приклади

1. **Симетричне шифрування (AES)**

Симетричні алгоритми шифрування, такі як AES (Advanced Encryption Standard), використовують один ключ для шифрування та розшифрування даних. Цей метод ефективний і швидкий, тому його застосовують для захисту великих обсягів інформації, наприклад, під час передачі файлів чи шифрування баз даних. Недоліком є необхідність захищеного обміну ключами між сторонами.

2. **Асиметричне шифрування (RSA)**

На відміну від симетричного, асиметричне шифрування, зокрема RSA (Rivest–Shamir–Adleman), використовує пару ключів — публічний і приватний. Публічний ключ доступний усім, а приватний зберігається у таємниці. Цей підхід забезпечує безпечний обмін інформацією між сторонами, навіть якщо вони раніше не контактували. Асиметричне шифрування широко використовується в електронному підписі та сертифікатах.

SSL/TLS-сертифікати: фундамент веб-захисту

Сертифікати SSL/TLS забезпечують шифрування зв’язку між клієнтом і сервером, захищаючи дані від несанкціонованого доступу. Наприклад:

SSL (Secure Sockets Layer) та **TLS (Transport Layer Security)** використовуються для забезпечення безпеки при передачі конфіденційної інформації, такої як паролі чи платіжні дані.

Наявність SSL/TLS-сертифіката гарантує, що сайт використовує захищений протокол HTTPS, забезпечуючи довіру користувачів.

Протоколи безпеки IPsec та HTTPS

1. **IPsec (Internet Protocol Security)**

IPsec шифрує дані на рівні мережевого протоколу, забезпечуючи конфіденційність і цілісність переданих пакетів. Цей протокол часто застосовується у VPN (віртуальних приватних мережах), що дозволяє безпечно підключатися до корпоративних мереж з віддалених пристроїв.

2. **HTTPS (Hypertext Transfer Protocol Secure)**

HTTPS, по суті, є HTTP-протоколом у поєднанні із SSL/TLS. Він забезпечує захищений доступ до вебсайтів, запобігаючи витоку особистих даних і атак типу «людина посередині» (MITM).

Практичний досвід: криптографія у використанні ключ-носіїв

На підприємстві, де я проходив практику, використовуються ключ-носії, які за виглядом нагадують звичайні флешки. Ці пристрої застосовуються для входу в бази даних через інтернет з різних пристроїв. Ключ-носій зберігає криптографічні ключі, які забезпечують автентифікацію користувача та шифрування з'єднання. Завдяки цьому доступ до корпоративних ресурсів стає захищеним навіть у разі використання відкритих мереж.

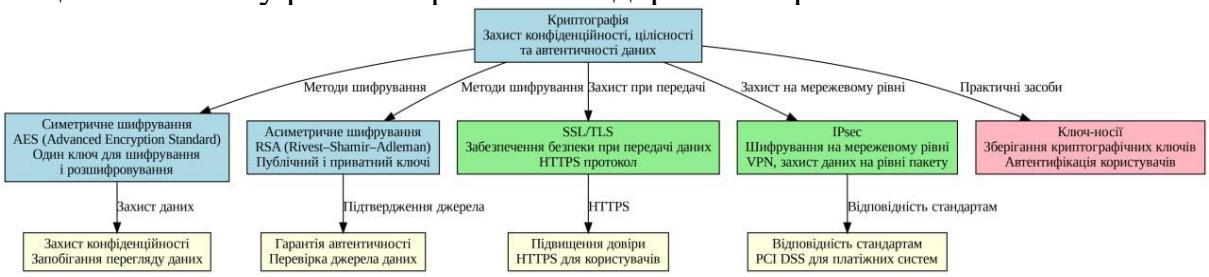


Рисунок 3.16 - Використання криптографії на практиці

Такий підхід потрібно використовувати тому що він гарантує:

1. **Захист конфіденційності**

Шифрування даних запобігає їх перегляду сторонніми особами під час передачі в мережі.

2. **Гарантія автентичності**

Криптографія дозволяє переконатися, що дані походять від надійного джерела, запобігаючи підміні інформації.

3. **Підвищення довіри**

Наявність захищеного з'єднання (HTTPS) підвищує довіру клієнтів до вебсайтів і сервісів.

4. **Відповідність стандартам безпеки**

Використання криптографії є обов'язковим для виконання багатьох міжнародних стандартів, наприклад, PCI DSS (для платіжних систем).

Таким чином, криптографія є основою для побудови безпечних мереж, що забезпечують захист даних у сучасному цифровому середовищі. Використання таких технологій, як AES, RSA, SSL/TLS, IPsec, а також апаратних ключів, дозволяє мінімізувати ризики та забезпечити безпеку інформації в будь-якому середовищі.

Резервування та відновлення: Ключ до стійкості та безпеки інформаційних систем

Резервування та відновлення є основоположними компонентами сучасної стратегії захисту інформації, які спрямовані на забезпечення цілісності, доступності та конфіденційності даних навіть у разі виникнення критичних ситуацій. У контексті зростаючих кіберзагроз і високої залежності бізнесу від технологій, ці заходи набувають ще більшого значення.

Роль резервних копій у забезпеченні захисту від атак і збоїв не можна недооцінювати. Резервне копіювання, або бекап, є процедурою створення копій даних, які зберігаються окремо від основних інформаційних систем. Такі копії слугують останньою лінією оборони у разі атак зловмисників, технічних збоїв або людських помилок. Наприклад, під час атак програм-вимагачів, які шифрують дані та вимагають викуп, наявність актуальних резервних копій дозволяє відновити інформацію без необхідності співпрацювати із зловмисниками. Крім того, резервування забезпечує захист у разі збоїв у роботі обладнання, коли апаратні несправності можуть спричинити втрату критично важливої інформації. Завдяки резервним копіям організації можуть швидко відновити доступ до даних, що мінімізує час простою бізнес-процесів і запобігає значним фінансовим втратам [20].

Процедури резервного копіювання вимагають чіткого дотримання правил. Зокрема, дані мають регулярно копіюватися за допомогою автоматизованих систем, які гарантують актуальність резервів. Також важливим аспектом є зберігання копій у географічно віддалених локаціях або хмарних сервісах для запобігання втратам у разі локальних катастроф, таких як пожежі, затоплення чи стихійні лиха. Не менш значущим є періодичний аудит резервних копій для перевірки їхньої доступності, цілісності та придатності для відновлення.

Планування процедур відновлення після інцидентів є критично важливим етапом захисту інформаційних систем. План відновлення після інцидентів, або Disaster Recovery Plan (DRP), представляє собою структурований документ, що визначає чіткі кроки для оперативного відновлення роботи систем після аварій чи атак. Його розробка включає аналіз ризиків, що можуть загрожувати інфраструктурі, оцінку ймовірності їхнього виникнення та впливу на бізнес.

Важливим аспектом є визначення пріоритетів: які дані та системи потребують відновлення в першу чергу для мінімізації впливу інциденту на ключові бізнес-процеси. У DRP також прописуються ролі й обов'язки відповідальних осіб, які мають чітко знати свої функції під час реалізації відновлення. Регулярне тестування цього плану дозволяє виявити слабкі місця, внести необхідні корективи й забезпечити готовність до непередбачуваних ситуацій.

Тестування систем на витривалість до атак є невіддільною складовою комплексного підходу до інформаційної безпеки. Завдяки моделюванню реальних сценаріїв атак організації можуть перевірити захищеність своїх систем, ідентифікувати слабкі місця та усунути їх до того, як ними скористаються зловмисники. Пентестинг, або тестування на проникнення, є одним із найпоширеніших методів, що передбачає імітацію дій кіберзлочинців. Навантажувальне тестування дає змогу оцінити, як система поводитиметься в умовах підвищеного навантаження, зокрема під час пікових періодів роботи чи під час DDoS-атак. Окремо варто зазначити про тестування резервних копій: перевірка їхньої доступності та працездатності є важливою складовою, яка гарантує можливість швидкого відновлення після інциденту.

Використання резервування та відновлення не лише знижує ризики втрати даних, а й сприяє збереженню репутації організації, забезпечує відповідність вимогам регуляторних органів і мінімізує фінансові збитки. Інформаційна безпека — це не тільки захист від кіберзагроз, а й інвестиція в стабільність бізнесу, яка дозволяє впевнено працювати навіть в умовах сучасних викликів.

Захист мереж на основі хмарних технологій

Таблиця 3.4 – Принципи захисту мережі на основі хмарних технологій

Розділ	Підрозділ	Опис	Приклади/Методи
Моделі захисту в хмарних середовищах	**IaaS (Infrastructure as a Service)**	Забезпечення безпеки базової інфраструктури: серверів, зберігання даних, мережевих компонентів, віртуалізації.	- Гіпервізори з інтегрованим захистом (VMware, Hyper-V) - Модульна архітектура мереж з використанням SDN - IDS/IPS для моніторингу та запобігання атакам

Продовження таблиці 3.4

	PaaS (Platform as a Service)	Забезпечення безпеки середовищ для розробки та розгортання додатків, включаючи бази даних, інструменти розробки, API.	- Використання контейнеризації (Docker, Kubernetes) - Верифікація коду та сканування вразливостей - API Gateway з функціями перевірки та моніторингу
	SaaS (Software as a Service)	Захист кінцевих користувачів і їхніх даних, доступу до хмарних додатків.	- SAML для єдиного входу (SSO) - Впровадження політики "Zero Trust" - Захист електронної пошти (email security gateways)
Захист даних під час передачі та зберігання	**Передача даних**	Забезпечення цілісності та конфіденційності інформації під час її передачі через мережі (локальні та глобальні).	- Використання SSL/TLS 1.3 - Протоколи обміну ключами (Diffie-Hellman, ECDHE) - Засоби моніторингу мережевого трафіку (NetFlow, Wireshark)

Продовження таблиці 3.4

	Зберігання даних	Захист чутливих даних у хмарних сховищах, запобігання витоку або несанкціонованого доступу до даних.	- Розподілене зберігання даних (Amazon S3, Google Cloud Storage) - Шифрування на стороні клієнта (E2EE) - Багатофакторна автентифікація для доступу до даних
Загрози та методи їхнього уникнення в хмарних середовищах	**Загрози**	Опис основних загроз, включаючи ризики через конфігураційні помилки, вразливості в програмному забезпеченні, соціальну інженерію.	- Фішингові атаки для отримання облікових даних користувачів - Експлойти, спрямовані на недоліки API - Атаки на відмову в обслуговуванні (DDoS)
	Методи уникнення	Використання технологій, методик та політик для мінімізації ризиків і ліквідації наслідків інцидентів.	- Налаштування політики шифрування даних "in-transit" і "at-rest" - Використання WAF (Web Application Firewall) - Резервне копіювання та планування відновлення після збоїв (DRP, BCP)

Продовження таблиці 3.4

Додаткові аспекти захисту	**Виявлення та реагування на інциденти**	Розробка інструментів і стратегій для моніторингу та оперативного реагування на інциденти кібербезпеки.	- SIEM-системи (Splunk, ArcSight) - Автоматизація реагування через SOAR (Security Orchestration, Automation, and Response) - Використання honeypot-систем для виявлення атак
	Управління доступом і ідентифікацією (IAM)	Забезпечення, що користувачі отримують лише ті привілеї, які необхідні для їхньої роботи.	- Системи управління доступом (Okta, Azure AD) - RBAC (Role-Based Access Control) - Використання U2F (Universal 2nd Factor) ключів для автентифікації
	Регуляторні та правові аспекти	Відповідність хмарних провайдерів та користувачів міжнародним стандартам та регуляторним вимогам.	- Відповідність стандартам GDPR, HIPAA, ISO/IEC 27001 - Укладання SLA (Service Level Agreement) з чіткими вимогами щодо безпеки

Продовження таблиці 3.4

	Освіта та підвищення обізнаності користувачів	Навчання користувачів основам безпеки для зниження ризиків соціальної інженерії та неправильної роботи з хмарними ресурсами.	- Регулярні тренінги з кібербезпеки - Симуляції фішингових атак - Впровадження політики використання особистих пристроїв (BYOD) з безпечними налаштуваннями
Інноваційні підходи до захисту	**Штучний інтелект та машинне навчання**	Використання AI/ML для аналізу аномалій, передбачення атак та автоматизації захисту.	- Виявлення аномальної поведінки користувачів та пристроїв (UEBA) - Автоматичне блокування підозрілої активності через AI-системи - Аналітика великих даних для пошуку потенційних вразливостей
	Квантова криптографія	Захист даних з використанням квантового шифрування для протидії квантовим обчисленням, які можуть розшифрувати традиційні алгоритми.	- Використання протоколів BB84 для захищеного обміну ключами - Інтеграція квантового шифрування у VPN та мережеві середовища

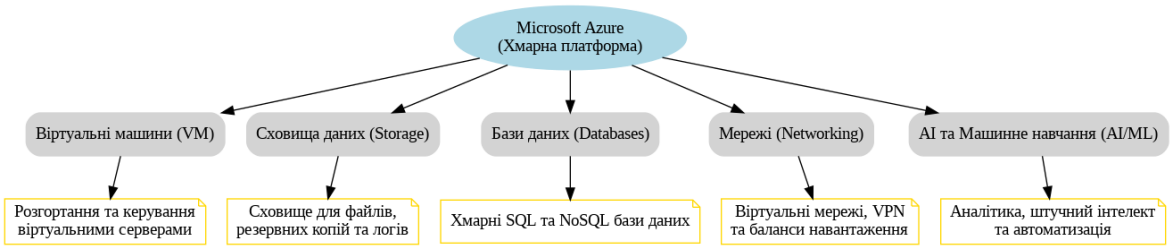


Рисунок 3.17 – Функціонал хмарної платформи Microsoft Azure

На основі поданої блок-схеми, яка демонструє принцип роботи Microsoft Azure, можна побачити, як ключові компоненти хмарної платформи взаємодіють між собою для забезпечення повного спектра послуг. Віртуальні машини (VM) у цій архітектурі займають центральне місце в розгортанні та управлінні віртуальними серверами. Вони дозволяють створювати потужні обчислювальні середовища для виконання різноманітних завдань, таких як тестування програмного забезпечення або хостинг веб-сервісів, що зображено у вигляді окремого блоку в схемі.

Сховище даних (Storage), яке представлено наступним компонентом, забезпечує сховище для файлів, резервних копій і логів. Цей елемент на схемі пов’язаний із забезпеченням постійної доступності даних для інших сервісів. Наприклад, лог-файли чи резервні копії баз даних можуть бути автоматично збережені у сховищах Azure, що гарантує захищеність навіть у разі апаратних збоїв.

Останній блок на схемі — AI/ML (штучний інтелект і машинне навчання) — демонструє потужність аналітичних інструментів Azure. Цей компонент використовується для аналізу даних, створення інтелектуальних моделей і автоматизації бізнес-процесів. Як приклад, компанія може прогнозувати попит на продукцію або аналізувати поведінку клієнтів, використовуючи сервіси машинного навчання Azure.

Таким чином, блок-схема чітко відображає структуру Microsoft Azure та демонструє, як різні компоненти взаємодіють для побудови єдиної, ефективної хмарної екосистеми, яка може бути адаптована під потреби різних бізнес-завдань.

Дослідження методів запобігання DDoS-атакам за допомогою NGINX Proxy Manager, Traefik, Cloudflare та інших технологій

Розподілені атаки на відмову в обслуговуванні (Distributed Denial of Service, DDoS) та атаки на відмову в обслуговуванні (Denial of Service, DoS) є одними з найсерйозніших загроз для сучасної інтернет-інфраструктури. Вони спрямовані на перевантаження серверів або мережевих ресурсів запитами, що призводить до їхньої недоступності для законних користувачів. Це дослідження розглядає механізми роботи цих атак, їхню природу, а також методи протидії за допомогою різних програмних рішень, зокрема **NGINX Proxy Manager**, **Traefik**, **Cloudflare** та інших технологій.

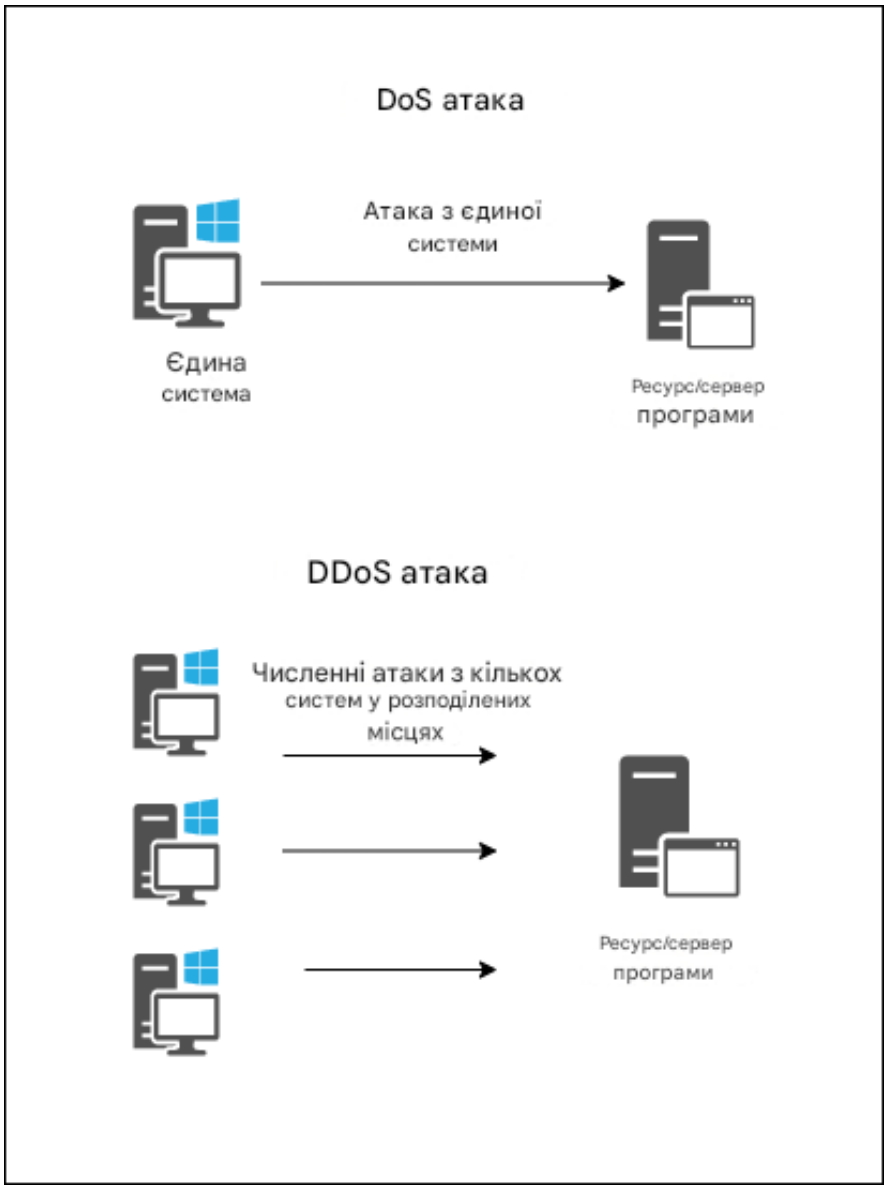


Рисунок 3.18 - Моделювання ДОС і ДДОс атаки

DoS-атаки здійснюються шляхом відправлення великої кількості запитів до цільового сервера з метою вичерпання його ресурсів. На відміну від них, **DDoS-атаки** залучають велику кількість пристроїв (зазвичай заражених ботнетом), які одночасно здійснюють масовану атаку.

Рисунок 3.19 - NGINX Proxy Manager

NGINX Proxy Manager є інструментом для реверс-проксі, що використовується для управління веб-запитами. Його основна мета — забезпечити маршрутизацію запитів, балансування навантаження та захист від атак.

Принцип роботи:

NGINX Proxy Manager функціонує як "фільтр" для вхідного трафіку. Уявіть собі вхід до театру, де кожен глядач повинен пройти перевірку квитка. NGINX Proxy Manager — це контролер, який перевіряє, чи має кожен відвідувач дійсний квиток (коректний запит). У разі виявлення нелегітимного відвідувача (шкідливого запиту), доступ блокується.

Як це зупиняє DDoS:

Обмеження швидкості: встановлення ліміту на кількість запитів від однієї IP-адреси.

Фільтрування запитів: блокування підозрілих заголовків HTTP або запитів, що не відповідають очікуваним шаблонам.

Балансування навантаження: розподіл запитів між кількома серверами.

Рисунок 3.20 - Traefik

Traefik

Traefik — це динамічний реверс-проксі, що автоматично інтегрується з контейнеризованими середовищами, такими як Docker або Kubernetes.

Принцип роботи:

Traefik подібний до розумного регулювальника дорожнього руху. Уявіть перегружене перехрестя, де потік машин (запитів) потрібно спрямувати до правильного пункту призначення (серверів). Traefik використовує динамічні конфігурації, щоб автоматично оновлювати маршрути і запобігати заторам.

Захист від DDoS:

Rate limiting: обмеження кількості запитів за певний час.

Middleware-фільтри: додаткові шари захисту, які аналізують запити на основі метаданих.

Інтеграція з іншими сервісами захисту: наприклад, Cloudflare.

Рисунок 3.21 - Cloudflare

Cloudflare

Cloudflare — це хмарна платформа, яка забезпечує масштабний захист від DDoS-атак.

Принцип роботи:

Cloudflare діє як "щит" перед вашим сервером. Уявіть собі фортецю, оточену стіною, через яку можуть пройти лише ті, хто пройшов перевірку. Cloudflare розміщує свій сервер перед вашим і перенаправляє весь трафік через себе.

Технології Cloudflare:

WAF (Web Application Firewall): блокує шкідливі запити.

Anycast: розподіляє трафік між кількома датацентрами.

Rate limiting: запобігає перевантаженню шляхом встановлення лімітів на запити.

Bot Management: виявлення та блокування автоматизованого трафіку.

Таблиця 3.5 - Порівняння технологій

Технологія	**Принцип дії**	**Переваги**	**Обмеження**
NGINX Proxy Manager	Реверс-проксі	Простота налаштування, обмеження швидкості	Менш ефективний для L3/L4 атак
Traefik	Динамічний реверс-проксі	Автоматизація, інтеграція з Docker/Kubernetes	Вимагає складнішої конфігурації
Cloudflare	Хмарний захист	Масштабованість, захист від L3-L7 атак	Додаткова затримка для трафіку
Geo-blocking	Блокування регіонів	Ефективність проти регіональних атак	Не працює для глобальних атак

Висновок до розділу 3

Ефективний захист від DoS та DDoS атак вимагає багаторівневого підходу, що включає використання таких інструментів, як NGINX Proxy Manager, Traefik і Cloudflare. Вони забезпечують баланс між локальним і глобальним захистом, дозволяючи знижувати ризик від атак на мережу та додатки. Вибір конкретної технології залежить від архітектури системи та рівня загроз, з якими вона стикається.

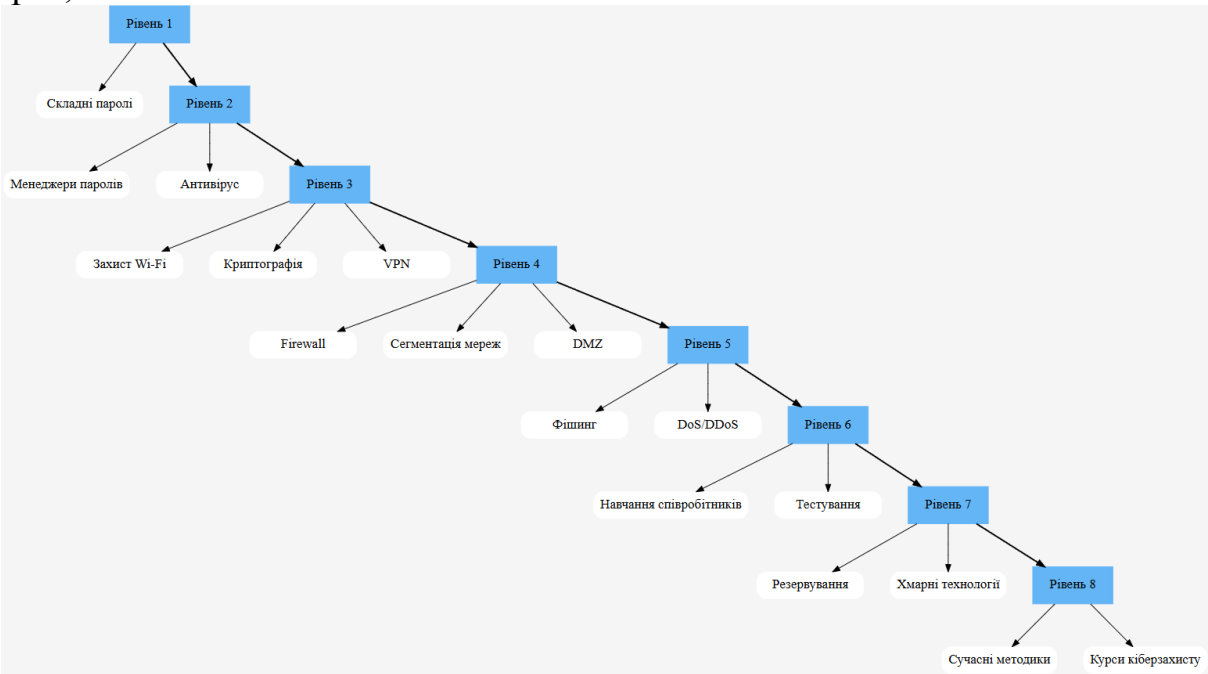


Рисунок 3.22 - Модель захисту функціональної організації та конфігурації фізичних компонентів комп'ютерних мереж

ВИСНОВОК

Актуальність проведених досліджень визначається швидким розвитком комп'ютерних мереж, які стали невід'ємною частиною сучасного суспільства, забезпечуючи критично важливі функції передачі даних, комунікацій та обміну інформацією. Зі зростанням складності мереж підвищується необхідність забезпечення їх захисту, особливо у контексті фізичних компонентів, які формують основу мережевої архітектури. Недостатній рівень захищеності цих компонентів може призвести до суттєвих ризиків для організацій та інфраструктур.

Розробка моделі захисту функціональної організації та конфігурації фізичних компонентів є важливим завданням, спрямованим на підвищення безпеки мережевих інфраструктур.
У ході дослідження проведено аналіз сучасних методів та моделей захисту, таких як сегментація мереж, використання брандмауерів, систем запобігання вторгнень та пісочниць (Sandbox). Окремо досліджено види кіберзагроз, включаючи фішинг, шкідливе програмне забезпечення, атаки на відмову в обслуговуванні (DDoS) та захоплення корпоративних рахунків (CATO), а також методи їхнього виявлення та протидії.

Методологія роботи базується на моделюванні та емпіричних дослідженнях. Розроблено математичну модель захисту, яка враховує специфіку функціональної організації мережевих компонентів та сучасні виклики кібербезпеки. Запропонована модель була перевірена в умовах експериментального середовища з використанням актуального активного та пасивного мережевого обладнання. Зокрема, проведено тестування роботи маршрутизаторів, комутаторів, точок доступу, кабельних систем, що забезпечують фізичну інфраструктуру мережі.
Наукова новизна роботи полягає у створенні нової моделі захисту, яка спрямована на зниження ризику несанкціонованого доступу до фізичних компонентів мережі та підвищення її стійкості до зовнішніх загроз.

Практичне значення полягає у можливості впровадження розробленої моделі для забезпечення безпеки інформаційних систем різного масштабу. Отримані результати підтверджують ефективність запропонованого підходу до захисту фізичних компонентів комп'ютерних мереж, що дозволяє значно знизити ризики, пов'язані з кіберзагрозами, забезпечити безперебійність функціонування мережі та її надійність у сучасних умовах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Marin, G. (2005). Network Security Basics. *IEEE Secur. Priv.*, 3, 68-72. URL: https://doi.org/10.1109/MSP.2005.153.
2. Cato, N. (2017). On Next Generation Network Security. *IEEE Netw.*, 31, 2. URL: https://doi.org/10.1109/MNET.2017.7884939.
3. Fuentes-García, M., Camacho, J., & Maciá-Fernández, G. (2021). Present and Future of Network Security Monitoring. *IEEE Access*, 9, 112744-112760. URL: https://doi.org/10.1109/ACCESS.2021.3067106.
4. Zhao, J., Masood, R., & Seneviratne, S. (2020). A Review of Computer Vision Methods in Network Security. *IEEE Communications Surveys & Tutorials*, 23, 1838-1878. URL: https://doi.org/10.1109/COMST.2021.3086475.
5. (2019). NETWORK SECURITY. URL: https://doi.org/10.4324/9781315063218-16.
6. Kriegeskorte, N., & Golan, T. (2019). Neural network models and deep learning. *Current Biology*, 29, R231-R236. URL: https://doi.org/10.1016/j.cub.2019.02.034.
7. Schonlau, M., & Zou, R. (2020). The random forest algorithm for statistical learning. *The Stata Journal*, 20, 29 - 3. URL: https://doi.org/10.1177/1536867X20909688.
8. Keith, M. (2020). Random Forest. *Machine Learning with Regression in Python*. URL: https://doi.org/10.1007/978-1-4419-9863-7_612.
9. Zave, P., & Rexford, J. (2019). Patterns and Interactions in Network Security. *ACM Computing Surveys (CSUR)*, 53, 1 - 37. URL: https://doi.org/10.1145/3417988.
10. Ganzhur, M., & Bryukhovetsky, A. (2022). Network security systems. *Herald of Dagestan State Technical University. Technical Sciences*. URL: https://doi.org/10.21822/2073-6185-2022-49-3-61-67.
11. Kizza, J. (2020). Guide to Computer Network Security. *Guide to Computer Network Security*. URL: https://doi.org/10.1007/978-3-030-38141-7.
12. Cernov, A. (2018). Security in Computer Networks. *International Journal of Information Security and Cybercrime*. URL: https://doi.org/10.19107/ijisc.2018.01.05.
13. Nassif, A., Talib, M., Nasir, Q., Albadani, H., & Dakalbab, F. (2021). Machine Learning for Cloud Security: A Systematic Review. *IEEE Access*, 9, 20717-20735. URL: https://doi.org/10.1109/ACCESS.2021.3054129.
14. Bhansali, A. (2023). Cloud Security and Privacy. *International Journal for Research in Applied Science and Engineering Technology*. URL: https://doi.org/10.22214/ijraset.2023.55416.

15. Kabir, A., Mitra, S., Akter, S., Islam, M., & Das, S. (2022). Developing a Network Design for a Smart Airport Using Cisco Packet Tracer. *Informatica Economica*. URL: https://doi.org/10.24818/issn14531305/26.1.2022.03.
16. Utsav, A., Abhishek, A., Kumari, A., & Daksh, H. (2022). Smart Irrigation System Using Cisco Packet Tracer. *2022 International Conference on Wireless Communications Signal Processing and Networking (WiSPNET)*, 297-301. URL: https://doi.org/10.1109/wispnet54241.2022.9767184.
17. Ashok, G., Akram, P., Neelima, M., Nagasaikumar, J., & , A. (2020). Implementation Of Smart Home By Using Packet Tracer. *International Journal of Scientific & Technology Research*, 9, 678-685.
18. Praseed, A., & Thilagam, P. (2019). DDoS Attacks at the Application Layer: Challenges and Research Perspectives for Safeguarding Web Applications. *IEEE Communications Surveys & Tutorials*, 21, 661-685. URL: https://doi.org/10.1109/COMST.2018.2870658.
19. Amrish, R., Bavapriyan, K., Gopinaath, V., Jawahar, A., & Kumar, V. (2022). DDoS Detection using Machine Learning Techniques. *March 2022*. URL: https://doi.org/10.36548/jismac.2022.1.003.
20. Roy, A., Dhanalakshmi, N., & Suresh, D. (2021). RESEARCH INVESTIGATIONS ON DDOS ATTACK. , 9, 1164-1173. URL: https://doi.org/10.17762/ITII.V9I1.250.
21. Manikandan, R., Dharshini, S., & Pavithra, N. (2023). DDoS Attack Prediction System. *International Journal for Research in Applied Science and Engineering Technology*. URL: https://doi.org/10.22214/ijraset.2023.52426.

ДОДАТОК А

Налаштування R5:

```
Router>enable
Router#configure terminal
Router(config)#ip route 10.10.110.0 255.255.255.0 10.10.10.2
Router(config)#exit
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#ip access-list standard PAT
Router(config-std-nacl)#permit 192.168.100.0 0.0.0.255
Router(config-std-nacl)#exit
Router(config)#ip nat inside source list PAT interface fastEthernet 0/1 overload
Router(config)#ip access-list extended outside
Router(config-ext-nacl)#permit icmp any host 192.168.101.2
Router(config-ext-nacl)#permit tcp any host 192.168.101.2
Router(config-ext-nacl)#deny ip any any
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip access-group outside in
Router(config-if)#exit
Router(config)#ip inspect name in-out http
Router(config)#ip inspect name in-out icmp
Router(config)#ip inspect name in-out tcp
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip inspect in-out in
Router# configure terminal
Router(config)#ip access-list extended DMZ
Router(config-ext-nacl)#deny ip host 192.168.101.2 192.168.100.0 0.0.0.255
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#exit
Router(config)#interface fastEthernet 1/0
Router(config-if)#ip access-group DMZ in
```

Налаштування R6:

```
Router>enable
Router#configure terminal
Router(config)#ip route 192.168.100.0 255.255.255.0 10.10.10.1
Router(config)#ip route 192.168.101.0 255.255.255.248 10.10.10.1

Router(config-if)#ip address 10.10.10.1 255.255.255.252
Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#ip address 192.168.101.1 255.255.255.248
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config)#ip route 10.10.110.0 255.255.255.0 10.10.10.2
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#ip access-list standard PAT
Router(config-std-nacl)#permit 192.168.100.0 0.0.0.255
Router(config-std-nacl)#exit
Router(config)#ip nat inside source list PAT interface fastEthernet 0/1 overload
Router(config)#ip access-list extended outside
Router(config-ext-nacl)#permit icmp any host 192.168.101.2
Router(config-ext-nacl)#permit tcp any host 192.168.101.2
Router(config-ext-nacl)#deny ip any a
Router(config-ext-nacl)#deny ip any any
Router(config-ext-nacl)#exit
Router(config)#interface fastEthernet 0/1
Router(config-if)#ip access-group outside in
Router(config-if)#exit
Router(config)#ip inspect name in-out http
Router(config)#ip inspect name in-out icmp
Router(config)#ip inspect name in-out tcp
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip inspect in-out in
Router(config-if)#exit
Router(config)#ip access-list extended DMZ
Router(config-ext-nacl)#deny ip host 192.168.101.2 192.168.101.0 0.0.0.255
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#exit
Router(config)#interface fastEthernet 1/0
```

```
Router(config-if)#ip access-group DMZ in
Router(config-if)#exit
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip access-list extended DMZ
Router(config-ext-nacl)#Router(config)#ip access-list extended DMZ
Router(config-ext-nacl)#deny ip host 192.168.101.2 192.168.100.0 0.0.0.255

Router#no deny ip host 192.168.101.2 192.168.101.0 0.0.0.255
Router(config)#ip access-list extended DMZ
Router(config-ext-nacl)#no deny ip host 192.168.101.2 192.168.101.0 0.0.0.255
Router(config-ext-nacl)#exit
Router(config)#interface fastEthernet 1/0
Router(config-if)#ip access-group DMZ in
Router(config-if)#exit
Router#show access-lists
Standard IP access list PAT
10 permit 192.168.100.0 0.0.0.255 (16 match(es))
Extended IP access list outside
10 permit icmp any host 192.168.101.2 (3 match(es))
20 permit tcp any host 192.168.101.2
30 deny ip any any (4 match(es))
Extended IP access list DMZ
20 permit ip any any (16 match(es))
30 deny ip host 192.168.101.2 192.168.100.0 0.0.0.255
Router#configure terminal
Router(config)#interface FastEthernet0/1
Router(config-if)# Router(config-if)#exit
Router(config)#interface FastEthernet1/0
Router(config-if)#shutdown
Router(config)#show access-lists DMZ
Router(config)#exit
Router#show access-lists DMZ
Extended IP access list DMZ
permit ip any any (20 match(es))
deny ip host 192.168.101.2 192.168.100.0 0.0.0.255
Router#configure terminal
Router(config)#interface fastEthernet 1/0
Router(config-if)#ip access-group DMZ in
```

Налаштування R0:

```
Router>enable
Router#configure terminal
Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 212.1.64.133 255.255.255.252
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 212.1.1.1 255.255.255.0
Router(config)#ip route 212.1.1.0 255.255.255.0 212.1.64.132
Router(config)#no ip route 192.168.1.0 255.255.255.0 212.1.64.132
```

Налаштування ASA:

```
ciscoasa#configure terminal
ciscoasa(config)#interface ethernet 0/2
ciscoasa(config-if)#switchport access vlan 3
ciscoasa(config-if)#exit
ciscoasa(config)#int vlan 3
ciscoasa(config-if)#nameif dmz
ciscoasa(config-if)#no forward interface vlan 1
ciscoasa(config-if)#nameif dmz
ciscoasa(config-if)#security-level 50
ciscoasa(config-if)#ip address 212.1.65.1 255.255.255.252
ciscoasa#configure terminal
ciscoasa(config)#access-list FROM-OUTSIDE extended permit tcp any host 212.1.65.2
ciscoasa(config)#access-list FROM-OUTSIDE extended permit tcp any host 212.1.65.2 eq www
ciscoasa(config)#access-group FROM-OUTSIDE in interface outside
ciscoasa>enable
ciscoasa#configure terminal
ciscoasa(config)#enable password c6s2u7MA
ciscoasa(config)#username admin password c6s2u7MA
ciscoasa(config)#ssh 192.168.1.0 255.255.255.0 inside
ciscoasa(config)#aaa authentication ssh console local
ciscoasa(config)#in vlan 1
ciscoasa(config-if)#security-level 99
ciscoasa(config)#int vlan2
ciscoasa(config-if)#ip address 212.1.64.132 255.255.255.252
ciscoasa(config)#route inside 212.1.1.0 255.255.255.0 212.1.64.133
ciscoasa(config)#class-map inspection_default
ciscoasa(config-cmap)#match default-inspection-traffic
ciscoasa(config-cmap)#exit
ciscoasa(config)#policy-map global_policy
ciscoasa(config)#policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#inspect icmp
```

```
ciscoasa(config-pmap-c)#inspect http
ciscoasa(config-pmap-c)#exit
ciscoasa(config)#service-policy global_policy global
ciscoasa(config)#policy-map global_policy
ciscoasa(config)#object network nat
ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0,
ciscoasa(config-network-object)#nat (inside,outside) dynamic interface
```

ДОДАТОК Б

```
import pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.tree import DecisionTreeClassifier
from sklearn.metrics import accuracy_score, classification_report, confusion_matrix
import matplotlib.pyplot as plt


file_path = 'diplom_updated.csv'
data = pd.read_csv(file_path)

def categorize_scores(score):
    if score >= 20:
        return 'Високий рівень'
    elif 10 <= score < 20:
        return 'Середній рівень'
    else:
        return 'Низький рівень'

data['Category'] = data['Scores'].apply(categorize_scores)

category_counts = data['Category'].value_counts()
print("Кількість людей у кожній категорії:")
print(category_counts)

average_scores = data.groupby('Category')['Scores'].mean()
print("\nСередній бал у кожній категорії:")
print(average_scores)

X = data[['Scores']]
y = data['Category']

X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2,
random_state=42)

clf = DecisionTreeClassifier()

clf.fit(X_train, y_train)

y_pred = clf.predict(X_test)
plt.figure(figsize=(6,6))
plt.pie(category_counts, labels=category_counts.index, autopct='%1.1f%%',
startangle=90, colors=['#ff9999','#66b3ff','#99ff99'])
plt.title('Співвідношення рівнів кібербезпеки')
plt.show()



import pandas as pd

df = pd.read_csv('diplom.csv')

from sklearn.preprocessing import LabelEncoder

label_encoders = {}
```

```
for column in df.select_dtypes(include=['object']).columns:
    le = LabelEncoder()
    df[column] = le.fit_transform(df[column])
    label_encoders[column] = le

correlation_matrix = df.corr()

correlation_text = correlation_matrix.to_string()
print("Кореляційна матриця:")
print(correlation_text)
```

```
import pandas as pd
import seaborn as sns
import matplotlib.pyplot as plt

df = pd.read_csv('diplom.csv')
from sklearn.preprocessing import LabelEncoder

label_encoders = {}
for column in df.select_dtypes(include=['object']).columns:
    le = LabelEncoder()
    df[column] = le.fit_transform(df[column])
    label_encoders[column] = le
correlation_matrix = df.corr()
plt.figure(figsize=(12, 10))
sns.heatmap(correlation_matrix, annot=True, fmt=".2f", cmap='coolwarm')
plt.title('Кореляційна матриця')
plt.show()
```

```
import numpy as np
from sklearn.ensemble import IsolationForest
import matplotlib.pyplot as plt

np.random.seed(42)
normal_data = np.random.normal(0, 1, (100, 2))
anomalous_data = np.random.uniform(low=-6, high=6, size=(10, 2))
data = np.vstack([normal_data, anomalous_data])

model = IsolationForest(contamination=0.1)
model.fit(data)

predictions = model.predict(data)

plt.scatter(data[:, 0], data[:, 1], c=predictions, cmap='coolwarm', edgecolor='k',
s=60)
plt.title("Загрози виявленні за допомогою Isolation Forest")
plt.xlabel("Feature 1")
plt.ylabel("Feature 2")
plt.colorbar(label='Prediction (-1: Аномалія, 1: Норма)')
plt.show()
```

```
import numpy as np
from sklearn.ensemble import IsolationForest
import matplotlib.pyplot as plt

np.random.seed(42)

normal_traffic = np.random.normal(0, 1, (200, 2))

ddos_attack = np.random.normal(loc=5, scale=0.5, size=(20, 2))

data = np.vstack([normal_traffic, ddos_attack])

model = IsolationForest(contamination=0.1, random_state=42)
model.fit(data)

predictions = model.predict(data)
anomaly_scores = model.decision_function(data)

plt.figure(figsize=(10, 6))

normal_points = data[predictions == 1]
anomalous_points = data[predictions == -1]

plt.scatter(normal_points[:, 0], normal_points[:, 1], c='blue', marker='o',
label='Нормальний трафік')
plt.scatter(anomalous_points[:, 0], anomalous_points[:, 1], c='red', marker='x',
label='Атака (DDoS)')
plt.title("Емуляція DDoS-атаки та її виявлення за допомогою Isolation Forest")
plt.xlabel("Feature 1")
plt.ylabel("Feature 2")
plt.legend()
plt.colorbar(label='Prediction Score')
plt.show()

print("Кількість дерев у лісі:", model.n_estimators)
print("Відсоток аномальних зразків:", model.contamination)
print("Розмір підвибірки для кожного дерева:", model.max_samples)

threshold = -0.2
high_risk_anomalies = data[anomaly_scores < threshold]
print("Кількість суттєвих аномалій:", high_risk_anomalies.shape[0])
print("Суттєві аномалії:", high_risk_anomalies)
```