МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
Циклова комісія *комп'ютерних систем та мереж*
(повна назва циклової комісії)

Допустити до захисту
Голова випускової циклової комісії
комп'ютерних систем та мереж
(повна назва циклової комісії)
_____ *Ірина КРАВЧУК*
(підпис) (ім'я, ПРІЗВИЩЕ)
« 10 » 06 2025 р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬО-ПРОФЕСІЙНОГО СТУПЕНЯ ФАХОВИЙ МОЛОДШИЙ БАКАЛАВР

Тема: *Розробка та реалізація моделі Zero Trust для корпоративної мережі*

Група: *3-013* Спеціальність: *123 «Комп'ютерна інженерія»*

Здобувач освіти _____ *Вадим МАКАРЕНКО*
(підпис) (ім'я, ПРІЗВИЩЕ)

Керівник роботи _____ *Олександр ГРИНЧЕНКО*
(підпис) (ім'я, ПРІЗВИЩЕ)

Консультант з оформлення пояснювальної записки _____ *Оксана ОСАДЧА*
(підпис) (ім'я, ПРІЗВИЩЕ)

Кривий Ріг 2025 р.

КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

Відділення *комп'ютерної та програмної інженерії*
Циклова комісія *комп'ютерних систем та мереж*
Освітньо-професійний ступінь *фаховий молодший бакалавр*
Спеціальність *123 «Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Голова випускової циклової комісії
комп'ютерних систем та мереж
(повна назва циклової комісії)
(підпис) *Ірина КРАВЧУК*
(ім'я, ПРІЗВИЩЕ)
« 10 « 03 2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ОСВІТИ

МАКАРЕНКО Вадима Віталійовича
(прізвище, ім'я, по батькові)

1.Тема роботи *Розробка та реалізація моделі Zero Trust для корпоративної мережі*

Керівник роботи *Гринченко Олександр Сергійович, викладач вищої категорії*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по коледжу від « *04* « *04* 2025 року № *50-ст*

2. Строк подання здобувачем освіти роботи з *01.03.2025* по *15.06.2025*

3. Вихідні дані до роботи *практичні рекомендації від NIST (SP 800-207) щодо реалізації Zero Trust Architecture (ZTA); технічна документація на маршрутизатор TP-Link WR940N з прошивкою OpenWRT; Tailscale, Linux; Android*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) *Теоретичні основи кіберпростору та інформаційної безпеки; Аналіз сучасних кіберзагроз і їх класифікація; Приклади впровадження Zero Trust у практиці; Побудова тестового середовища з маршрутизатором OpenWRT і VPN Tailscale; Реалізація VLAN, ACL, автентифікації та контролю доступу.*

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

Презентація Microsoft PowerPoint

6. Консультанти розділів роботи (проекту)

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

7. Дата видачі завдання

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	*Узгодження технічного завдання з керівником дипломної роботи*	*01.03.2025*	*виконано*
2	*Підбір та вивчення науково-технічної літератури за темою дипломної роботи*	*15.03.2025*	*виконано*
3	*Розділ 1. Теоретичні основи кібербезпеки та моделі захисту інформації*	*28.04.2025*	*виконано*
4	*Розділ 2. Концепція Zero Trust: принципи, реалізація та застосування*	*14.05.2025*	*виконано*
5	*Розділ 3. Реалізація концепції Zero Trust у тестовому середовищі*	*26.05.2025*	*виконано*
6	*Підготовка матеріалів до презентації*	*30.05.2025*	*виконано*
7	*Написання та оформлення пояснювальної записки*	*06.06.2025*	*виконано*
8	*Захист дипломної роботи*		

Здобувач освіти _____ *Вадим МАКАРЕНКО*
(підпис) (ім'я, ПРІЗВИЩЕ)

Керівник роботи _____ *Олександр ГРИНЧЕНКО*
(підпис) (ім'я, ПРІЗВИЩЕ)

StrikePlagiarism.com

Дата звіту 6/4/2025
Дата редагування ---

Документ прийнятий

Звіт подібності

метадані

Назва організації
Ukrainian national aviation university
Заголовок
Макаренко В_3-013_2025_КПІ
Автор Науковий керівник / Експерт
Макаренко ВГринченко О
підрозділ
Криворізький Фаховий коледж

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.

2.23%
2.23%
КП 1

2.28%
2.28%
КЦ

25
Довжина фрази для коефіцієнта подібності 2

14205
Кількість слів

111364
Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв		0
Інтервали		0
Мікропробіли		0
Білі знаки		0
Парафрази (SmartMarks)	a	23

Подібності за списком джерел

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз — Колір тексту

ПОРЯДКОВИЙ НОМЕР	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	https://ppt-online.org/445363	23 0.16 %
2	Дружина_3-012_2025_КПІ_123 [redacted] 5/29/2025 Ukrainian national aviation university (Криворізький Фаховий коледж)	22 0.15 %
3	Дружина_3-012_2025_КПІ_123 [redacted] 5/29/2025 Ukrainian national aviation university (Криворізький Фаховий коледж)	18 0.13 %

РЕФЕРАТ

Кваліфікаційна робота «Розробка та реалізація моделі *Zero Trust* для корпоративної мережі» містить 83 сторінок, 23 рисунків, 5 таблиць, 25 використаних літературних джерел.

ZERO TRUST, КІБЕРБЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА, КОРПОРАТИВНА МЕРЕЖА, АВТЕНТИФІКАЦІЯ, КОНТРОЛЬ ДОСТУПУ, ШИФРУВАННЯ, МІКРОСЕГМЕНТАЦІЯ, OPENWRT, TAILSCALE, ACL, VLAN, VPN, ЗАГРОЗИ БЕЗПЕКИ, ЦИФРОВА ТРАНСФОРМАЦІЯ, МОДЕЛІ БЕЗПЕКИ, APT, МЕРЕЖЕВИЙ ЗАХИСТ, ШТУЧНИЙ ІНТЕЛЕКТ.

Кваліфікаційна робота на тему «Розробка та реалізація моделі *Zero Trust* для корпоративної мережі» присвячена дослідженню сучасних підходів до кіберзахисту корпоративних мереж в умовах зростання складності кіберзагроз. У роботі проаналізовано еволюцію концепцій інформаційної безпеки, виділено обмеження традиційних моделей типу «Замок і Рів», обґрунтовано потребу у впровадженні архітектури *Zero Trust*, що ґрунтується на принципі «ніколи не довіряй, завжди перевіряй».

Дослідження містить теоретичне підґрунтя концепції *Zero Trust*, приклади її використання у світовій практиці, а також практичну реалізацію моделі у тестовому середовищі з використанням маршрутизатора *TP-Link* з прошивкою *OpenWRT* та *VPN*-сервісу *Tailscale*. Запропоновано авторський підхід до налаштування сегментації мережі (*VLAN*), політик доступу (*ACL*), а також аналіз результатів впровадження з точки зору ефективності, безпечності та надійності.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 6

РОЗДІЛ 1 ТЕОРЕТИЧНІ ОСНОВИ КІБЕРБЕЗПЕКИ ТА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЇ 8

1.1 Поняття кіберпростору та інформаційної безпеки 8

1.2 Етапи розвитку інформаційної безпеки в корпоративних мережах 13

1.3 Основні загрози безпеці в сучасному інформаційному середовищі 18

1.4 Традиційні моделі безпеки: переваги та обмеження 23

1.5 Висновок до розділу 1 28

РОЗДІЛ 2 КОНЦЕПЦІЯ *ZERO TRUST*: ПРИНЦИПИ, РЕАЛІЗАЦІЯ ТА ЗАСТОСУВАННЯ 30

2.1 Виникнення та розвиток концепції *Zero Trust* 30

2.2 Основні принципи моделі *Zero Trust* 34

2.3 Сфери застосування концепції *Zero Trust* в корпоративних середовищах 39

2.4 Приклади впровадження *Zero Trust* у сучасних компаніях 43

2.5 Порівняння *Zero Trust* із традиційними моделями безпеки 46

2.6 Висновок до розділу 2 49

РОЗДІЛ 3 РЕАЛІЗАЦІЯ КОНЦЕПЦІЇ *ZERO TRUST* У ТЕСТОВОМУ СЕРЕДОВИЩІ 51

3.1 Вибір і опис тестового обладнання та ПЗ 51

3.2 Підготовка маршрутизатора *TP-Link WR*940*N* з прошивкою *OpenWRT* 55

3.3 Ознайомлення з сервісом *Tailscale* як *Zero Trust VPN* 59

3.4 Налаштування *Windows, Linux, Android*-клієнтів 63

3.5 Реалізація *VLAN, ACL,* та авторизаційних політик 68

3.6 Проведення експериментів і логування подій 73

3.7 Аналіз результатів та оцінка ефективності підходу 76

3.8 Висновок до розділу 3 78

ВИСНОВКИ 80

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 82

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ACL	*Access Control List* – список керування доступом
AI	*Artificial Intelligence* – штучний інтелект
APT	*Advanced Persistent Threat* – розвинена цілеспрямована загроза
BYOD	*Bring Your Own Device* – політика використання власних пристроїв
CIA	*Confidentiality, Integrity, Availability* – конфіденційність, цілісність, доступність
DDoS	*Distributed Denial of Service* – розподілена атака на відмову в обслуговуванні
EDR	*Endpoint Detection and Response* – виявлення та реагування на загрози на кінцевих точках
IDS/IPS	*Intrusion Detection/Prevention System* – система виявлення/запобігання вторгненням
IoT	*Internet of Things* – Інтернет речей
MFA	*Multi-Factor Authentication* – багатофакторна автентифікація
NAC	*Network Access Control* – контроль доступу до мережі
OT	*Operational Technology* – операційні технології
RBAC	*Role-Based Access Control* – модель контролю доступу на основі ролей
SIEM	*Security Information and Event Management* – система управління подіями безпеки
SOAR	*Security Orchestration, Automation and Response* – оркестрація та автоматизація безпеки
UEBA	*User and Entity Behavior Analytics* – аналітика поведінки користувачів та сутностей
VPN	*Virtual Private Network* – віртуальна приватна мережа
ZTA	*Zero Trust Architecture* – архітектура «нульової довіри»

ВСТУП

У сучасному світі інформаційні технології стали невід'ємною частиною всіх сфер людської діяльності, від особистих комунікацій до управління критичною інфраструктурою держав. Ця цифрова трансформація породила кіберпростір – складне, динамічне та взаємопов'язане середовище, яке відкриває безмежні можливості, але водночас несе значні ризики. Зростання складності кіберзагроз, таких як програми-вимагачі, цілеспрямовані атаки (*APT*), інсайдерські загрози та атаки на ланцюжки постачання, а також розмиття традиційного мережевого периметра через хмарні технології, мобільність і політики *BYOD,* роблять традиційні моделі безпеки, такі як «Замок і Рів» чи «Захист у глибину», недостатньо ефективними. У цих умовах концепція *Zero Trust,* що базується на принципі «ніколи не довіряй, завжди перевіряй», стає новою парадигмою кібербезпеки, яка дозволяє організаціям адаптуватися до сучасного ландшафту загроз.

Метою даної роботи є всебічний аналіз концепції *Zero Trust,* її теоретичних основ, принципів, а також практичної реалізації в тестовому середовищі з використанням сучасних інструментів, таких як *OpenWRT* і *Tailscale*. Робота структурована у трьох основних розділах: перший розділ присвячено теоретичним основам кібербезпеки, еволюції підходів до захисту інформації та аналізу сучасних загроз; другий – детальному розгляду концепції *Zero Trust,* її принципів і порівнянню з традиційними моделями безпеки; третій розділ описує практичну реалізацію *Zero Trust* у контрольованому тестовому середовищі, включаючи налаштування апаратного та програмного забезпечення, експерименти та аналіз результатів.

Такий підхід дозволяє не лише теоретично обґрунтувати доцільність використання *Zero Trust,* але й продемонструвати її практичну застосовність для підвищення рівня безпеки корпоративних мереж.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ КІБЕРБЕЗПЕКИ ТА МОДЕЛІ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Поняття кіберпростору та інформаційної безпеки

Сучасний світ неможливо уявити без інформаційних технологій, які проникли в усі сфери людської діяльності – від повсякденного спілкування до управління критичною інфраструктурою держав. Ця цифрова трансформація породила нове середовище – кіберпростір, який, поряд із безмежними можливостями, несе й значні ризики. Забезпечення безпеки в цьому просторі, тобто кібербезпека, стало одним із ключових пріоритетів для організацій будь-якого масштабу та форми власності, а також для національної безпеки держав.

Термін «кіберпростір» (*cyberspace*) вперше був популяризований письменником-фантастом Вільямом Гібсоном у його романі «Нейромант» [1], де він описувався як «консенсусна галюцинація». Однак сьогодні це поняття вийшло далеко за межі наукової фантастики і стало об'єктом дослідження для технічних спеціалістів, юристів, соціологів та військових.

Існує багато визначень кіберпростору, але узагальнено його можна схарактеризувати як глобальне середовище, сформоване взаємопов'язаними інформаційними та комунікаційними технологіями, що включає комп'ютерні мережі, апаратне та програмне забезпечення, дані, користувачів та процеси їх взаємодії.

З технічної точки зору, кіберпростір охоплює:

- фізичний рівень - це сервери, комп'ютери, мобільні пристрої, мережеве обладнання (маршрутизатори, комутатори, кабелі), системи зберігання даних.
- логічний рівень - це програмне забезпечення (операційні системи, прикладні програми, системи управління базами даних), протоколи передачі даних (*TCP/IP, HTTP, DNS* та ін.), віртуальні машини, хмарні сервіси.

˜ інформаційний рівень - це дані, що створюються, обробляються, зберігаються та передаються в цьому середовищі, включаючи текстову інформацію, мультимедіа, бази даних, метадані.

˜ соціальний (людський) рівень - це користувачі, їхні цифрові ідентичності, взаємодії, спільноти, а також зловмисники та їхні мотиви.

На рисунку 1.1 наглядно з технічної точки зору продемонстрована структура кіберпростору.

Рисунок 1.1 - Багаторівнева структура кіберпростору

Ключовими характеристиками кіберпростору є:

1. Глобальність та транскордонність. Кіберпростір не має чітких географічних кордонів, що ускладнює правове регулювання та реагування на інциденти.

2. Динамічність. Технології та конфігурації мереж постійно змінюються, з'являються нові сервіси та вразливості.

3. Взаємопов'язаність. Компоненти кіберпростору тісно пов'язані, що означає, що інцидент в одній частині системи може швидко поширитися на інші.

4. Анонімність (псевдоанонімність). Можливість діяти анонімно або під вигаданою особою створює сприятливі умови для зловмисної діяльності.

5. Уразливість. Складність систем та наявність програмних і апаратних недоліків роблять кіберпростір вразливим до атак.

Для корпоративного середовища кіберпростір – це не просто зовнішнє середовище, а й внутрішній цифровий ландшафт компанії, що включає її локальні мережі, хмарні ресурси, пристрої співробітників (включаючи *BYOD – Bring Your Own Device*)[2], системи Інтернету речей (*IoT*)[3] та операційні технології (*OT*).

Інформаційна безпека (ІБ) – це стан захищеності інформації та інфраструктури, що її підтримує, від випадкових або навмисних впливів природного чи штучного характеру, здатних завдати шкоди власникам або користувачам інформації та інфраструктури. Основною метою інформаційної безпеки є забезпечення трьох фундаментальних властивостей інформації, відомих як тріада CIA (конфіденційність, цілісність, доступність).

1. Конфіденційність (*Confidentiality*) - це гарантія того, що інформація доступна лише авторизованим користувачам, процесам або системам. Захист від несанкціонованого розкриття даних. Методи забезпечення: шифрування, контроль доступу, автентифікація.

2. Цілісність (*Integrity*) - це гарантія того, що інформація та програмне забезпечення не були змінені неавторизованим чином та є точними й повними. Захист від несанкціонованої модифікації або знищення даних. Методи забезпечення: хешування, цифрові підписи, контроль версій, системи виявлення вторгнень.

3. Доступність (*Availability*) - це гарантія того, що авторизовані користувачі мають своєчасний та безперешкодний доступ до інформації та пов'язаних з нею активів, коли це необхідно. Захист від відмови в обслуговуванні. Методи забезпечення: резервне копіювання, відмовостійкі системи, захист від *DDoS*-атак.

На рисунку 1.2 наглядно показана відома модель безпеки – тріада *CIA* (*Confidentiality, Integrity, Availability*).

Рисунок 1.2 - Тріада інформаційної безпеки (CIA)

Окрім тріади CIA, сучасні концепції інформаційної безпеки часто включають додаткові важливі властивості:

- невідмовність (*Non-repudiation*) узагальнює неможливість для суб'єкта (користувача або системи) відмовитися від факту виконання певних дій або авторства інформації. Забезпечується за допомогою цифрових підписів, журналювання дій.
- автентичність (*Authenticity*) узагальнює впевненість у тому, що суб'єкт або ресурс є саме тим, за кого себе видає. Перевірка справжності джерела даних або особи користувача. Забезпечується паролями, біометрією, сертифікатами.
- підзвітність (*Accountability*) узагальнює можливість однозначно ідентифікувати дії кожного суб'єкта в системі та пов'язати їх з цим суб'єктом. Забезпечується через системи аудиту та моніторингу.
- спостережуваність (*Observability*) узагальнює здатність системи надавати дані про свій внутрішній стан, що дозволяє виявляти аномалії та інциденти безпеки.

Співвідношення понять «інформаційна безпека» та «кібербезпека» часто використовуються як синоніми, проте між ними існує певна різниця, хоча межі досить розмиті.

1. Інформаційна безпека є ширшим поняттям. Вона охоплює захист інформації в будь-якій формі (електронній, паперовій, усній) та в будь-якому середовищі. Вона стосується не лише технічних, а й організаційних, правових та фізичних аспектів захисту.

2. Кібербезпека фокусується на захисті інформаційних активів саме в кіберпросторі. Це набір технологій, процесів та практик, призначених для захисту мереж, комп'ютерів, програм та даних від атак, пошкоджень або несанкціонованого доступу в цифровому середовищі. Тобто, кібербезпеку можна розглядати як важливу складову інформаційної безпеки, що спеціалізується на загрозах, які виникають у кіберпросторі.

Для цілей даної роботи, де розглядається захист корпоративної мережі та впровадження моделі *Zero Trust*[4], яка є переважно технологічною та орієнтованою на цифрове середовище, термін «кібербезпека» буде центральним, проте він нерозривно пов'язаний із загальними принципами інформаційної безпеки.

Забезпечення інформаційної безпеки в корпоративному середовищі вимагає комплексного підходу, що включає:

- політику безпеки де є документально оформлені правила та процедури;
- організаційні заходи де є розподіл відповідальності, навчання персоналу, управління ризиками;
- технічні засоби захисту де є програмні та апаратні рішення (антивіруси, міжмережеві екрани, системи виявлення вторгнень, шифрування тощо);
- фізичну безпеку де є контроль доступу до приміщень, захист обладнання;
- правові аспекти де є дотримання законодавства про захист даних (*GDPR*, українське законодавство про захист персональних даних);

Розуміння цих фундаментальних понять є відправною точкою для аналізу еволюції підходів до захисту та обґрунтування необхідності переходу до більш сучасних моделей, таких як *Zero Trust,* в умовах постійно зростаючих кіберзагроз.

1.2 Етапи розвитку інформаційної безпеки в корпоративних мережах

Історія розвитку інформаційної безпеки в корпоративних мережах тісно пов'язана з еволюцією самих інформаційних технологій, архітектур мереж та, звісно, методів, які використовують зловмисники. Можна виділити кілька ключових етапів, кожен з яких характеризувався своїми домінуючими технологіями, основними загрозами та філософією захисту.

Етап 1: Ера мейнфреймів та ізольованих систем (1960-ті – початок 1980-х). Технологічний ландшафт - це домінування великих, централізованих комп'ютерів – мейнфреймів. Мережі були рідкістю, а якщо й існували, то переважно у вигляді термінальних підключень до центрального комп'ютера.

1. Основні загрози:

- фізичний несанкціонований доступ до обладнання;
- помилки операторів;
- збої обладнання;
- внутрішні зловживання з боку невеликої кількості довірених осіб, що мали доступ;

2. Філософія та методи захисту:

- фізична безпека де основний акцент робився на захисті приміщень, де знаходились мейнфрейми;
- контроль доступу на рівні системи - це прості механізми парольного захисту для доступу до системи та файлів;
- резервне копіювання де використовується створення копій даних на магнітних стрічках;
- обмежене коло користувачів де доступ мали лише спеціально навчені оператори та програмісти;

3. Обмеження. Модель безпеки була простою, оскільки системи були переважно ізольованими. Поняття «корпоративна мережа» у сучасному розумінні ще не існувало.

Етап 2: Поява локальних обчислювальних мереж (*LAN*) та перших глобальних підключень (середина 1980-х – середина 1990-х). Технологічний ландшафт - це поширення персональних комп'ютерів (ПК) та їх об'єднання в локальні мережі (*LAN*). Поява перших підключень до глобальних мереж, таких як *ARPANET*[5], а згодом – Інтернету. Використання файлових серверів, принтер-серверів.

1. Основні загрози:
   - появa перших комп'ютерних вірусів (через дискети);
   - несанкціонований доступ до ресурсів всередині *LAN*;
   - потенційні загрози від перших зовнішніх підключень;
   - витік даних через неконтрольоване копіювання на дискети;
2. Філософія та методи захисту:
   - антивірусне програмне забезпечення;
   - розмежування доступу на рівні ОС та мережевих ОС (*NOS*);
   - Парольний захист;
   - Концепція «периметра»;
3. Обмеження. Засоби захисту були переважно реактивними. Складність управління безпекою зростала зі збільшенням кількості ПК та серверів.

Етап 3: Розквіт Інтернету та побудова «фортеці» (середина 1990-х – середина 2000-х) Технологічний ландшафт - це масове підключення корпоративних мереж до Інтернету. Розвиток веб-технологій (*WWW*)[6], електронної пошти. З'являються інтранет- та екстранет-рішення.

1. Основні загрози:
   - інтернет-черв'яки (*Morris Worm, Code Red, SQL Slammer*[7]);
   - мережеві атаки (сканування портів, *DoS*-атаки);
   - хакерські вторгнення з метою крадіжки або модифікації даних;
   - спам та фішинг (ранні форми);
2. Філософія та методи захисту - це модель «Замок і Рів» (*Castle and Moat*)[8]
   - міжмережеві екрани (*Firewalls*);
   - системи виявлення вторгнень (*IDS*);

- *VPN* (*Virtual Private Networks*);
- проксі-сервери;
- централізоване управління антивірусами;

3. Обмеження. Ця модель добре працювала проти зовнішніх загроз, але була вразливою до внутрішніх атак (інсайдерів) та загроз, що оминали периметр (через заражені *USB*-носії або соціальну інженерію). «Тверда оболонка, м'яка середина».

На рисунку 1.3 є схематичне зображення корпоративної мережі як фортеці, оточеної ровом (Інтернет), з мостом (міжмережевий екран) як єдиною точкою входу/виходу.

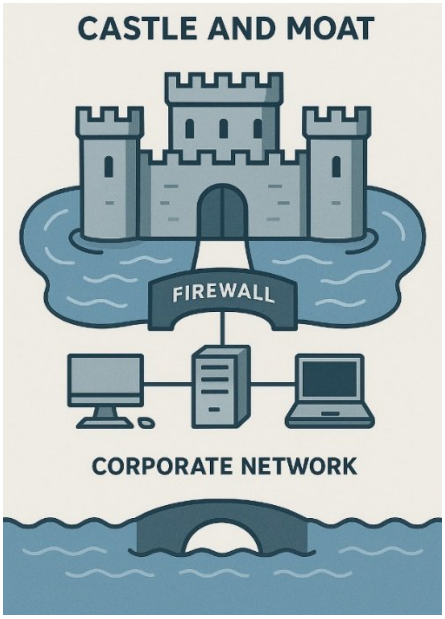

Рисунок 1.3 - Класична модель безпеки «Замок і Рів»

Етап 4: Деперіметризація та виклики мобільності й хмар (середина 2000-х – середина 2010-х). Технологічний ландшафт - це широке розповсюдження мобільних пристроїв (смартфони, планшети), політики *BYOD*. Активне впровадження хмарних сервісів (*SaaS, PaaS, IaaS*). Розвиток бездротових мереж (*Wi-Fi*). Соціальні мережі та веб 2.0.

1. Основні загрози:

- розмиття традиційного периметра де дані та користувачі знаходяться поза контролем корпоративної мережі.
- загрози для мобільних пристроїв (втрата, крадіжка, шкідливі програми);

- атаки на веб-додатки (*SQL*-ін'єкції, *XSS*);
- цілеспрямовані атаки (*Advanced Persistent Threats – APT*);
- збільшення ролі соціальної інженерії;
- витік даних через хмарні сховища;

2. Філософія та методи захисту - Розширення та ускладнення захисту:

- *Next-Generation Firewalls* (*NGFW*) – це більш інтелектуальні міжмережеві екрани з функціями контролю додатків, *IPS*;
- *SIEM* (*Security Information and Event Management*) – це системи збору та аналізу подій безпеки;
- *DLP* (*Data Loss Prevention*) - це системи запобігання витоку даних;
- *MDM* (*Mobile Device Management*) - це управління мобільними пристроями;
- *WAF* (*Web Application Firewall*) - це захист веб-додатків;
- посилена автентифікація - це багатофакторна автентифікація (*MFA*);
- захист кінцевих точок (*Endpoint Protection Platforms - EPP, Endpoint Detection and Response - EDR*);

3. Обмеження. Периметр стає все більш умовним. Традиційні підходи, засновані на довірі до внутрішньої мережі, демонструють свою неефективність. Зростає складність управління різнорідними засобами захисту.

Етап 5: Ера цільових атак, інсайдерських загроз та пошук нових парадигм (середина 2010-х – наш час). Гіперконвергентні інфраструктури, Інтернет речей (*IoT*), штучний інтелект (*AI*) та машинне навчання (*ML*) в атаках та захисті, контейнеризація, мікросервісна архітектура. Подальше розмиття периметра.

1. Основні загрози:

- витончені та довготривалі *APT*-атаки;
- атаки на ланцюжки постачання;
- зростання кількості та складності програм-вимагачів (*ransomware*);
- зловживання штучним інтелектом для атак;
- інсайдерські загрози (навмисні та випадкові);
- атаки на *IoT*-пристрої;

˜ крадіжка облікових даних та їх використання для горизонтального переміщення в мережі;

2. Філософія та методи захисту: Рух до «Нульової Довіри»[9] та проактивної безпеки

˜ визнання неминучості компрометації – це припущення, що зловмисник вже всередині мережі або може туди потрапити;

˜ *Zero Trust Architecture* (*ZTA*) – це парадигма «ніколи не довіряй, завжди перевіряй». Мікросегментація, строгий контроль доступу на основі ідентичності та контексту, моніторинг всього трафіку;

˜ *SOAR* (*Security Orchestration, Automation and Response*) – це автоматизація реагування на інциденти;

˜ *Threat Intelligence* – це використання даних про загрози для проактивного захисту;

˜ *User and Entity Behavior Analytics* (*UEBA*) – це аналіз поведінки користувачів та сутностей для виявлення аномалій;

˜ безпека, вбудована в розробку (*DevSecOps*)[10];

3. Обмеження традиційних підходів. Стає очевидним, що покладатися на периметр та неявну довіру всередині мережі – вкрай небезпечно.

Таблиця 1.1 - Еволюція підходів до корпоративної безпеки

Етап	Роки	Домінуючі технології	Основні загрози	Філософія захисту
Ера мейнфреймів	1960 1980	Мейнфрейми, термінали	Фізичний доступ, помилки операторів	Фізична безпека, базовий контроль доступу
Локальні мережі (*LAN*)	1980 1990	ПК, *LAN*, перші сервери	Віруси, несанкціонований доступ всередині *LAN*	Антивіруси, паролі, розмежування доступу
Розквіт Інтернету «Замок і Рів»	1990 2000	Інтернет, веб, *email*, міжмережеві екрани, *VPN*	Інтернет-черв'яки, мережеві атаки, хакерські вторгнення	Захист периметра, *IDS*

Продовження таблиці 1.1

Деперіметризація	2000 2010	Мобільні пристрої, хмарні сервіси, *Wi-*	Атаки на веб-додатки, *APT*, за-	Розширений захист, *MFA*, *DLP*,

		Fi, NGFW, SIEM	грози мобільності	*EPP*/*EDR*
Сучасний етап *Zero Trust*	2010 – н.ч.	*IoT, AI*/*ML, ZTA, SOAR, UEBA*	Витончені *APT, ransomware,* інсайдерські загрози	«Ніколи не довіряй, завжди перевіряй»

Цей історичний огляд демонструє, що підходи до інформаційної безпеки постійно адаптуються до мінливого ландшафту технологій та загроз. Обмеження попередніх моделей стимулюють розробку нових, більш ефективних стратегій захисту, однією з яких і є концепція *Zero Trust*.

1.3 Основні загрози безпеці в сучасному інформаційному середовищі

Сучасне інформаційне середовище характеризується безпрецедентною складністю, взаємопов'язаністю та динамічністю. Це створює сприятливі умови для виникнення та поширення різноманітних загроз безпеці, які можуть мати руйнівні наслідки для корпоративних мереж та організацій в цілому. Розуміння актуального ландшафту загроз є ключовим для побудови ефективної системи захисту.

Загрози інформаційній безпеці можна класифікувати за різними критеріями: за джерелом (внутрішні/зовнішні), за мотивацією (фінансова вигода, шпигунство, хактивізм, кібервійна), за об'єктом атаки (дані, інфраструктура, користувачі), за методом впливу. Нижче розглянемо найбільш поширені та небезпечні категорії загроз.

1. Шкідливе програмне забезпечення (*Malware*)[11] - це широкий клас програм, розроблених для завдання шкоди комп'ютерним системам або для несанкціонованого доступу до них.

- віруси – це програми, що прикріплюються до інших файлів і поширюються при їх запуску;
- черв'яки (*Worms*)[12] – які самостійно поширюються мережею, експлуатуючи вразливості систем;
- троянські програми (*Trojans*)[13] – які маскуються під легітимне ПЗ, але виконують приховані шкідливі функції (крадіжка даних, створення бекдорів);

˜ програми-вимагачі (*Ransomware*)[14] – що шифрують дані на комп'ютері жертви або блокують доступ до системи, вимагаючи викуп за відновлення. Це одна з найбільш прибуткових та руйнівних загроз для бізнесу. Приклади: *WannaCry, Petya*/*NotPetya, Ryuk, Conti*;

˜ шпигунське ПЗ (*Spyware*) – що таємно збирає інформацію про користувача та його дії (паролі, банківські дані, історію веб-перегляду);

˜ рекламне ПЗ (*Adware*) – що автоматично відображає небажану рекламу;

˜ ботнети (*Botnets*) – це мережі заражених комп'ютерів («зомбі»), керовані зловмисником для здійснення *DDoS*-атак, розсилки спаму, майнінгу криптовалют тощо;

˜ руткити (*Rootkits*) – що надають зловмиснику привілейований доступ до системи, приховуючи свою присутність;

˜ безфайлові шкідливі програми (*Fileless Malware*) – що існують лише в оперативній пам'яті, не залишаючи слідів на жорсткому диску, що ускладнює їх виявлення традиційними антивірусами;

2. Атаки методом соціальної інженерії – це маніпулятивні техніки, спрямовані на обман людей з метою отримання конфіденційної інформації або спонукання їх до виконання певних дій, що компрометують безпеку. Людський фактор залишається однією з найслабших ланок у системі захисту.

˜ фішинг (*Phishing*) – це масова розсилка підроблених електронних листів, *SMS* або повідомлень в месенджерах, що імітують легітимні повідомлення від банків, державних установ, відомих сервісів;

˜ цільовий фішинг (*Spear Phishing*) – це більш персоніфікована атака, спрямована на конкретну особу або невелику групу осіб.

˜ вішинг (*Vishing*) – це голосовий фішинг, коли зловмисники використовують телефонні дзвінки для обману;

˜ смішинг (*SMiShing*) – це фішинг через *SMS*-повідомлення;

˜ претекстинг (*Pretexting*) – це створення вигаданого сценарію (претексту) для отримання інформації від жертви;

˜ приманка (*Baiting*) – це залишення заражених фізичних носіїв (*USB*-флешки) в місцях, де їх можуть знайти та використати співробітники;

3. Атаки на відмову в обслуговуванні (*DoS*/*DDoS*):

˜ *DoS* (*Denial of Service*) – це атака, спрямована на те, щоб зробити комп'ютерну систему або мережевий ресурс недоступним для легітимних користувачів шляхом перевантаження його запитами або експлуатації вразливостей.

˜ *DDoS* (*Distributed Denial of Service*) – це розподілена атака на відмову в обслуговуванні, що здійснюється одночасно з великої кількості скомпрометованих комп'ютерів (ботнету). Такі атаки значно потужніші та складніші для відбиття. *DDoS*-атаки можуть бути спрямовані на веб-сайти, сервери, мережеву інфраструктуру.

4. Атаки на веб-додатки та сервіси. Оскільки багато корпоративних сервісів доступні через веб-інтерфейси, вони стають привабливими цілями для атак.

˜ *SQL*-ін'єкції (*SQL Injection*) – це впровадження шкідливого *SQL*-коду в запити до бази даних, що дозволяє зловмиснику отримати, змінити або видалити дані.

˜ Міжсайтовий скриптинг (*Cross-Site Scripting – XSS*) – це впровадження шкідливого *JavaScript*-коду на веб-сторінку, який виконується в браузері користувача, дозволяючи викрадати сесійні кукі, облікові дані тощо.

˜ Підробка міжсайтових запитів (*Cross-Site Request Forgery – CSRF*) – що змушує браузер користувача виконувати небажані дії на сайті, де користувач вже автентифікований.

˜ Атаки на *API* (*Application Programming Interfaces*) – це коли зі зростанням використання *API* для взаємодії між сервісами, вони також стають об'єктом атак (недостатня автентифікація, витік даних).

5. Інсайдерські загрози (*Insider Threats*) – це загрози, що походять від осіб, які мають легітимний доступ до систем та даних компанії (співробітники, підрядники, партнери).

˜ зловмисні інсайдери – це навмисно завдають шкоди, крадуть дані, саботують системи (ображені співробітники, шпигуни);

˜ недбалі або необережні інсайдери – це ненавмисно створюють ризики через порушення політик безпеки, помилки, втрату пристроїв, потрапляння на вудку фішерів. Це найпоширеніший тип інсайдерської загрози;

˜ скомпрометовані інсайдери – це облікові записи легітимних користувачів захоплені зловмисниками;

6. Цілеспрямовані атаки (*Advanced Persistent Threats – APT*) – це складні, багатоетапні та довготривалі атаки, що зазвичай здійснюються добре організованими та фінансованими групами (часто державними або спонсорованими державою) з метою шпигунства, кіберсаботажу або великої фінансової вигоди. *APT*-атаки характеризуються:

˜ високою цілеспрямованістю коли атакують конкретні організації або галузі;

˜ прихованістю коли використовують складні техніки для уникнення виявлення протягом тривалого часу;

˜ наполегливістю якщо одна спроба не вдається, атакуючі шукають інші шляхи;

˜ використанням 0-*day* вразливостей – це експлуатація невідомих раніше вразливостей;

˜ багатовекторністю – це використання різних каналів та методів для проникнення та поширення;

7. Атаки на ланцюжки постачання (*Supply Chain Attacks*) – це компрометація менш захищених постачальників програмного або апаратного забезпечення з метою отримання доступу до їхніх клієнтів (більш великих та захищених організацій). Приклад: атака на *SolarWinds*.

8. Загрози, пов'язані з *IoT* та *OT*:

˜ Інтернет речей (*IoT*) – це велика кількість підключених пристроїв (камери, сенсори, розумні прилади) часто мають слабкий захист, що робить їх легкою мішенню для створення ботнетів або отримання доступу до корпоративної мережі.

˜ Операційні технології (*OT*) – це системи управління промисловими процесами (*SCADA, ICS*) все частіше підключаються до корпоративних мереж та Інтернету, що робить їх вразливими до кібератак, які можуть мати фізичні наслідки (зупинка виробництва, аварії).

9. Крадіжка та компрометація облікових даних. Паролі залишаються слабкою ланкою. Зловмисники використовують різні методи для їх отримання: підбір (*brute-force, dictionary attacks*), фішинг, шкідливе ПЗ, аналіз витоків даних з інших сервісів. Скомпрометовані облікові дані дозволяють отримати несанкціонований доступ та здійснювати горизонтальне переміщення всередині мережі.

10. Загрози, пов'язані з хмарними технологіями. Хоча хмарні провайдери забезпечують високий рівень безпеки своєї інфраструктури, відповідальність за безпеку даних та конфігурацій в хмарі часто лежить на клієнті (модель спільної відповідальності). Неправильні конфігурації, слабкий контроль доступу, незахищені *API* можуть призвести до витоку даних.

На рисунку 1.4 показана діаграма, що ілюструє приблизний розподіл частоти або впливу різних типів атак на мережу.

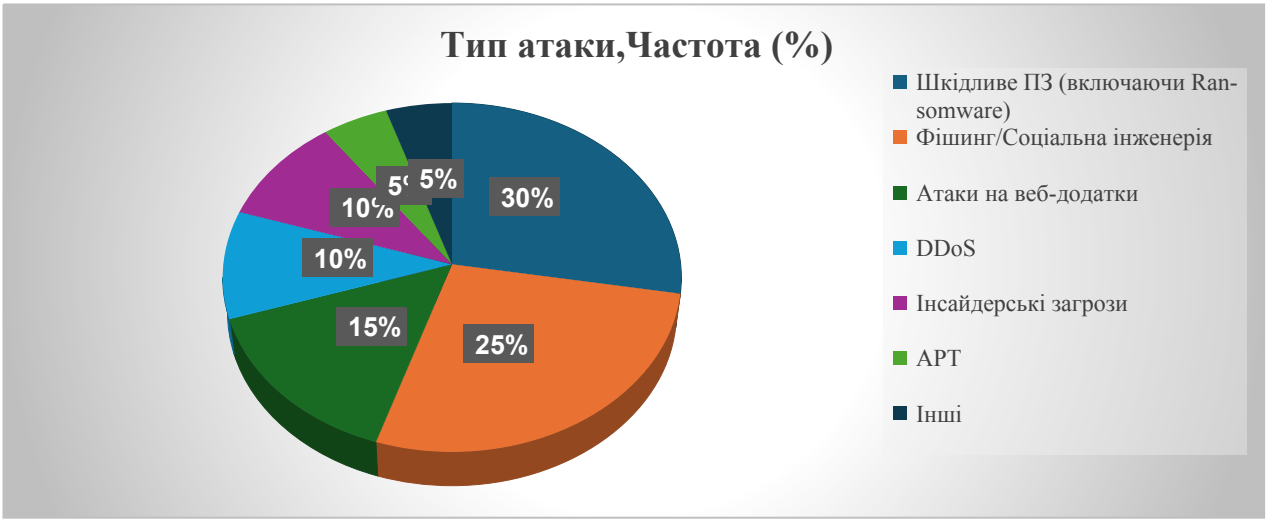

Рисунок 1.4 - Статистика типів кібератак

Наслідки успішних кібератак можуть бути катастрофічними:

˜ фінансові збитки;

˜ репутаційна шкода;

˜ операційні збої;

- правові наслідки;
- втрата інтелектуальної власності;.
- загроза національній безпеці;

Розуміння цих загроз та їх потенційних наслідків підкреслює нагальну потребу в ефективних стратегіях кібербезпеки. Традиційні моделі, зосереджені на захисті периметра, все частіше виявляються недостатніми для протистояння сучасному різноманіттю векторів атак та витонченості зловмисників, що й обумовлює перехід до нових парадигм, таких як *Zero Trust*.

1.4 Традиційні моделі безпеки: переваги та обмеження

Протягом десятиліть корпоративні мережі покладалися на певні усталені моделі безпеки для захисту своїх інформаційних активів. Ці моделі еволюціонували разом із технологіями, проте їхні фундаментальні принципи часто залишалися незмінними, базуючись на ідеї чіткого розмежування «довіреного» внутрішнього середовища та «недовіреного» зовнішнього світу. Розглянемо ключові традиційні моделі, їхні сильні сторони та, що особливо важливо для контексту даної роботи, їхні обмеження в сучасних умовах.

1. Модель «Замок і Рів» (*Perimeter Security Model* / *Castle and Moat*) - це, мабуть, найвідоміша і найдовше використовувана модель корпоративної безпеки.

Основний принцип – це побудова міцного захисного периметра навколо корпоративної мережі, подібного до стін замку, оточеного ровом. Внутрішня мережа (*LAN*) вважається довіреною зоною («всередині замку»), тоді як зовнішній світ (Інтернет) – недовіреною (рисунок 1.5)

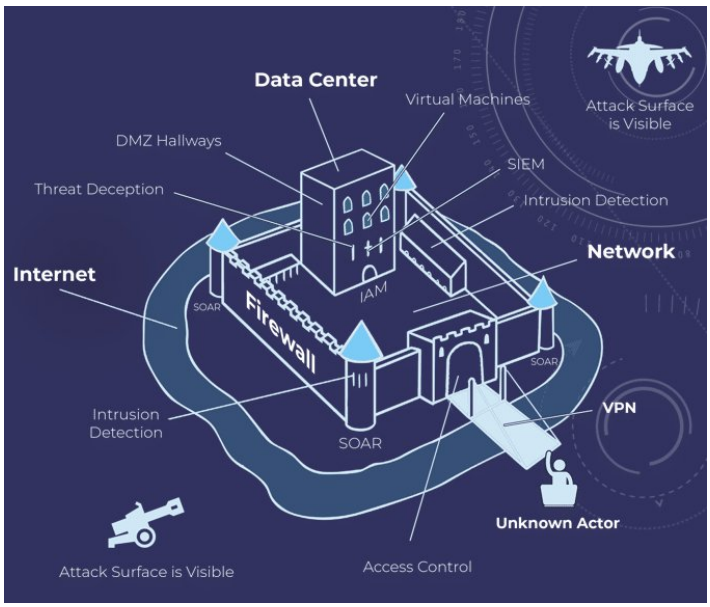

Рисунок 1.5 - Деталізована схема моделі «Замок і Рів»

Ключові технології:

- міжмережеві екрани (*Firewalls*);
- системи виявлення/запобігання вторгнень (*IDS*/*IPS*);
- *VPN* (*Virtual Private Networks*);
- проксі-сервери;
- демілітаризовані зони (*DMZ*);

Переваги:

- простота концепції та реалізації;
- чітке розмежування;
- ефективність проти масових, нецільових зовнішніх атак;
- централізований контроль;

Обмеження:

- «Тверда оболонка, м'яка середина», якщо зловмиснику вдається подолати периметр (через фішинг, 0-*day* вразливість, скомпрометований *VPN*-акаунт), він отримує відносно вільний доступ до ресурсів всередині «довіреної» мережі, оскільки внутрішній трафік часто не піддається такому ж ретельному контролю.
- інсайдерські загрози, тут модель практично не захищає від зловмисних або недбалих дій інсайдерів, які вже знаходяться всередині довіреного периметра.

˜ розмиття периметра тут сучасні тенденції, такі як хмарні сервіси, мобільні пристрої (*BYOD*), віддалена робота, *IoT,* роблять традиційний периметр все більш умовним та важко контрольованим. Дані та користувачі знаходяться як всередині, так і поза ним.

˜ горизонтальне переміщення (*Lateral Movement*), після компрометації однієї системи всередині мережі зловмисники можуть легко переміщатися до інших систем, оскільки між ними існує високий рівень довіри.

˜ шифрований трафік, це зростання частки шифрованого трафіку (*HTTPS, SSL*/*TLS*) ускладнює його інспекцію традиційними міжмережевими екранами без використання ресурсоємних технік *SSL Inspection* (*Man-in-the-Middle*).

˜ складність управління політиками, зі зростанням бізнесу та кількості сервісів правила на міжмережевих екранах можуть стати надзвичайно складними, що призводить до помилок конфігурації.

˜ припущення про довіру, це фундаментальна проблема – неявна довіра до будь-чого, що знаходиться всередині периметра.

2. Модель «Захист у глибину» (*Defense in Depth*) - ця модель є розвитком ідеї периметрального захисту та визнає, що жоден окремий засіб захисту не є абсолютно надійним.

Основний принцип – це створення кількох рівнів (шарів) захисту, які дублюють один одного. Якщо один рівень буде подолано, наступний повинен зупинити або сповільнити зловмисника.

Схематичне зображення цілі в центрі, оточеної концентричними колами, що представляють різні рівні захисту: політики та процедури, фізична безпека, безпека периметра, безпека внутрішньої мережі, безпека хостів, безпека додатків, безпека даних (рисунок 1.6).

Рисунок 1.6 - Модель «Захист у глибину»

Ключові технології та підходи:

- захист кінцевих точок (*Endpoint Security*);
- мережева сегментація;
- контроль доступу (*Access Control*);
- шифрування даних;
- моніторинг та аудит безпеки;
- управління вразливостями та патч-менеджмент;
- навчання користувачів з питань безпеки;
- фізична безпека;

Переваги:

- підвищена стійкість до атак;
- уповільнення зловмисника;
- зменшення поверхні атаки на кожному рівні;
- можливість виявлення на різних етапах атаки;

Обмеження:

- впровадження та підтримка численних рівнів захисту може бути складним та дорогим;
- різні засоби захисту від різних виробників можуть погано взаємодіяти між собою;
- все ще може базуватися на неявній довірі всередині сегментів;

- неправильна конфігурація будь-якого з рівнів або помилки користувачів можуть нівелювати переваги моделі;
- не вирішує проблему фундаментальної довіри;

3. Моделі контролю доступу (*Access Control Models*) - це не самостійні архітектурні моделі безпеки мережі, вони є фундаментальними компонентами будь-якої системи захисту і традиційно використовуються в рамках вищезгаданих моделей.

Дискреційна модель контролю доступу (*DAC – Discretionary Access Control*): Власник ресурсу (файлу, об'єкта) сам визначає, хто має до нього доступ і які права (читання, запис, виконання). Приклад: права доступу до файлів у *Windows* або *Linux*.

Мандатна модель контролю доступу (*MAC – Mandatory Access Control*): Доступ до ресурсів регулюється на основі міток безпеки, присвоєних суб'єктам (користувачам) та об'єктам (файлам). Система (адміністратор безпеки) централізовано визначає правила доступу. Часто використовується у військових та урядових системах.

Рольова модель контролю доступу (*RBAC – Role-Based Access Control*): Права доступу надаються не окремим користувачам, а ролям (наприклад, «бухгалтер», «адміністратор», «менеджер»). Користувачам присвоюються відповідні ролі. Це найпоширеніша модель у корпоративному середовищі.

Фундаментальною проблемою більшості традиційних моделей безпеки є їхня опора на концепцію «довіреної мережі». Як тільки зловмисник або шкідливе ПЗ потрапляє всередину цієї «довіреної» зони, він часто отримує значну свободу дій. Сучасний ландшафт загроз, де атаки стають все більш витонченими, а інсайдерські загрози та компрометація облікових даних – поширеними явищами, демонструє недостатність такого підходу.

Крім того, традиційні моделі погано адаптуються до таких реалій, як:

- хмарні обчислення;
- мобільність та *BYOD*;
- віддалена робота;

- інтернет речей (*IoT*);
- складні ланцюжки постачання ПЗ та послуг;

Ці обмеження чітко вказують на те, що парадигма безпеки, заснована на периметрі та неявній довірі, більше не відповідає вимогам часу. Необхідний перехід до моделі, яка не довіряє жодному користувачеві чи пристрою за замовчуванням, незалежно від його місцезнаходження, і постійно перевіряє легітимність кожного запиту на доступ. Саме такою моделлю є «Нульова Довіра» (*Zero Trust*), детальний розгляд якої буде предметом наступних розділів.

1.5 Висновок до розділу 1

У даному розділі було закладено теоретичний фундамент для розуміння проблематики кібербезпеки в контексті сучасних корпоративних мереж та обґрунтування необхідності переходу до нових моделей захисту інформації.

По-перше, ми визначили ключові поняття: кіберпростір як складне, багатогранне середовище взаємодії інформаційних технологій, та інформаційна безпека як стан захищеності інформації, що ґрунтується на принципах конфіденційності, цілісності та доступності (тріада КЦД), а також додаткових аспектах, таких як невідмовність, автентичність та підзвітність. Було підкреслено, що кібербезпека є невід'ємною частиною інформаційної безпеки, сфокусованою на захисті в цифровому середовищі.

По-друге, проаналізовано етапи розвитку інформаційної безпеки в корпоративних мережах, починаючи від ери мейнфреймів з акцентом на фізичний захист, через становлення периметральної безпеки в епоху розквіту Інтернету («замок і рів»), до сучасного етапу деперіметризації, спричиненого хмарними технологіями, мобільністю та складними цільовими атаками. Ця еволюція чітко демонструє, як підходи до безпеки постійно адаптувалися до змін у технологічному ландшафті та спектрі загроз.

По-третє, було розглянуто основні загрози безпеці в сучасному інформаційному середовищі. Від традиційного шкідливого ПЗ та фішингу до витонче-

них *APT*-атак, програм-вимагачів, інсайдерських загроз та атак на ланцюжки постачання – їх різноманітність та складність невпинно зростають. Наслідки таких атак можуть бути руйнівними, включаючи значні фінансові втрати, репутаційну шкоду та операційні збої.

По-четверте, було проведено критичний аналіз традиційних моделей безпеки, зокрема моделі «замок і рів» та «захисту в глибину», а також розглянуто класичні моделі контролю доступу. Було визнано їхні історичні переваги, такі як простота концепції периметральної безпеки та підвищена стійкість завдяки багаторівневому захисту. Однак, головний акцент було зроблено на їхніх фундаментальних обмеженнях в умовах сучасних викликів.

Таким чином, аналіз теоретичних основ кібербезпеки, еволюції захисних стратегій, сучасного ландшафту загроз та обмежень традиційних моделей безпеки логічно підводить до висновку про нагальну потребу в переосмисленні підходів до захисту корпоративних інформаційних систем. Стає очевидним, що стара парадигма «довіряй, але перевіряй», яка часто трансформувалася на практиці в «довіряй за замовчуванням всередині периметра», більше не є життєздатною.

Ці висновки створюють необхідне підґрунтя для переходу до розгляду більш прогресивних концепцій безпеки, зокрема моделі «Нульової Довіри» (*Zero Trust*).

РОЗДІЛ 2
КОНЦЕПЦІЯ *ZERO TRUST*: ПРИНЦИПИ, РЕАЛІЗАЦІЯ ТА ЗАСТОСУВАННЯ

2.1 Виникнення та розвиток концепції *Zero Trust*

Концепція *Zero Trust* не виникла миттєво; її появі передував тривалий період усвідомлення обмеженості традиційних підходів до безпеки, особливо в умовах стрімкого розвитку інформаційних технологій, зміни ландшафту загроз та трансформації корпоративних мереж. Традиційна модель безпеки, що базувалася на периметрі, виявилася все менш ефективною в світі, де дані та користувачі розподілені, а поняття «внутрішньої» довіреної мережі втратило свою актуальність.

Передумови виникнення:

˜ деперіметризація: як зазначалося в Розділі 1, зростання популярності хмарних сервісів, мобільних технологій, віддаленої роботи та політик *BYOD* (*Bring Your Own Device*) призвело до розмиття чіткого корпоративного периметра. Організації більше не могли покладатися на захист лише на межі своєї мережі.

˜ еволюція загроз: кіберзагрози ставали все більш складними та цілеспрямованими. Зростала кількість успішних атак, що долали периметральний захист, а також інсайдерських загроз. Стало очевидним, що припущення про безпечність внутрішньої мережі є хибним.

˜ ранні ініціативи: ще до формалізації *Zero Trust* існували ініціативи та концепції, що ставили під сумнів периметральну модель. Наприклад, на початку 2000-х років група аналітиків під назвою *Jericho Forum*® активно просувала ідею «деперіметризації» (*de-perimeterisation*). Вони стверджували, що покладатися на єдиний укріплений периметр недостатньо, і необхідно зосередитися на захисті самих даних, незалежно від їхнього місцезнаходження. Їхні роботи підкреслювали важливість шифрування, безпечної співпраці та контролю доступу на рівні даних.

˜ роботи Агентства оборонних інформаційних систем США (*DISA*): у 2007 році *DISA* опублікувало стратегію «*Global Information Grid* (*GIG*) *Content Delivery Service Initial Capabilities Document*», де обговорювалися ідеї безпеки, орієнтованої на дані, та необхідність перевірки користувачів і пристроїв перед наданням доступу, що перегукувалося з майбутніми принципами *Zero Trust*.

Формалізація концепції Джоном Кіндервагом. Термін «*Zero Trust*» був вперше запропонований та популяризований Джоном Кіндервагом (*John Kindervag*), на той час аналітиком компанії *Forrester Research,* у 2010 році. У своїй доповіді «*No More Chewy Centers*: *Introducing The Zero Trust Model Of Information Security*» Кіндерваг розкритикував традиційну модель безпеки «замок і рів», яка передбачала «тверду оболонку, але м'яку, вразливу середину». Він стверджував, що довіра є вразливістю, і що в контексті мережевої безпеки її слід усунути.

Кіндерваг запропонував три основні концепції для побудови архітектури *Zero Trust*:

1. Забезпечення доступу до всіх ресурсів на основі потреби в інформації (*Ensure all resources are accessed securely regardless of location*): Незалежно від того, де знаходиться ресурс (в дата-центрі, хмарі) чи користувач (в офісі, віддалено), доступ має надаватися безпечно.

2. Застосування принципу найменших привілеїв та суворий контроль доступу (*Adopt a least privilege strategy and strictly enforce access control*): Користувачі, пристрої та додатки повинні мати лише мінімально необхідні права для виконання своїх завдань.

3. Інспекція та логування всього трафіку (*Inspect and log all traffic*): Увесь мережевий трафік, як внутрішній, так і зовнішній, повинен перевірятися на наявність загроз, а всі дії – логуватися для аудиту та виявлення аномалій.

Ключовим гаслом моделі стало: «Ніколи не довіряй, завжди перевіряй» (*Never trust, always verify*).

Це означало, що жоден користувач, пристрій чи додаток не повинен вважатися довіреним за замовчуванням, навіть якщо він знаходиться всередині

корпоративної мережі. Кожен запит на доступ до ресурсу має бути автентифікований та авторизований.

Після публікацій *Forrester* концепція *Zero Trust* почала набирати популярність, хоча її впровадження на початкових етапах було повільним через необхідність зміни парадигми мислення та значних технологічних перебудов (рисунок 2.1).

Рисунок 2.1 - Хронологія розвитку концепції *Zero Trust*

˜ розширення моделі (*Zero Trust eXtended - ZTX*): *Forrester* згодом розширила початкову модель до *Zero Trust eXtended* (*ZTX*) *Ecosystem,* визнаючи, що *Zero Trust* – це не окремий продукт, а комплексна стратегія, що охоплює дані, мережі, робочі навантаження, людей та пристрої. *ZTX* запропонувала більш детальну дорожню карту для впровадження.

˜ вплив *Google BeyondCorp*: у 2014 році *Google* опублікувала низку статей, що описували їхню внутрішню ініціативу безпеки під назвою *BeyondCorp*. Ця модель реалізовувала принципи *Zero Trust,* дозволяючи співробітникам безпечно працювати з будь-якої мережі без необхідності використання традиційного *VPN*. *BeyondCorp* продемонструвала практичну реалізацію *Zero Trust* у великій організації та значно сприяла популяризації концепції.

Ключові ідеї *BeyondCorp* включали:

˜ доступ до сервісів не повинен залежати від того, з якої мережі він здійснюється;

˜ доступ до сервісів надається на основі того, що відомо про користувача та його пристрій;

˜ увесь доступ до сервісів повинен бути автентифікований, авторизований та зашифрований;

˜ стандартизація та керівництва (*NIST, CISA*): важливим етапом стало визнання та стандартизація концепції *Zero Trust* державними установами.

˜ *NIST Special Publication* 800-207 «*Zero Trust Architecture*» (2020): Національний інститут стандартів і технологій США (*NIST*) опублікував детальний документ, що визначає архітектуру *Zero Trust,* її логічні компоненти, сценарії розгортання та міркування щодо міграції. Цей документ став ключовим орієнтиром для організацій, що планують впровадження *ZTA*.

˜ керівництва *CISA* (*Cybersecurity and Infrastructure Security Agency*): *CISA* також активно розробляє та публікує керівництва щодо впровадження *Zero Trust* для федеральних установ та приватного сектору, підкреслюючи її важливість для національної кібербезпеки.

˜ розвиток таких технологій, як програмно-визначені мережі (*SDN*), програмно-визначені периметри (*SDP*), мікросегментація, рішення для управління ідентифікацією та доступом (*IAM*), багатофакторна автентифікація (*MFA*), аналітика поведінки користувачів та сутностей (*UEBA*), та інструменти оркестрації та автоматизації безпеки (*SOAR*) значно спростили практичну реалізацію принципів *Zero Trust*.

˜ акцент на ідентичності: з часом фокус *Zero Trust* все більше зміщується з мережево-центричного підходу на ідентично-центричний. Ідентичність (користувача, пристрою, сервісу, робочого навантаження) стає новим периметром безпеки.Сьогодні *Zero Trust* – це не просто модне слово, а фундаментальна стратегія безпеки, яку активно впроваджують організації різного масштабу по всьому світу для захисту своїх активів у складному та динамічному кіберпросторі. Вона

визнана провідними аналітичними агентствами та постачальниками рішень безпеки як найбільш ефективний підхід до протистояння сучасним кіберзагрозам.

2.2 Основні принципи моделі *Zero Trust*

Модель *Zero Trust* базується на кількох фундаментальних принципах, які разом формують цілісний підхід до забезпечення безпеки. Ці принципи кардинально відрізняються від припущень, що лежать в основі традиційних моделей безпеки. Центральною ідеєю, як вже зазначалося, є відмова від поняття «довіреної» внутрішньої мережі та перехід до моделі, де довіра ніколи не надається за замовчуванням.

1. «Ніколи не довіряй, завжди перевіряй» (*Never Trust, Always Verify*) Це головний девіз і наріжний камінь *Zero Trust*. Він означає, що кожен користувач, пристрій, додаток, мережевий потік або запит на доступ до ресурсу повинен розглядатися як потенційно ворожий, незалежно від його походження (внутрішнього чи зовнішнього).

˜ відсутність неявної довіри: на відміну від традиційних моделей, де пристрої та користувачі всередині корпоративної мережі часто мали неявну довіру, *Zero Trust* вимагає явної перевірки кожного запиту;

˜ безперервна перевірка: перевірка не є одноразовим актом на вході. Вона має відбуватися постійно протягом усього сеансу доступу. Зміна контексту (наприклад, геолокації користувача, поведінки пристрою) може вимагати повторної автентифікації або зміни рівня доступу;

2. Припущення про компрометацію (*Assume Breach* / *Assume Compromise*) *Zero Trust* виходить з того, що атакуючі вже присутні в мережі або неминуче зможуть туди проникнути. Це фундаментальна зміна мислення порівняно з традиційним підходом, який зосереджувався на запобіганні проникненню на периметрі.

˜ фокус на виявленні та реагуванні: якщо припустити, що компрометація неминуча, акцент зміщується з чистої превенції на швидке виявлення зловмисної активності всередині мережі та ефективне реагування на інциденти;

˜ обмеження «вибухової хвилі»: механізми *Zero Trust,* такі як мікросегментація, спрямовані на те, щоб у разі компрометації одного сегмента чи ресурсу, зловмисник не міг легко поширитися на інші частини системи (обмеження горизонтального переміщення);

3. Явна перевірка (*Explicit Verification*). Кожен запит на доступ до ресурсу повинен бути явно перевірений на основі максимально можливої кількості доступних точок даних (сигналів). Це включає, але не обмежується:

˜ ідентичність користувача: хто намагається отримати доступ? перевірка облікових даних, ролей, атрибутів;

˜ стан пристрою (*device posture*): з якого пристрою здійснюється доступ? чи відповідає пристрій політикам безпеки (оновлення ос, наявність антивірусу, відсутність шкідливого пз, сертифікати)?

˜ місцезнаходження (*location*): звідки здійснюється доступ (географічне положення, *ip*-адреса, тип мережі)?

˜ тип сервісу/додатку (*service*/*application*): до якого ресурсу запитується доступ? наскільки чутливий цей ресурс?

˜ тип даних (*data sensitivity*): які дані запитуються? рівень їхньої конфіденційності.

˜ час та частота запитів: чи є запит аномальним порівняно зі звичайною поведінкою?

4. Застосування принципу найменших привілеїв (*Least Privilege Access*). Користувачам, додаткам та системам надається лише мінімально необхідний рівень доступу та прав для виконання конкретного завдання або функції. Цей принцип застосовується як до тривалості доступу (*Just-in-Time access*), так і до обсягу прав (*Just-Enough access*).

˜ гранулярний контроль: замість надання широкого доступу до цілих сегментів мережі або наборів ресурсів, доступ надається до конкретних додатків, сервісів або даних.

˜ зменшення поверхні атаки: обмеження привілеїв значно зменшує потенційну шкоду, яку може завдати скомпрометований обліковий запис або вразливий додаток. Якщо зловмисник отримує контроль над таким акаунтом, його можливості для подальшого просування та завдання шкоди будуть суттєво обмежені.

5. Мікросегментація (*Microsegmentation*). На відміну від традиційної макросегментації (наприклад, поділу мережі на *DMZ,* внутрішню мережу, гостьову мережу), мікросегментація передбачає створення значно менших, гранулярних зон безпеки навколо окремих робочих навантажень, додатків, або навіть окремих серверів чи віртуальних машин.

˜ ізоляція робочих навантажень: кожен мікросегмент має власні політики безпеки, що контролюють трафік, який входить та виходить з нього;

˜ стримування загроз: якщо один мікросегмент скомпрометовано, інші сегменти залишаються захищеними, що обмежує можливість горизонтального переміщення зловмисників по мережі;

˜ технології реалізації: мікросегментація може бути реалізована за допомогою програмно-визначених мереж (*sdn*), міжмережевих екранів наступного покоління (*ngfw*), агентів на хостах та інших технологій;

Для більшого розуміння на рисунку 2.2 продемонстрована схема основних принципів моделі.

Рисунок 2.2 - Концептуальна діаграма основних принципів *Zero Trust*

6. Використання багатофакторної автентифікації (*MFA*) повсюдно Багатофакторна автентифікація є критично важливим компонентом *Zero Trust*. Вона вимагає від користувачів надання двох або більше доказів (факторів) для підтвердження своєї особи. Типові фактори включають:

- щось, що користувач знає (пароль, *pin*-код);
- щось, чим користувач володіє (апаратний токен, смарт-карта, мобільний телефон для отримання одноразових кодів);
- щось, що є частиною користувача (біометричні дані: відбиток пальця, розпізнавання обличчя);
- зменшення ризику компрометації облікових даних: *mfa* значно ускладнює зловмисникам отримання несанкціонованого доступу, навіть якщо їм вдалося викрасти пароль;

7. Моніторинг, аналітика та автоматизація (*Monitoring, Analytics, and Automation*) *Zero Trust* вимагає безперервного моніторингу активності в мережі, на кінцевих точках та в додатках для виявлення аномалій та потенційних загроз.

˜ збір та аналіз логів: системи *SIEM* (*Security Information and Event Management*) та *UEBA* (*User and Entity Behavior Analytics*) відіграють ключову роль у зборі, кореляції та аналізі даних з різних джерел для виявлення підозрілої активності;

˜ виявлення загроз у реальному часі: аналіз поведінки дозволяє виявляти відхилення від норми, що можуть свідчити про компрометацію або інсайдерську загрозу;

˜ автоматизоване реагування: інструменти *SOAR* (*Security Orchestration, Automation and Response*) дозволяють автоматизувати реакцію на певні типи інцидентів (наприклад, блокування скомпрометованого облікового запису, ізоляція зараженого пристрою), що прискорює реагування та зменшує навантаження на аналітиків безпеки;

Ці принципи не є ізольованими; вони взаємопов'язані та підсилюють один одного. Впровадження *Zero Trust* – це не встановлення одного продукту, а побудова комплексної архітектури та зміна культури безпеки в організації, де безпека інтегрована в усі процеси та системи (рисунок 2.3).

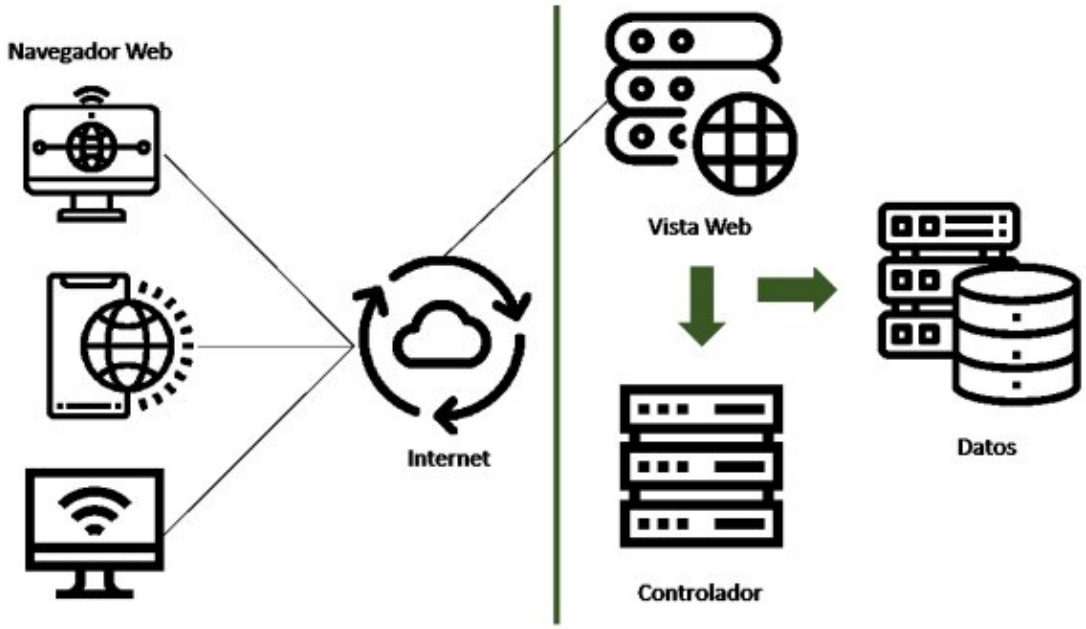

Рисунок 2.3 - Схематичне порівняння макросегментації та мікросегментації

2.3 Сфери застосування концепції *Zero Trust* в корпоративних середовищах

Концепція *Zero Trust* є універсальною і може застосовуватися до різних аспектів корпоративної IT-інфраструктури та бізнес-процесів. Її гнучкість дозволяє організаціям поетапно впроваджувати принципи Нульової Довіри, фокусуючись на найбільш критичних ділянках. Нижче розглянуто основні сфери застосування *ZTA*.

1. Захист користувачів та ідентичностей (*Protecting Users and Identities*). Ідентичність є центральним елементом в архітектурі *Zero Trust*. Захист користувачів охоплює:

- надійна автентифікація: повсюдне впровадження багатофакторної автентифікації (*MFA*) для всіх користувачів (співробітників, підрядників, клієнтів) при доступі до будь-яких корпоративних ресурсів. Використання адаптивної *MFA,* де вимоги до автентифікації змінюються залежно від контексту (ризику сесії, геолокації, поведінки);
- управління життєвим циклом ідентичностей (*IAM*): централізоване управління створенням, модифікацією та видаленням облікових записів. Автоматизація процесів надання та відкликання доступів;
- аналітика поведінки користувачів (*UEBA*): моніторинг дій користувачів для виявлення аномальної поведінки, що може свідчити про компрометацію облікового запису або інсайдерську загрозу;
- захист привілейованих облікових записів (*PAM*): особлива увага до адміністративних та сервісних акаунтів, впровадження рішень для управління привілейованим доступом (обмеження часу доступу, ротація паролів, моніторинг сесій);
- застосування до віддалених працівників та *BYOD*: забезпечення безпечного доступу для співробітників, що працюють з дому або використовують власні пристрої, шляхом суворої перевірки ідентичності та стану пристрою;

2. Захист пристроїв (*Protecting Devices* / *Endpoints*). Кожен пристрій, що отримує доступ до корпоративних ресурсів (ПК, ноутбуки, мобільні телефони, сервери, *IoT*-пристрої), розглядається як потенційна точка входу для зловмисників.

˜ перевірка стану пристрою (*Device Posture Assessment*): перед наданням доступу система перевіряє відповідність пристрою політикам безпеки: наявність оновлень ОС, антивірусного ПЗ, відсутність відомих вразливостей, статус шифрування диска, наявність корпоративних сертифікатів;

˜ управління мобільними пристроями (*MDM*) / уніфіковане управління кінцевими точками (*UEM*): інструменти для централізованого управління політиками безпеки на корпоративних та особистих мобільних пристроях (*BYOD*);

˜ платформи захисту кінцевих точок (*EPP*) та виявлення та реагування на кінцевих точках (*EDR*): розширені засоби для запобігання, виявлення та реагування на загрози на кінцевих пристроях;

˜ ізоляція скомпрометованих пристроїв: можливість автоматичної або ручної ізоляції пристрою від мережі у разі виявлення ознак компрометації;

3. Захист мережі (*Protecting the Network*). Хоча *Zero Trust* децентралізує фокус з периметра, мережева безпека залишається важливою, але трансформується.

˜ мікросегментація та програмно-визначені периметри (*SDP*): створення гранулярних сегментів навколо критичних ресурсів для обмеження горизонтального переміщення. *SDP* (також відомі як «чорні хмари») роблять інфраструктуру невидимою для неавторизованих користувачів;

˜ інспекція трафіку: глибока інспекція всього мережевого трафіку (включаючи внутрішній та шифрований) для виявлення шкідливої активності, аномалій та порушень політик. Це може включати *SSL*/*TLS* інспекцію;

˜ системи запобігання вторгненням (*IPS*): для виявлення та блокування відомих атак на мережевому рівні;

˜ контроль доступу до мережі (*NAC*): забезпечення того, що тільки авторизовані та відповідні політикам пристрої можуть підключатися до мережі.

˜ безпека *Wi-Fi*: застосування принципів *ZT* до бездротових мереж, включаючи надійну автентифікацію користувачів та пристроїв;

4. Захист робочих навантажень (*Protecting Workloads*). Робочі навантаження – це додатки, сервіси, віртуальні машини, контейнери, функції без сервера, що виконують бізнес-логіку.

˜ безпека *API*: захист інтерфейсів програмування додатків (*API*), через які відбувається взаємодія між сервісами. Включає автентифікацію, авторизацію, обмеження швидкості запитів, валідацію вхідних даних;

˜ безпека контейнерів та *Kubernetes*: впровадження політик безпеки на всіх етапах життєвого циклу контейнерів (збірка, розгортання, виконання). Сканування образів на вразливості, контроль доступу, мережева сегментація в середовищах *Kubernetes*;

˜ безпека «інфраструктура як код» (*IaC*): застосування політик безпеки та сканування на вразливості до шаблонів *IaC* (*Terraform, CloudFormation*) для запобігання розгортанню небезпечних конфігурацій;

˜ мікросегментація на рівні додатків: ізоляція окремих компонентів додатку або мікросервісів;

5. Захист даних (*Protecting Data*) Однією з кінцевих цілей *Zero Trust* є захист даних, незалежно від того, де вони зберігаються, передаються чи обробляються.

˜ класифікація даних: ідентифікація та класифікація даних за рівнем чутливості для застосування відповідних політик захисту;

˜ шифрування: шифрування даних під час зберігання (*data-at-rest*) та передачі (*data-in-transit*). Управління ключами шифрування;

˜ системи запобігання витоку даних (*DLP*): моніторинг та контроль переміщення чутливих даних для запобігання їх несанкціонованому витоку;

˜ управління правами доступу до даних: гранулярний контроль того, хто і за яких умов може отримувати доступ до конкретних наборів даних;

˜ резервне копіювання та відновлення: забезпечення наявності захищених резервних копій для відновлення даних у разі інциденту (наприклад, атаки програми-вимагача);

6. Видимість та аналітика (*Visibility and Analytics*). Збір, кореляція та аналіз даних з усіх компонентів IT-середовища є критично важливими для *Zero Trust*.

˜ централізований збір логів (*Siem*): агрегація логів з мережевих пристроїв, серверів, додатків, систем безпеки для комплексного аналізу;

˜ аналітика загроз (*Threat Intelligence*): використання даних про актуальні загрози, вразливості та тактики зловмисників для проактивного захисту;

˜ моніторинг відповідності (*Compliance Monitoring*): забезпечення дотримання внутрішніх політик безпеки та зовнішніх регуляторних вимог;

˜ візуалізація та звітність: надання чітких дашбордів та звітів про стан безпеки, інциденти та ризики;

7. Автоматизація та оркестрація (*Automation and Orchestration*). Автоматизація рутинних завдань безпеки та оркестрація процесів реагування підвищують ефективність та швидкість.

˜ *SOAR*-платформи: автоматизація процесів реагування на інциденти, таких як блокування *IP*-адрес, ізоляція пристроїв, відкликання облікових записів.

˜ автоматизоване застосування політик: динамічне оновлення та застосування політик безпеки на основі змін у ризиковому ландшафті або контексті доступу.

˜ *DevSecOps*: інтеграція практик безпеки в процеси розробки та експлуатації програмного забезпечення (*CI*/*CD*) для раннього виявлення та усунення вразливостей.

Застосування *Zero Trust* не обмежується лише цими сферами. Принципи можуть бути адаптовані до специфічних потреб організації, включаючи захист *IoT* та *OT* середовищ, забезпечення безпеки ланцюжків постачання та захист хмарних інфраструктур. Ключовим є розуміння, що *Zero Trust* – це стратегічний підхід, який вимагає комплексного планування та послідовного впровадження (рисунок 2.4).

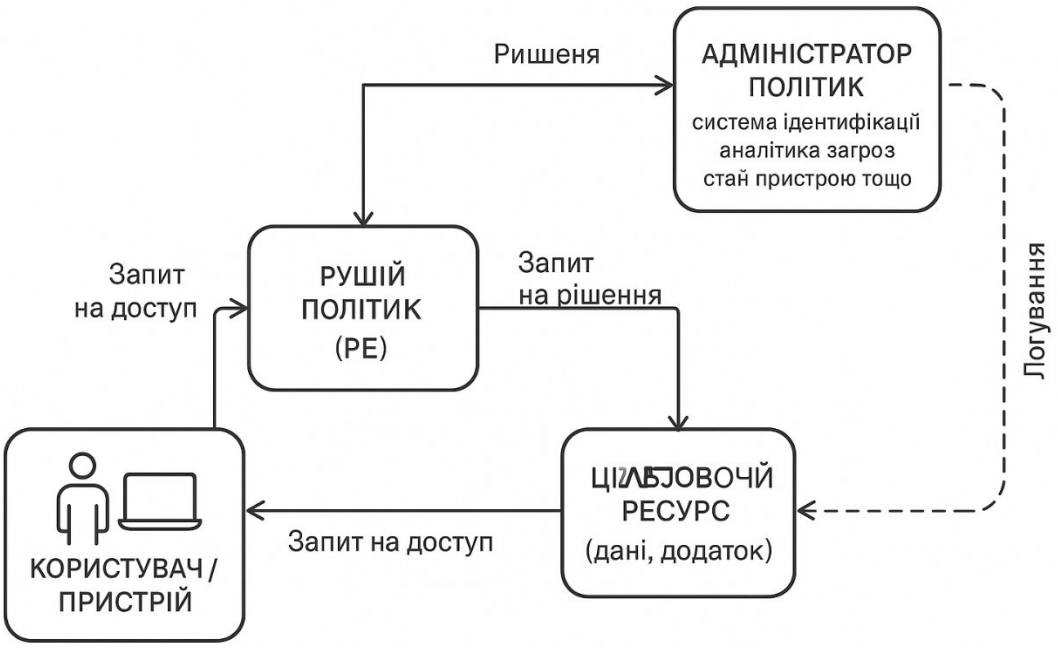

Рисунок 2.4 - Діаграма потоку запиту на доступ в архітектурі *Zero Trust*

2.4 Приклади впровадження *Zero Trust* у сучасних компаніях

Хоча повне впровадження *Zero Trust* є тривалим процесом, багато компаній вже досягли значних успіхів у реалізації цієї концепції, демонструючи її практичну цінність. Розглянемо кілька прикладів та підходів.

1. *Google*: *BeyondCorp*. Ініціатива *Google BeyondCorp,* розпочата ще у 2011 році та детально описана у публікаціях з 2014 року, є одним із найбільш відомих та впливових прикладів реалізації *Zero Trust*. *Google* зіткнулася з обмеженнями традиційної периметральної моделі та вирішила фундаментально змінити свій підхід до корпоративної безпеки.

Передумови:

- зростання кількості мобільних та віддалених працівників;
- використання різноманітних пристроїв (корпоративних та особистих);
- потреба у безпечному доступі до внутрішніх додатків з будь-якої точки світу;
- усвідомлення, що внутрішня мережа не є апріорі безпечною;

Результати та переваги:

- значне підвищення рівня безпеки;
- можливість для співробітників безпечно працювати з будь-якого місця та пристрою;
- спрощення доступу до ресурсів порівняно з традиційним *Vpn*;
- гранулярний контроль доступу до кожного додатку;

BeyondCorp є яскравим прикладом того, як компанія може відмовитися від традиційної мережевої довіри на користь моделі, де довіра динамічно оцінюється для кожного запиту.

2. *Microsoft*: *Zero Trust Maturity Model Microsoft* є одним з провідних постачальників рішень безпеки та активно просуває концепцію *Zero Trust,* пропонуючи власну модель зрілості та набір інструментів для її реалізації.

Підхід *Microsoft*: *Zero Trust* в розумінні *Microsoft* базується на трьох основних принципах:

1. *Verify explicitly* (Явна перевірка). Завжди автентифікувати та авторизувати на основі всіх доступних точок даних.

2. *Use least privileged access* (Використання найменших привілеїв). Обмежувати доступ користувачів за допомогою *Just-In-Time* та *Just-Enough Access* (*JIT*/*JEA*), адаптивних політик на основі ризиків.

3. *Assume breach* (Припущення про компрометацію). Мінімізувати «*blast radius*» та сегментувати доступ. Перевіряти наскрізне шифрування. Використовувати аналітику для отримання видимості, виявлення загроз та покращення захисту.

Microsoft пропонує модель зрілості *Zero Trust* (*Traditional, Advanced, Optimal*), яка допомагає організаціям оцінити свій поточний стан та розробити дорожню карту для поступового впровадження принципів *ZT*.

Фокус на інтеграції: Сила підходу *Microsoft* полягає в інтеграції різних продуктів безпеки, що дозволяє створювати комплексне рішення *Zero Trust*.

3. *Netflix*: Управління доступом та безпека хмарних ресурсів *Netflix,* компанія, що значною мірою покладається на хмарну інфраструктуру (перева-

жно *AWS*), також впроваджує принципи *Zero Trust* для захисту своїх сервісів та даних.

Виклики:

- величезна, динамічна та розподілена хмарна інфраструктура;
- велика кількість розробників та інженерів, яким потрібен доступ до ресурсів;
- необхідність забезпечити високу доступність та надійність сервісів;

Підходи до *Zero Trust*:

- гранулярне управління доступом (*Fine-Grained Access Control*);
- короткоживучі облікові дані;
- автоматизація безпеки;
- моніторинг та логування;
- «*Paved Road*»;

Основний акцент робиться на автоматизації управління доступом, безпеці конфігурацій та безперервному моніторингу в динамічному хмарному середовищі.

4. Впровадження *Zero Trust* у фінансовому секторі. Фінансові установи є привабливою ціллю для кібератак, тому вони одними з перших почали адаптувати принципи *Zero Trust*. Драйвери:

- захист чутливих клієнтських даних та фінансових транзакцій;
- дотримання суворих регуляторних вимог (*PCI DSS, GDPR*);
- зростання кількості онлайн-сервісів та мобільних додатків;

Типові напрямки впровадження:

- мікросегментація: ізоляція критичних систем обробки платежів, баз даних клієнтів, торгових платформ;
- посилена автентифікація: широке використання *mfa* для клієнтів та співробітників, особливо для доступу до чутливих систем;
- захист даних: шифрування, токенізація, *dlp*-системи;
- моніторинг транзакцій та виявлення шахрайства: аналітика для виявлення підозрілої активності в реальному часі;

~ безпека *api*: захист *api,* що використовуються для взаємодії з фінтех-партнерами та мобільними додатками;

Інтеграція з успадкованими (*legacy*) системами, забезпечення відповідності численним регуляціям, управління великою кількістю користувачів та транзакцій. Загальні патерни та етапи впровадження, які незалежно від галузі, компанії часто проходять схожі етапи на шляху до *Zero Trust,* які наведені у таблиці 2.1.

Таблиця 2.1 - Фази впровадження *Zero Trust* та ключові активності

Фаза Впровадження	Ключові Активності
1. Визначення та планування	Ідентифікація критичних активів (*protect surface*), аналіз ризиків, розробка стратегії та дорожньої карти *ZT*.
2. Пілотні проекти	Впровадження *ZT* для обмеженої групи користувачів або окремих критичних додатків/систем. Збір досвіду.
3. Розширення	Поступове розгортання *ZT* на інші частини організації: ідентичності, пристрої, мережі, додатки, дані.
4. Оптимізація	Налаштування політик, інтеграція інструментів, автоматизація процесів, впровадження розширеної аналітики.
5. Безперервне вдосконалення	Регулярний перегляд та оновлення архітектури *ZT* відповідно до змін у ландшафті загроз та бізнес-потребах.

Ці приклади демонструють, що *Zero Trust* – це не теоретична концепція, а практична стратегія, яка вже допомагає компаніям підвищувати рівень своєї кіберстійкості. Ключ до успіху полягає в комплексному підході, підтримці з боку керівництва та готовності до поступових змін.

2.5 Порівняння *Zero Trust* із традиційними моделями безпеки

Як було детально розглянуто в Розділі 1, традиційні моделі безпеки, такі як «Замок і Рів» (*Perimeter Security Model*) та «Захист у глибину» (*Defense in Depth*), відігравали важливу роль протягом багатьох років. Однак, в умовах сучасного ландшафту загроз та трансформації ІТ-середовищ, їхні обмеження стають все більш очевидними. Модель *Zero Trust* пропонує кардинально інший підхід, заснований на принципі «ніколи не довіряй, завжди перевіряй».

Давайте проведемо детальне порівняння цих підходів за ключовими аспектами.

1. Основне припущення про довіру:

Відкидає поняття довіреної мережі. Жоден користувач, пристрій чи мережевий потік не вважається довіреним за замовчуванням, незалежно від його місцезнаходження. Гасло: «Ніколи не довіряй, завжди перевіряй».

2. Фокус захисту:

Фокус зміщується з захисту мережевого периметра на захист конкретних ресурсів (дані, додатки, активи, сервіси – так звана «поверхня захисту» або «*protect surface*»). Ідентичність стає новим периметром.

3. Контроль доступу:

Реалізує гранулярний контроль доступу на основі принципу найменших привілеїв до кожного окремого ресурсу. Доступ надається тільки до тих ресурсів, які необхідні для виконання конкретного завдання, і тільки на необхідний час (*JIT*/*JEA*).

4. Мережева сегментація:

Пропагує мікросегментацію – створення невеликих, ізольованих зон безпеки навколо окремих додатків, робочих навантажень або навіть окремих серверів. Це значно обмежує можливість горизонтального переміщення зловмисників.

5. Перевірка та автентифікація:

Вимагає постійної, явної перевірки для кожного запиту на доступ до ресурсу. Використовує багатофакторну автентифікацію (*MFA*) та динамічну оцінку ризиків на основі.

6. Припущення про загрози:

Працює за принципом «припущення про компрометацію» (*assume breach*) – тобто виходить з того, що зловмисник вже може бути всередині мережі або неминуче туди потрапить.

7. Реакція на мобільність, хмари, *IoT*:

За своєю суттю розроблена для гетерогенних середовищ. Оскільки довіра не прив'язана до місцезнаходження, модель однаково добре застосовується до локальних, хмарних та гібридних інфраструктур, а також до мобільних пристроїв та *IoT*.

8. Видимість та аналітика трафіку:

Вимагає всебічного моніторингу та інспекції всього трафіку, включаючи внутрішній. Активно використовуються інструменти аналітики (*SIEM, UEBA*) для виявлення аномалій та загроз у реальному часі.

Таблиця 2.2 - Порівняльна таблиця традиційних моделей безпеки та *Zero Trust*

Характеристика	Традиційна модель («Замок і Рів»)	Модель «Захист у глибину»	Модель *Zero Trust*
Припущення про довіру	«Довірена» внутрішня мережа	Багато рівнів, але всередині сегментів може бути довіра	Немає довіри за замовчуванням
Фокус захисту	Захист периметра	Кілька рівнів захисту (периметр, мережа, хости, дані)	Захист ресурсів (дані, додатки, активи, сервіси)
Контроль доступу	Широкий доступ всередині периметра	Політики доступу на кожному рівні, але можлива надлишковість	Гранульований, на основі потреби, принцип найменших привілеїв
Мережева сегментація	Макросегментація (*DMZ, VLAN*)	Можлива детальніша сегментація	Мікросегментація
Перевірка / Автентифікація	На вході в периметр	Перевірки на різних рівнях	Постійна, для кожного запиту, *MFA* повсюдно
Горизонтальне переміщення	Високий ризик, якщо периметр подолано	Зменшений, але можливий всередині сегментів	Значно обмежене мікросегментацією
Інсайдерські загрози	Слабкий захист	Кращий захист, але залежить від реалізації	Більш ефективне виявлення та стримування
Підтримка мобільності/хмар	Обмежена, ускладнена	Адаптується, але може бути складною	Вбудована концептуально, не залежить від місцезнаходження
Реагування на компрометацію	Фокус на запобіганні, повільне реагування всередині	Виявлення на різних етапах	«Припущення про компрометацію», швидке стримування

Переваги *Zero Trust* над традиційними моделями:

1. Покращений захист від сучасних загроз.

2. Зменшення поверхні атаки.

3. Краща видимість та контроль.

4. Підтримка сучасних IT-середовищ.

5. Спрощення відповідності регуляторним вимогам.

6. Підвищена гнучкість та масштабованість бізнесу.

Незважаючи на очевидні переваги, перехід на *Zero Trust* є складним та тривалим процесом, що вимагає значних зусиль, інвестицій та зміни корпоративної культури. Однак, з огляду на обмеження традиційних підходів та невпинну еволюцію кіберзагроз, *Zero Trust* стає необхідною стратегією для забезпечення стійкості та безпеки сучасних організацій (див. рисунок 2.5).

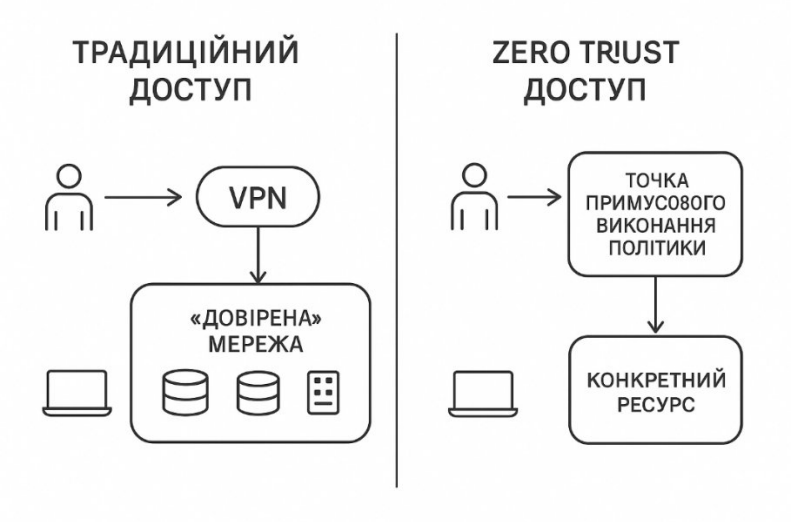

Рисунок 2.5 - Візуальне порівняння підходів до доступу

2.6 Висновок до розділу 2

У даному розділі було всебічно розглянуто концепцію *Zero Trust,* яка є сучасною парадигмою забезпечення кібербезпеки, що кардинально змінює підходи до захисту інформаційних активів в корпоративних середовищах.

По-перше, ми простежили виникнення та розвиток концепції *Zero Trust,* починаючи від усвідомлення обмежень традиційних периметральних моделей і ранніх ідей деперіметризації, до формалізації моделі Джоном Кіндервагом та її подальшої еволюції під впливом практичних реалізацій, таких як *Google BeyondCorp,* і стандартизаційних зусиль з боку *NIST* та інших організацій.

По-друге, детально проаналізовано основні принципи моделі *Zero Trust*. Центральним є гасло «ніколи не довіряй, завжди перевіряй», яке доповнюється такими ключовими положеннями, як припущення про компрометацію, явна перевірка на основі багатьох сигналів, застосування принципу найменших привілеїв, впровадження мікросегментації, повсюдне використання багатофакторної автентифікації, а також безперервний моніторинг, аналітика та автоматизація. Ці принципи формують основу для побудови стійкої та адаптивної архітектури безпеки.

По-третє, було розглянуто сфери застосування концепції в корпоративних середовищах. Особливу увагу приділено важливості видимості, аналітики та автоматизації для ефективного функціонування моделі.

По-четверте, наведено приклади впровадження *Zero Trust* у сучасних компаніях, таких як *Google* (*BeyondCorp*) та *Microsoft,* а також узагальнено підходи для фінансового сектору. Ці приклади демонструють практичну реалізацію та переваги *Zero Trust,* а також підкреслюють, що її впровадження є поетапним процесом, що вимагає стратегічного планування.

По-п'яте, проведено детальне порівняння *Zero Trust* із традиційними моделями безпеки, такими як «Замок і Рів» та «Захист у глибину». Було чітко окреслено фундаментальні відмінності в підходах до довіри, фокусу захисту, контролю доступу, сегментації та реагування на сучасні виклики. Це порівняння переконливо демонструє переваги *Zero Trust* у протистоянні актуальним кіберзагрозам та підтримці динамічних бізнес-середовищ.

Таким чином, концепція *Zero Trust* представляє собою не просто набір технологій, а стратегічну зміну філософії безпеки. Розуміння принципів, архітектури та переваг *Zero Trust,* викладених у цьому розділі, створює необхідне підґрунтя для переходу до практичних аспектів розробки та реалізації такої моделі в корпоративній мережі, що буде детально розглянуто в наступних розділах роботи.

РОЗДІЛ 3
РЕАЛІЗАЦІЯ КОНЦЕПЦІЇ *ZERO TRUST* У ТЕСТОВОМУ СЕРЕДОВИЩІ

3.1 Вибір і опис тестового обладнання та ПЗ

Цей розділ присвячений практичній реалізації та валідації моделі *Zero Trust,* розробленої в попередніх розділах. Він охоплює детальний опис тестового середовища, конфігурацію ключових компонентів, імплементацію політик довіри та безпеки, а також методологію проведення експериментів і аналізу їхніх результатів. Метою даного розділу є демонстрація функціональності та ефективності підходу *Zero Trust* у контрольованому лабораторному середовищі, що дозволить підтвердити його застосовність для корпоративних мереж.

Основою тестового стенда є мережеве обладнання та кінцеві пристрої, що імітують робочі станції та мобільні пристрої користувачів.

Як центральний елемент мережі обрано *TP-Link WR*940*N*. Цей маршрутизатор є поширеним бюджетним рішенням, що підтримує встановлення кастомних прошивок, зокрема *OpenWRT*. Його використання дозволяє отримати повний контроль над мережевими функціями, такими як *VLAN, ACL* та маршрутизація, що є критично важливим для реалізації сегментації та політик доступу *Zero Trust* (рисунок 3.1)

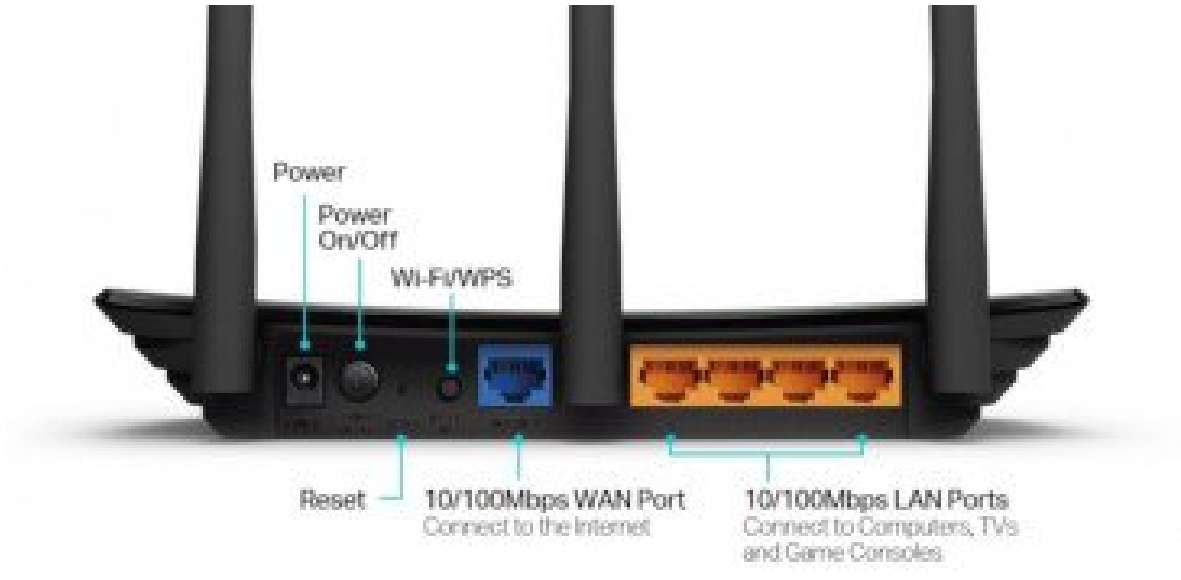

Рисунок 3.1 - Маршрутизатор *TP-Link WR*940*N*

Для імітації різноманітності кінцевих точок, характерної для корпоративного середовища, використовуються:

- персональний комп'ютер/ноутбук з ОС *Windows* 10/11: представляє типову робочу станцію офісного працівника;
- віртуальна машина або фізичний комп'ютер з ОС *Linux* (*Ubuntu Desktop*): Імітує робочу станцію розробника або адміністратора, яка часто використовується в IT-відділах;
- смартфон/планшет з ОС *Android*: представляє мобільний пристрій, що використовується для доступу до корпоративних ресурсів поза офісом (рисунок 3.2);

Рисунок 3.2 - Схема тестового стенда

Програмне забезпечення відіграє ключову роль у реалізації принципів *Zero Trust,* забезпечуючи ідентифікацію, авторизацію, сегментацію та моніторинг.

1. Операційна система для маршрутизатора:

- *OpenWRT* – це вбудована операційна система на базі *Linux,* яка є відкритою та повністю кастомізованою. Вибір *OpenWRT* для маршрутизатора *TP-Link WR940N* обумовлений її розширеними мережевими можливостями, включаючи підтримку *VLAN,* гнучкі налаштування файрволу (*iptables*), підтримку *VPN*-протоколів та можливість встановлення додаткових пакетів для моніторингу та управління. *OpenWRT* дозволяє перетворити споживчий маршрутизатор на по-

тужний мережевий шлюз з функціоналом, наближеним до професійного обладнання (рисунок 3.3).

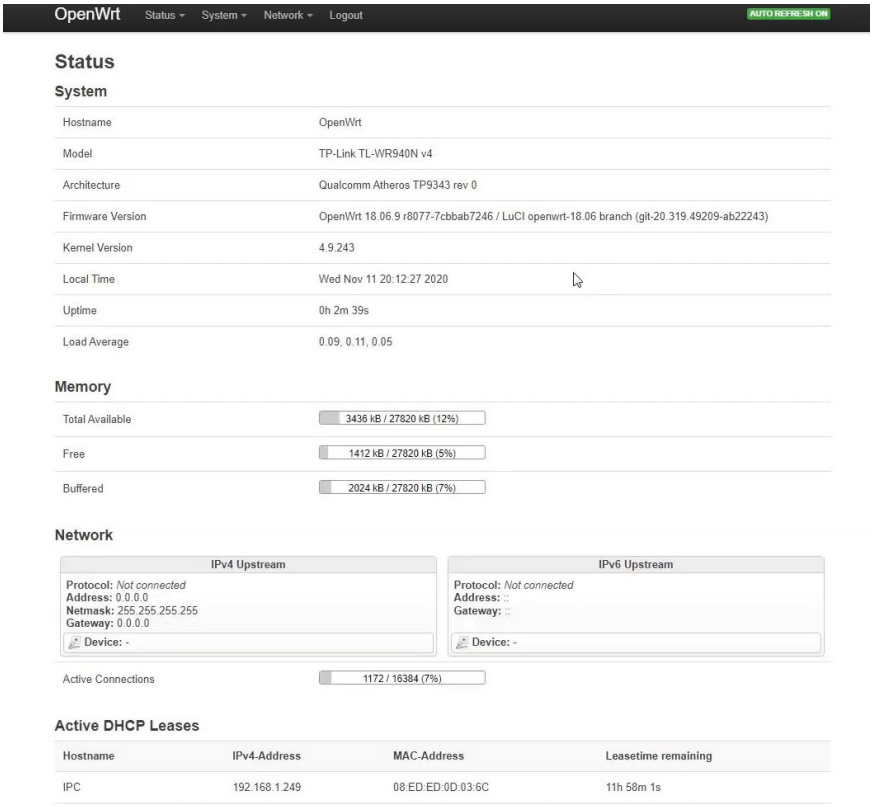

Рисунок 3.3 - Скріншот веб-інтерфейсу *OpenWRT*

2. *Zero Trust VPN* сервіс:

˜ *Tailscale* – це сервіс обрано як ключовий компонент для реалізації *Zero Trust VPN. Tailscale* базується на протоколі *WireGuard* і спрощує побудову *mesh*-мереж, забезпечуючи безпечне та пряме з'єднання між усіма пристроями, незалежно від їхнього місцезнаходження. Він автоматично обробляє *NAT*-траверсинг та роумінг, що робить його ідеальним для сучасних розподілених корпоративних середовищ;

3. Операційні системи для клієнтських пристроїв:

˜ *Windows* 10/11 – це популярна ОС для робочих станцій, що вимагає налаштування клієнта *Tailscale* та відповідних політик безпеки;

˜ *Ubuntu Desktop,* вимагає встановлення та конфігурації клієнта *Tailscale,* а також перевірки взаємодії з мережевими сервісами;

˜ *Android* – це мобільна ОС, що дозволяє протестувати доступ з мобільних пристроїв та інтеграцію *Tailscale* у мобільне середовище;

4. Допоміжне програмне забезпечення:

- термінал/*SSH*-клієнт (*PuTTY, OpenSSH*) – для віддаленого доступу та конфігурації маршрутизатора *OpenWRT*;
- веб-браузер – для доступу до веб-інтерфейсів *OpenWRT* та *Tailscale*;
- інструменти мережевого аналізу (*Wireshark, nmap*) – це для моніторингу трафіку, сканування портів та верифікації реалізованих політик безпеки (рисунок 3.4);

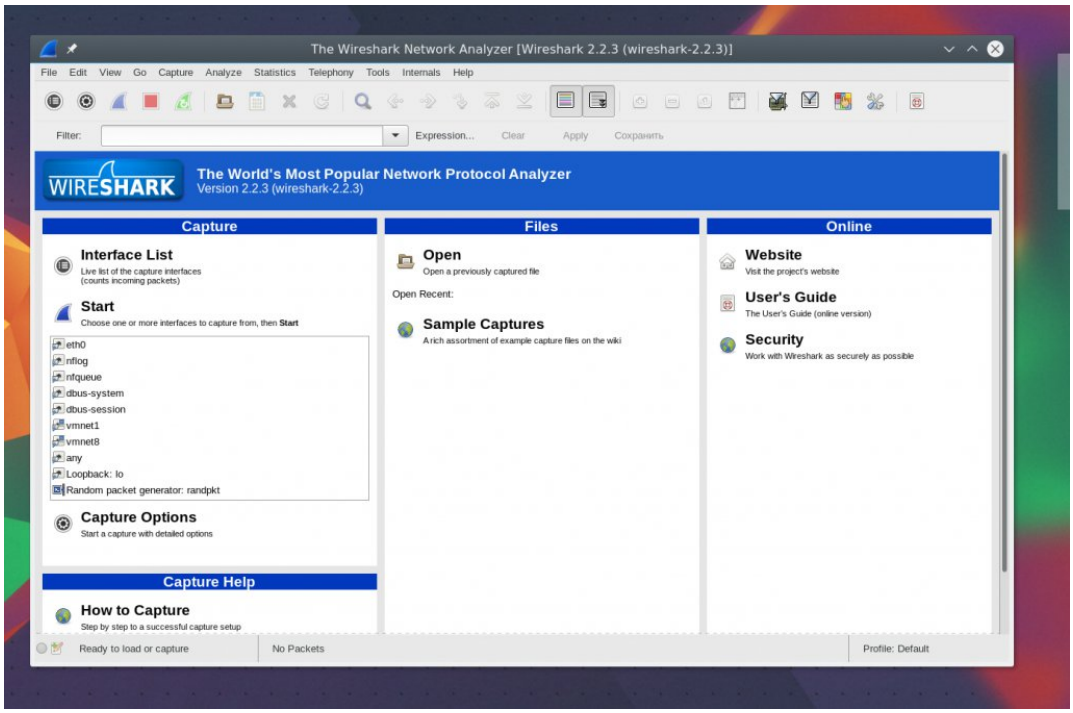

Рисунок 3.4 - Скріншот інтерфейсу *Wireshark*

Вибір даного комплексу апаратного та програмного забезпечення базується на кількох ключових критеріях:

1. Доступність та економічність. Використання поширеного споживчого маршрутизатора та безкоштовного або недорогого програмного забезпечення робить тестове середовище економічно вигідним та легким для відтворення.

2. Гнучкість та кастомізація. *OpenWRT* та *Tailscale* надають широкі можливості для тонкого налаштування мережевих параметрів, що дозволяє експериментувати з різними аспектами архітектури *Zero Trust*.

3. Релевантність до корпоративного середовища. Обрані компоненти відображають типові технології, що використовуються в сучасних корпоративних

мережах (*VPN,* різні ОС, мережева сегментація), що забезпечує практичну цінність отриманих результатів.

4. Спрощення розгортання *Zero Trust*. *Tailscale* суттєво спрощує процес розгортання *Zero Trust VPN,* дозволяючи зосередитися на логіці політик, а не на складнощах налаштування мережевої інфраструктури.

3.2 Підготовка маршрутизатора *TP-Link WR*940*N* з прошивкою *OpenWRT*

Підготовка маршрутизатора *TP-Link WR*940*N* до роботи як ключового елемента *Zero Trust* мережі є критично важливим кроком. Це включає встановлення альтернативної прошивки *OpenWRT* та базову конфігурацію, яка забезпечить необхідні мережеві можливості.

OpenWRT трансформує стандартний споживчий маршрутизатор у потужний інструмент мережевого управління. Його архітектура, заснована на *Linux,* надає повний контроль над мережевими протоколами та сервісами. Для концепції *Zero Trust* особливо цінними є такі можливості:

1. Розширений фаєрвол (*iptables*). Дозволяє створювати деталізовані правила фільтрації трафіку на основі джерела, призначення, порту, протоколу та навіть стану з'єднання. Це є основою для реалізації політик «найменших привілеїв» та мікросегментації.

2. Підтримка *VLAN*. Можливість створення віртуальних локальних мереж дозволяє логічно розділити пристрої та сервіси на ізольовані сегменти, навіть якщо вони підключені до одного фізичного порту. Це ключовий елемент для реалізації мережевої сегментації, що є фундаментальним принципом *Zero Trust*.

3. *VPN*-сервер/клієнт. *OpenWRT* підтримує широкий спектр *VPN*-протоколів (*OpenVPN, WireGuard*), що дозволяє інтегрувати маршрутизатор у загальну *Zero Trust VPN*-архітектуру або використовувати його як шлюз для віддаленого доступу.

4. *DNS*-сервер та *DNS*-фільтрація. Можливість налаштування локального *DNS*-сервера та використання таких інструментів, як *AdGuard Home* або *Dnsmasq,* дозволяє контролювати доступ до доменів та фільтрувати небажаний трафік.

5. Моніторинг та логування. *OpenWRT* надає засоби для збору та аналізу мережевих подій, що є необхідним для виявлення аномалій та забезпечення безперервної верифікації.

Встановлення *OpenWRT* на *TP-Link WR*940*N* вимагає дотримання певної послідовності кроків, щоб уникнути пошкодження пристрою.

1. Перевірка сумісності та завантаження прошивки:

- необхідно перевірити точну апаратну версію маршрутизатора (*WR*940*N v*4, *v*6 тощо), оскільки для кожної версії може бути своя унікальна прошивка. Ця інформація зазвичай вказана на етикетці знизу маршрутизатора;
- завантажити відповідну стабільну версію прошивки *OpenWRT* (*.bin* файл) з офіційного сайту *OpenWRT* (*openwrt.org*). Важливо завантажити версію «*factory*» для первинного встановлення з рідної прошивки маршрутизатора (таблиця 3.1);

Таблиця 3.1 - Приклад таблиці сумісності *TP-Link WR*940*N* з файлами прошивки *OpenWRT*

Версія апаратного забезпечення	Підтримувана версія *OpenWrt*	Файл прошивки (*Factory*)	Файл прошивки (*Sysupgrade*)	Метод встановлення	Коментарі
*TL-WR*940*N v*1	10.03–18.06.9	*openwrt-18.06.9-ar71xx-tiny-tl-wr941nd-v5-squashfs-factory.bin*	*openwrt-18.06.9-ar71xx-tiny-tl-wr941nd-v5-squashfs-sysupgrade.bin*	*GUI OEM, U-Boot TFTP recovery*	Сумісний із прошивками для *TL-WR*941*ND v*5.
*TL-WR*940*N v*2	10.03–18.06.9	*openwrt-18.06.9-ar71xx-tiny-tl-wr941nd-v5-bin*	*openwrt-18.06.9-ar71xx-tiny-tl-wr941nd-v5-squashfs-sysupgrade.bin*	*GUI OEM, U-Boot TFTP recovery*	Сумісний із прошивками для *TL-WR*941*ND v*5.

Продовження таблиці 3.1

*TL-WR*940*N v*3	10.03–18.06.9	*openwrt-18.06.9-ar*71*xx-tiny-tl-wr*941*nd-v*6*-squashfs-factory.bin*	*openwrt-18.06.9-ar*71*xx-tiny-tl-wr*941*nd-v*6*-squashfs-sysupgrade.bin*	*GUI OEM, U-Boot TFTP recovery*	Сумісний із прошивками для *TL-WR*941*ND v*6.
*TL-WR*940*N v*4	18.06.9	*openwrt-18.06.9-ar*71*xx-tiny-tl-wr*940*n-v*4*-squashfs-factory.bin*	*openwrt-18.06.9-ar*71*xx-tiny-tl-wr*940*n-v*4*-squashfs-sysupgrade.bin*	*GUI OEM, U-Boot TFTP recovery*	Для *TFTP* перейменуйте *factory*-прошивку в *wr*940*nv*4*_tp_recovery.bin*.
*TL-WR*940*N v*6	18.06.8–18.06.9	*openwrt-18.06.9-ar*71*xx-tiny-tl-wr*940*n-v*6*-squashfs-factory.bin*	*openwrt-18.06.9-ar*71*xx-tiny-tl-wr*940*n-v*6*-squashfs-sysupgrade.bin*	*GUI OEM, U-Boot TFTP recovery*	Обмежена підтримка через низький обсяг пам’яті.

2. Підготовка маршрутизатора:

- підключити маршрутизатор до джерела живлення;
- з'єднати комп'ютер з одним з *LAN*-портів маршрутизатора за допомогою *Ethernet*-кабелю. Переконатися, що на комп'ютері встановлено статичну *IP*-адресу з того ж діапазону, що і *IP*-адреса маршрутизатора за замовчуванням (зазвичай 192.168.0.1 або 192.168.1.1).

3. Оновлення прошивки через веб-інтерфейс (або *TFTP*):

- відкрити веб-браузер та перейти за *IP*-адресою маршрутизатора за замовчуванням;
- увійти в панель управління (логін/пароль за замовчуванням зазвичай *admin*/*admin*);

˜ знайти розділ «Оновлення прошивки» (*Firmware Upgrade*/*System Tools -> Firmware Upgrade*);

˜ вибрати завантажений файл прошивки *OpenWRT* та розпочати оновлення;

˜ важливо: не вимикати маршрутизатор і не відключати мережевий кабель під час процесу прошивки. Це може призвести до «цегляної» (*bricked*) пристрою;

4. Перший запуск *OpenWRT*:

˜ після успішного оновлення маршрутизатор перезавантажиться. Його *IP*-адреса за замовчуванням в *OpenWRT* зазвичай змінюється на 192.168.1.1;

˜ знову підключитися до маршрутизатора через веб-браузер (*LuCI*-інтерфейс) або за допомогою *SSH*-клієнта (рисунок 3.5).

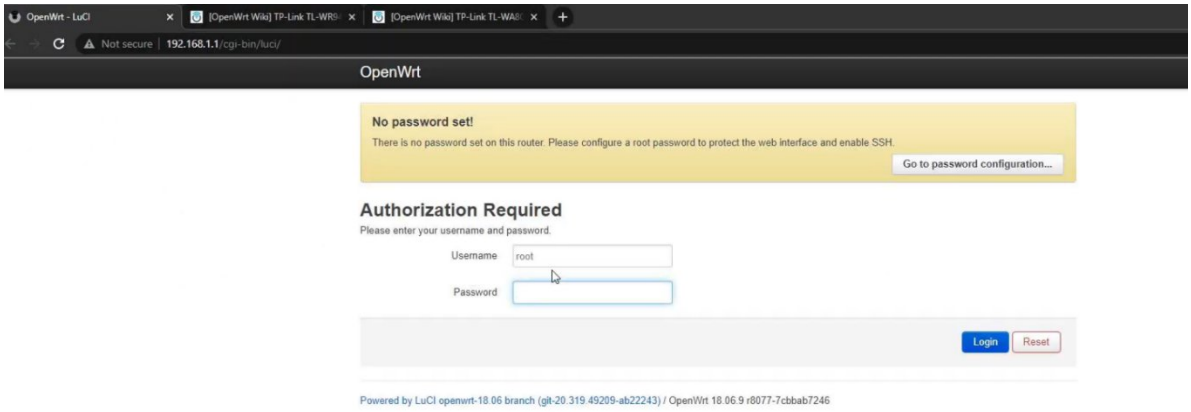

Рисунок 3.5 - Скріншот початкового екрану входу в *LuCI*-інтерфейс *OpenWRT* після першого запуску

Після встановлення *OpenWRT* необхідно виконати базові налаштування для забезпечення стабільної роботи та підготовки до подальших кроків.

1. Зміна пароля *root*. Першим і найважливішим кроком є встановлення надійного пароля для облікового запису *root* (адміністратора) через веб-інтерфейс або *SSH*.

2. Налаштування *WAN*-інтерфейсу. Конфігурація підключення до Інтернету (*DHCP*-клієнт, статична *IP*-адреса, *PPPoE* – залежно від типу підключення провайдера).

3. Налаштування *LAN*-інтерфейсу та *DHCP*-сервера. Визначення *IP*-адресного діапазону для локальної мережі та налаштування *DHCP*-сервера для автоматичної видачі *IP*-адрес клієнтам. Рекомендується використовувати інший *IP*-діапазон, ніж 192.168.1.1/24, щоб уникнути конфліктів при підключенні до інших мереж.

4. Оновлення пакетів. Виконати *opkg update* та *opkg upgrade* через *SSH* для оновлення списку доступних пакетів та встановлених компонентів.

5. Встановлення необхідних пакетів. Залежно від подальших планів, можуть знадобитися додаткові пакети, такі як *nano* (текстовий редактор), *htop* (моніторинг ресурсів), *tcpdump* (аналіз трафіку) тощо.

6. Налаштування брандмауера за замовчуванням. Переконатися, що стандартні правила брандмауера *OpenWRT* правильно налаштовані, дозволяючи вихідний трафік та блокуючи небажані вхідні з'єднання(рисунок 3.6).

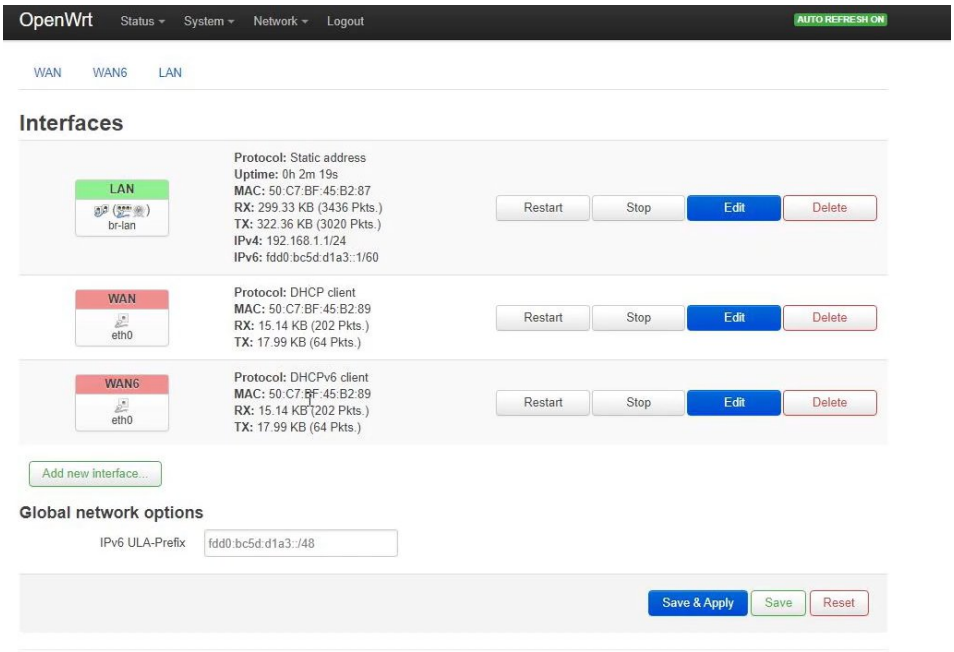

Рисунок 3.6 - Скріншот сторінки «*Interfaces*» в *LuCI*-інтерфейсі *OpenWRT*

Ці кроки забезпечують функціональну основу для подальшої реалізації концепції *Zero Trust,* дозволяючи перейти до інтеграції сервісів та налаштування деталізованих політик.

3.3 Ознайомлення з сервісом *Tailscale* як *Zero Trust VPN*

Tailscale є одним з провідних рішень для реалізації концепції *Zero Trust* у контексті віртуальних приватних мереж. Він відрізняється від традиційних *VPN*-рішень своєю архітектурою та підходом до безпеки, що робить його ідеальним інструментом для сучасних розподілених корпоративних середовищ.

Tailscale базується на протоколі *WireGuard* – сучасному, швидкому та безпечному *VPN*-протоколі. Однак, *Tailscale* не є просто обгорткою над *WireGuard*; він значно розширює його функціональність, спрощуючи розгортання та управління.

Основними принципами роботи *Tailscale* є:

1. *Peer-to-peer* (*P*2*P*) з'єднання. На відміну від традиційних централізованих *VPN*-серверів, *Tailscale* створює зашифровані *P*2*P*-з'єднання між усіма пристроями у вашій мережі (*tailnet*). Це означає, що трафік між двома пристроями йде безпосередньо від одного до іншого, минаючи центральний сервер *Tailscale* (за винятком випадків, коли пряме *P*2*P*-з'єднання неможливе через *NAT,* тоді використовується релейний вузол *DERP*).

2. *Zero Trust* підхід за замовчуванням. *Tailscale* реалізує принципи *Zero Trust,* «ніколи не довіряти, завжди перевіряти». Кожен пристрій та користувач у *tailnet* автентифікуються та авторизуються для кожного окремого з'єднання. Доступ до ресурсів надається лише після успішної перевірки ідентичності та відповідності політикам.

3. Інтеграція з провайдерами ідентичності (*IdP*). *Tailscale* інтегрується з популярними *IdP,* такими як *Google Workspace, Microsoft Entra ID* (*Azure AD*), *Okta, Auth*0 тощо. Це дозволяє використовувати вже існуючі облікові записи користувачів для аутентифікації, спрощуючи управління доступом та забезпечуючи централізоване управління ідентичністю.

4. Автоматичне управління ключами та *IP*-адресами. *Tailscale* автоматично генерує та розподіляє криптографічні ключі для *WireGuard,* а також призначає *IP*-адреси з приватного діапазону (100.*x*.*y*.*z*/8) кожному пристрою. Це значно спрощує конфігурацію та усуває необхідність ручного налаштування *IPsec* або *OpenVPN*.

5. *NAT Traversal* та *DERP*-сервери. Для подолання проблем з *NAT* (*Network Address Translation*) та файрволами, *Tailscale* використовує релейні сервери *DERP* (*Designated Encrypted Relay for Packets*). Якщо пряме *P*2*P*-з'єднання неможливе, трафік маршрутизується через найближчий *DERP*-сервер, забезпечуючи зв'язок між пристроями. Однак весь трафік залишається зашифрованим від кінця до кінця.

Ключові особливості *Tailscale* для реалізації *Zero Trust*:

1. Ідентичність на основі користувачів та пристроїв. Замість традиційних *IP*-адрес, *Tailscale* використовує ідентифікатори користувачів та пристроїв, що робить політики доступу більш гранульованими та орієнтованими на особистість, а не на місцезнаходження в мережі.

2. Політики доступу (*ACLs*). *Tailscale* дозволяє визначити деталізовані політики контролю доступу (*Access Control Lists*) у форматі *JSON*. Ці політики визначають, які користувачі (або групи користувачів) можуть підключатися до яких пристроїв або сервісів у мережі. Це дозволяє реалізувати принцип «найменших привілеїв», надаючи доступ лише до необхідних ресурсів (таблиця 3.2).

Таблиця 3.2 - Приклад фрагмента *ACL*-файлу *Tailscale,* що показує правила доступу для різних груп користувачів до певних сервісів

Група користувачів	Ресурс/Сервіс	Дозволені дії	*IP*/Підмережа	Порт	Опис
group:*admins*	Веб-сервер	*accept*	100.64.0.10	80,443	Доступ до адмін-панелі веб-сервера
group:*developers*	*Dev*-сервер	*accept*	100.64.0.20	22	*SSH*-доступ для розробників
group:*guests*	Файловий сервер	*accept*	100.64.0.30	445	Доступ до загальних файлів
group:*guests*	Веб-сервер	*deny*	100.64.0.10	80,443	Заборона доступу до веб-сервера
group:*admins*	База даних	*accept*	100.64.0.40	5432	Доступ до *PostgreSQL* для адміністраторів
group:*developers*	База даних	*accept*	100.64.0.40	5432	Читання/запис для розробників
group:*everyone*	Внутрішній чат	*accept*	100.64.0.50	8080	Доступ до чату для всіх користувачів

3. *Subnet Routers* (Маршрутизатори підмереж). *Tailscale* дозволяє використовувати один пристрій у вашій *tailnet* як маршрутизатор підмереж. Це дозволяє пристроям у *Tailscale*-мережі безпечно отримувати доступ до ресурсів у фізичних локальних підмережах, які не є частиною *Tailscale*-мережі, без необхідності встановлення *Tailscale*-клієнта на кожен пристрій у цій підмережі. Це ідеально підходить для доступу до серверів, *NAS* або інших пристроїв, які не можуть запустити клієнт *Tailscale*.

4. *Funnel* та *Tailscale SSH*. Додаткові функції, такі як *Funnel* (публікація сервісів *Tailscale* у зовнішній Інтернет через захищений тунель) та *Tailscale SSH* (безпарольний доступ *SSH* через *Tailscale*), ще більше розширюють можливості безпечного доступу.

5. Логування та аудит. *Tailscale* надає можливості логування з'єднань та подій, що є критично важливим для моніторингу безпеки, виявлення аномалій та відповідності регуляторним вимогам.

У таблиці 3.3 наведено порівняння *Tailscale* (*Zero Trust VPN*) з традиційними *VPN*-рішеннями.

Таблиця 3.3 – Порівняльний аналіз моделей

Характеристика	Традиційний *VPN* (*IPsec*/*OpenVPN*)	*Tailscale* (*Zero Trust VPN*)
Архітектура	«*Hub-and-spoke*» (централізований сервер)	«*Mesh*» (*P2P* з'єднання)
Довіра	Довіра до мережі після підключення до *VPN*-сервера	«Нульова довіра» – кожен запит перевіряється
Доступ	Доступ до всієї мережі або широких сегментів після підключення	Гранульований доступ до окремих сервісів/пристроїв
Ідентифікація	Зазвичай за *IP*-адресою, рідше за користувачем	Завжди за ідентичністю користувача та пристрою
Складність налаштування	Висока (сертифікати, конфігурації фаєрволів, *NAT*)	Низька (автоматичне управління ключами, *IP*-адресами, *NAT*-траверсинг)
Масштабованість	Складна при зростанні кількості користувачів та віддалених офісів	Висока, легко додавати нові пристрої та користувачів
Безпека	Схильність до «бічного переміщення» після компрометації *VPN*-сервера	Обмеження «бічного переміщення» завдяки мікросегрануляції

Інтеграція *IdP*	Зазвичай вимагає додаткових налаштувань	Вбудована, спрощує *SSO* та управління ідентичністю

3.4 Налаштування *Windows, Linux, Android*-клієнтів

Налаштування клієнтів на різних операційних системах є ключовим етапом для інтеграції пристроїв у *Zero Trust* мережу, побудовану за допомогою *Tailscale*. Процес встановлення та конфігурації є відносно простим завдяки архітектурі *Tailscale,* але має свої особливості для кожної платформи.

Налаштування *Windows*-клієнта, починається з завантаження та встановлення клієнта на ПК (див. рисунок 3.6).

˜ відвідайте офіційний сайт *Tailscale* (*tailscale.com/download*) та завантажте інсталятор для *Windows*;

˜ запустіть інсталятор (*.exe* файл) та дотримуйтесь інструкцій. Процес встановлення є стандартним для *Windows*-додатків;

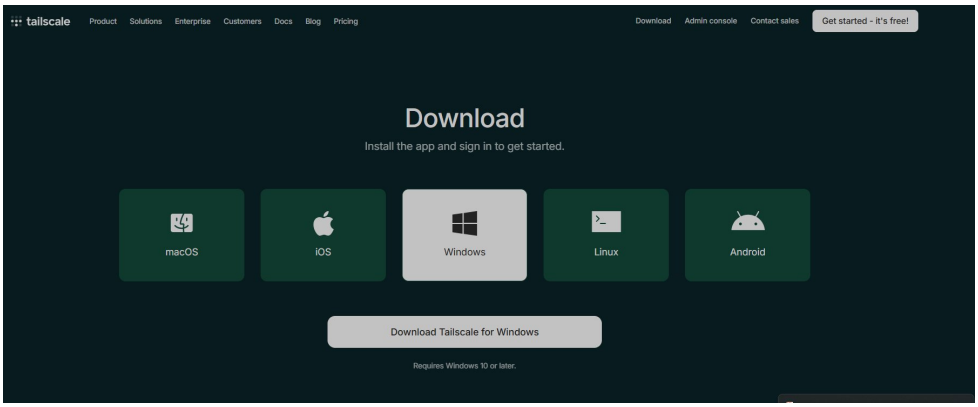

Рисунок 3.6 - Скріншот екрану завантаження *Tailscale* для *Windows*

2. Аутентифікація та підключення (рисунок 3.7):

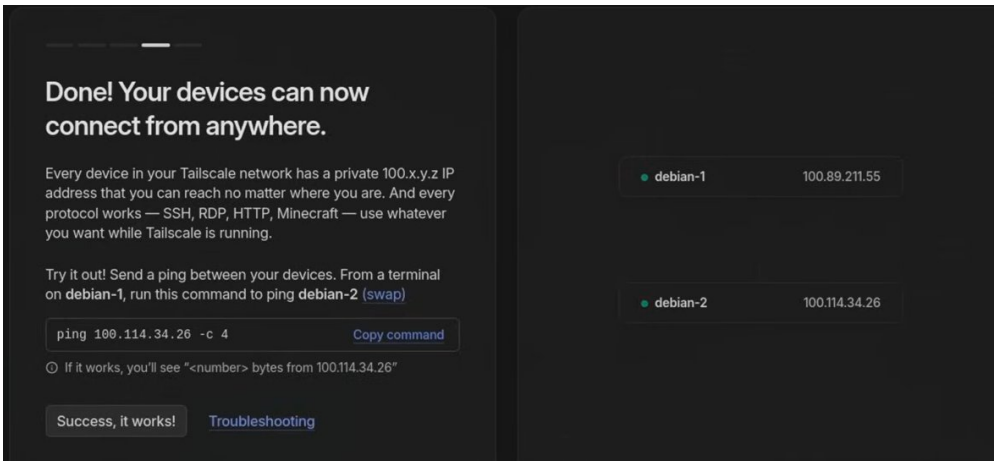

Рисунок 3.7 - Скріншот вікна браузера з вибором провайдера ідентичності для входу в *Tailscale*

˜ після встановлення, *Tailscale* автоматично запустить мініатюрний віконний додаток або з'явиться іконка в системному треї;

˜ клацніть на іконку *Tailscale* та виберіть «*Log in*» або «*Sign in*»;

˜ буде відкрито веб-браузер, який перенаправить вас на сторінку аутентифікації *Tailscale*. Виберіть свого провайдера ідентичності (*Google, Microsoft*) і увійдіть, використовуючи ваші облікові дані;

˜ після успішної аутентифікації, пристрій буде додано до вашої *Tailscale* мережі (*tailnet*).

3. Перевірка підключення та доступ до ресурсів (див. рисунок3.8):

˜ відкрийте інтерфейс *Tailscale* (з системного трея). Ви побачите список підключених пристроїв у вашій *tailnet,* включаючи власний пристрій та його *Tailscale IP*-адресу (100.*x.y.z*);

˜ спробуйте пінгувати інші пристрої в мережі *Tailscale* за їхніми *IP*-адресами або іменами хостів;

˜ перевірте доступ до спільних ресурсів, якщо вони доступні через *Tailscale*;

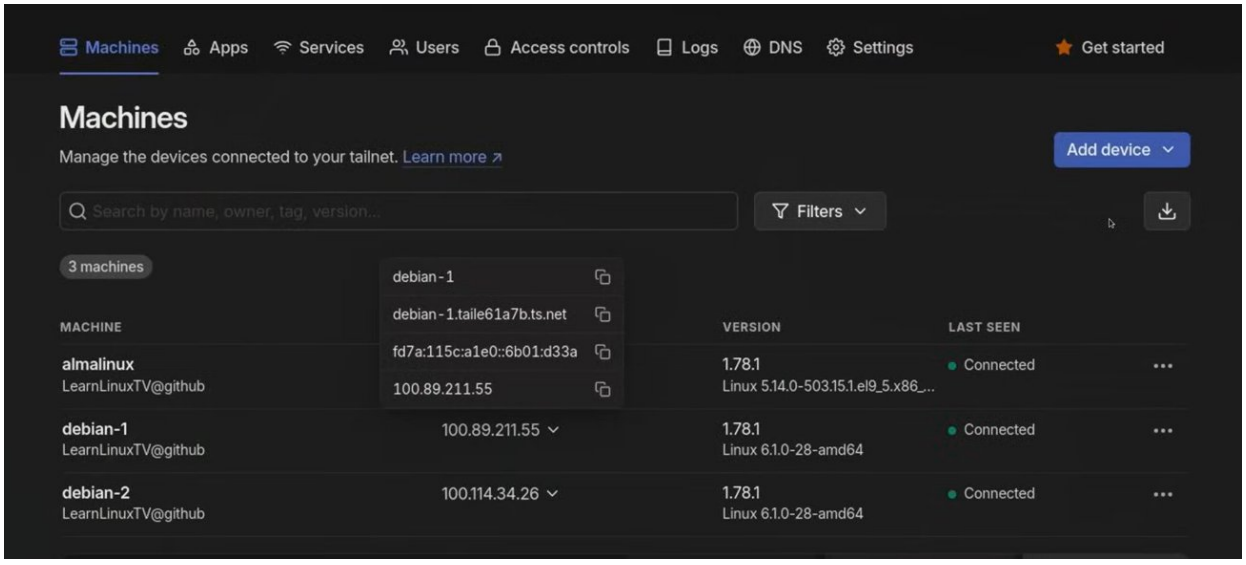

Рисунок 3.8 - Скріншот інтерфейсу *Tailscale* в *Windows,* що показує список підключених пристроїв та їхні *IP*-адреси

Налаштування *Tailscale* на *Linux* зазвичай виконується через термінал, хоча для деяких дистрибутивів можуть бути доступні і графічні інтерфейси (див. рисунок 3.9).

1. Встановлення *Tailscale*:

- відкрийте термінал;
- Виконайте команди для додавання репозиторію *Tailscale* та встановлення пакету. Приклад для *Debian*/*Ubuntu*:

Bash

curl -fsSL https://tailscale.com/install.sh | sh

sudo apt update

sudo apt install tailscale

Рисунок 3.9 - Скріншот терміналу *Linux,* що показує виконання команд встановлення *Tailscale*

2. Запуск та аутентифікація:

- запустіть сервіс *Tailscale*:

Bash

sudo systemctl enable --now tailscaled

˜ аутентифікуйте пристрій:

Bash

tailscale up

˜ ця команда виведе посилання в терміналі. Скопіюйте це посилання, вставте його в веб-браузер і виконайте аутентифікацію через обраного провайдера ідентичності, як це було зроблено для *Windows*;

3. Перевірка підключення (див. рисунок 3.10):

˜ перевірте статус *Tailscale*:

Bash

tailscale status

˜ ця команда покаже список підключених пристроїв та їхні *IP*-адреси *Tailscale*;

˜ спробуйте пінгувати інші пристрої в мережі *Tailscale*;

```
$ tailscale status
100.101.102.103   user-linux     linux      idle    -
100.64.10.5       phone-android  android    active  -
100.64.20.15      win-desktop    windows    active  -
```

Рисунок 3.10 - Скріншот терміналу *Linux,* що показує вивід команди *tailscale status*

Налаштування *Tailscale* на *Android* є інтуїтивно зрозумілим і виконується через мобільний додаток (рисунок 3.11).

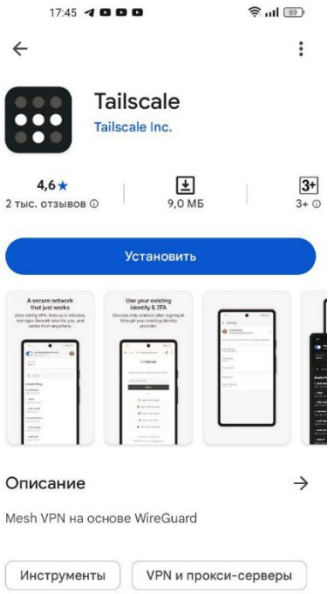

Рисунок 3.11 - Скріншот сторінки додатка *Tailscale* в *Google Play Store*

1. Завантаження та встановлення:

- відкрийте *Google Play Store* на вашому *Android*-пристрої;
- знайдіть додаток «*Tailscale*» та встановіть його;

2. Аутентифікація та підключення:

- відкрийте встановлений додаток *Tailscale*;
- натисніть кнопку «*Log in*» або «*Sign in*»;
- додаток перенаправить вас на сторінку аутентифікації у веб-браузері. Виберіть провайдера ідентичності та увійдіть;
- після успішної аутентифікації, додаток попросить дозволу на створення *VPN*-з'єднання. Надайте цей дозвіл.

3. Перевірка підключення та використання (див. рисунок 3.12):

- після підключення, додаток *Tailscale* покаже статус «*Connected*» та список пристроїв у вашій *tailnet*;
- тепер ваш *Android*-пристрій має доступ до інших пристроїв у *Tailscale* мережі, наприклад, ви можете відкрити веб-сторінку, що розміщена на *Linux*-сервері, використовуючи його *Tailscale IP*-адресу;

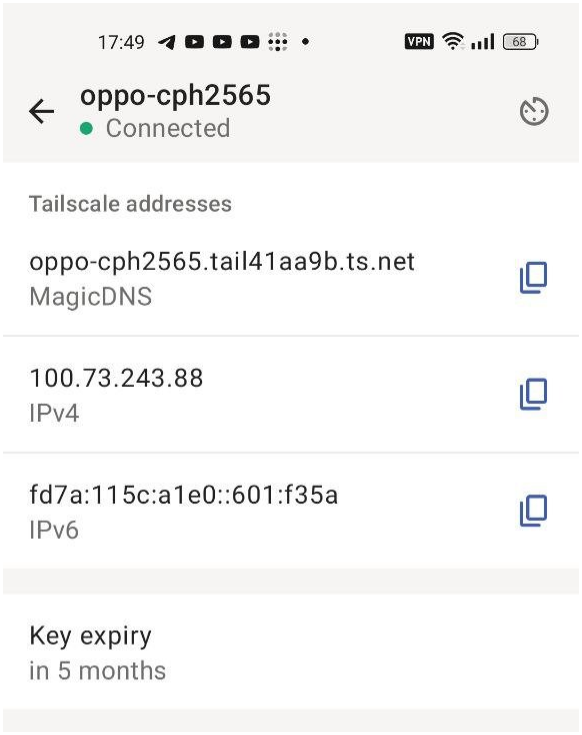

Рисунок 3.12 - Скріншот інтерфейсу *Android*-додатка *Tailscale,* що показує статус підключення та список пристроїв

Додаткові налаштування та рекомендації додатка.

Увімкніть функцію *MagicDNS* в панелі управління *Tailscale* (*admin console*). Це дозволить звертатися до пристроїв за їхніми іменами хостів, а не лише за *IP*-адресами, що значно підвищує зручність використання.

Subnet Routers. Якщо ви хочете, щоб пристрої в *Tailscale* могли отримувати доступ до вашої локальної мережі (наприклад, до принтера або *NAS,* які не мають клієнта *Tailscale*), налаштуйте один з пристроїв (наприклад, *Linux*-сервер або маршрутизатор *OpenWRT,* якщо він підтримує *Tailscale*) як *Subnet Router*. Це дозволить маршрутизувати трафік з *Tailscale* до вашої локальної мережі через цей пристрій.

Виключення з *VPN* (*Split Tunneling*). У деяких випадках може бути корисно налаштувати виключення з *VPN* (*Split Tunneling*), щоб лише трафік, призначений для *Tailscale* мережі, проходив через *VPN,* а весь інший трафік – безпосередньо в Інтернет. Це економить трафік і може покращити продуктивність для не-*Tailscale* ресурсів.

Оновлення клієнтів: Регулярно оновлюйте клієнтські програми *Tailscale* на всіх пристроях, щоб отримувати останні функції, виправлення помилок та оновлення безпеки.

Ці кроки забезпечують повне підключення всіх обраних клієнтських пристроїв до *Zero Trust* мережі *Tailscale,* що є фундаментом для подальшого застосування політик доступу та проведення експериментів.

3.5 Реалізація *VLAN, ACL,* та авторизаційних політик

Реалізація *Zero Trust* у тестовому середовищі вимагає імплементації ключових принципів: мікросегментації за допомогою *VLAN* та контролю доступу за допомогою *ACL,* а також визначення деталізованих авторизаційних політик. Ці елементи працюють у тандемі, забезпечуючи, що кожен запит на доступ до ресурсів проходить сувору перевірку.

Віртуальні локальні мережі (*VLAN*) дозволяють логічно розділити одну фізичну мережу на кілька ізольованих широкомовних доменів. Це фундаментальний крок у мікросегментації, що обмежує «бічне переміщення» зловмисника у випадку компрометації одного з сегментів.

1. Планування *VLAN*-сегментації:

˜ перед налаштуванням необхідно визначити, які групи пристроїв або сервісів будуть розміщені в окремих *VLAN*. Наприклад:

˜ *VLAN* 10 (Управління) - для адміністративного доступу до маршрутизатора та інших мережевих пристроїв;

˜ *VLAN* 20 (Користувачі) - для робочих станцій та мобільних пристроїв звичайних користувачів;

˜ *VLAN* 30 (Сервери/Ресурси) - для критично важливих сервісів або серверів, доступ до яких буде жорстко контролюватися (тестовий вебсервер, база даних);

˜ *VLAN* 40 (Гості) - для гостьових пристроїв з обмеженим доступом до Інтернету;

У таблиці 3.3 продемонстровано конфігурацію *VLAN*, яка відображає структуру сегментації мережі для забезпечення ефективного управління, безпеки та розподілу мережевих ресурсів між різними категоріями пристроїв і користувачів.

Таблиця 3.3 - Таблиця *VLAN*-ідентифікаторів, імен та асоційованих підмереж/призначень

VLAN ID	Ім'я *VLAN*	Підмережа (*CIDR*)	Призначення
10	*Management*	192.168.10.0/24	Управління мережевими пристроями
20	*Staff*	192.168.20.0/24	Робочі станції персоналу
30	*Guest*	192.168.30.0/24	Гостьова мережа
40	*Servers*	192.168.40.0/24	Серверне обладнання
50	*IoT*	192.168.50.0/24	*IoT*-пристрої
100	*Voice*	192.168.100.0/24	*VoIP*-телефонія

2. Налаштування *VLAN* у *OpenWRT*:

˜ доступ до інтерфейсу *OpenWRT* (*LuCI* або *SSH*): краще використовувати *SSH* для тонкого налаштування;

˜ конфігурація комутатора (*Switch*): *TP-Link WR*940*N* має вбудований мережевий комутатор. У *LuCI* перейдіть до «*Network*» -> «*Switch*». Тут ви можете призначити порти до різних *VLAN ID*. Кожен порт можна налаштувати як «*Tagged*» (для транкових портів, що передають трафік кількох *VLAN*) або «*Untagged*» (для кінцевих пристроїв у певній *VLAN*);

˜ створення нових інтерфейсів *VLAN*: після налаштування комутатора, створіть нові мережеві інтерфейси для кожної *VLAN*. Перейдіть до «*Network*» -> «*Interfaces*» та додайте новий інтерфейс, вибравши протокол «*Static address*» та вказавши відповідну *IP*-адресу підмережі та *VLAN ID* (наприклад, *eth*0.10 для *VLAN* 10);

˜ налаштування *DHCP*-серверів для кожної *VLAN*: для кожного нового інтерфейсу *VLAN* налаштуйте окремий *DHCP*-сервер, щоб пристрої в цій *VLAN* отримували *IP*-адреси зі свого діапазону;

Після сегментації мережі за допомогою *VLAN,* необхідно застосувати правила *ACL* на брандмауері *OpenWRT* для контролю трафіку між цими сегментами. Це забезпечить, що трафік між *VLAN* дозволений лише за принципом «найменших привілеїв».

1. Створення зон фаєрволу. В *OpenWRT* кожному мережевому інтерфейсу (включаючи інтерфейси *VLAN*) можна призначити окрему зону брандмауера («*Network*» -> «*Firewall*» -> «*Zones*»). Це дозволяє застосовувати політики до цілих зон, а не до окремих інтерфейсів.

2. Налаштування правил міжзонної взаємодії:

- за замовчуванням трафік між різними зонами блокується. Це ідеально відповідає принципу *Zero Trust*;
- дозволяйте лише необхідний трафік між зонами;
- кожне правило має бути якомога більш специфічним: вказувати вихідну та цільову зони, вихідний та цільовий *IP*-адреси/діапазони, протокол та номери портів;

Tailscale доповнює мережеву сегментацію на рівні маршрутизатора своїми власними *ACL,* які оперують на рівні ідентичностей користувачів та пристроїв, а не лише *IP*-адрес. Це реалізує контекстно-залежний доступ.

1. Доступ до панелі управління *Tailscale*: Увійдіть до адміністративної панелі *Tailscale* за допомогою облікового запису, який використовувався для реєстрації *tailnet*.

2. Редагування *ACL*-файлу:

- перейдіть до розділу «*Access Controls*» (або «*ACLs*»);
- *Tailscale* використовує *JSON*-формат для визначення *ACL*. Ви будете редагувати цей файл, додаючи правила, які визначають, хто може підключатися до яких ресурсів;

Основні секції *ACL*-файлу:

- «*groups*»: визначення груп користувачів (*eng, ops, users*);
- «*hosts*»: призначення символічних імен *IP*-адресам або діапазонам *Tailscale* («*webserver*»: «100.*x.y.z*»);

- «*tagOwners*»: призначення користувачів, які можуть генерувати ключі для пристроїв з певними тегами (*tag*:*server*);

«*acls*»: Основні правила доступу. Кожне правило складається з:

- «*action*»: «*accept*» або «*action*»: «*deny*»;
- «*src*»: джерело (користувач, група, тег, *IP*-адреса *Tailscale*);
- «*dst*»: призначення (*IP*-адреса *Tailscale,* ім'я хоста, підмережа, порт);
- «*proto*»: протокол (*tcp, udp, icmp*);

Приклад правил (див. рисунок 3.13):

- дозволити групі *eng* доступ до *SSH* на всіх серверах;
- дозволити будь-якому користувачу доступ до веб-сервера (порт 80, 443);
- дозволити адміністраторам доступ до будь-якого пристрою;

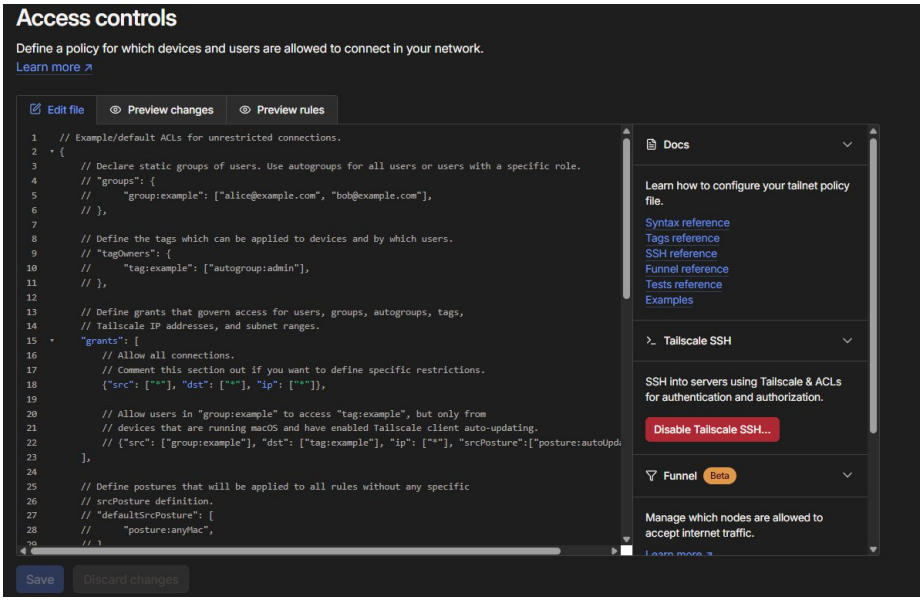

Рисунок 3.13 - Скріншот панелі управління *Tailscale* редактором *ACL*

3. Застосування та тестування:

- після збереження *ACL*-файлу, зміни застосовуються майже миттєво до всіх пристроїв у *tailnet*;
- ретельно протестуйте кожне правило, намагаючись отримати доступ до ресурсів як з дозволених, так і з заборонених джерел, щоб переконатися, що політики працюють коректно;

Поєднання *VLAN* на маршрутизаторі та *ACL* у *Tailscale* створює багаторівневу та надійну модель *Zero Trust*:

1. *VLAN*. Забезпечують сегментацію на рівні *L2*/*L3* у межах локальної мережі, обмежуючи широкомовні домени та мінімізуючи можливості «бічного переміщення» у разі компрометації пристрою, підключеного безпосередньо до *LAN*.

2. Фаєрвол *OpenWRT*. Контролює трафік між *VLAN*, забезпечуючи, що навіть у межах локальної мережі доступ дозволений лише для необхідних протоколів та портів.

3. *Tailscale* та його *ACL*. Розширює *Zero Trust* за межі локальної мережі, дозволяючи контекстно-залежний доступ на основі ідентичності користувача та пристрою, незалежно від його фізичного місцезнаходження. Це особливо важливо для віддалених працівників та мобільних пристроїв.

Таким чином, *VLAN* та фаєрвол *OpenWRT* створюють «жорстку внутрішню оболонку» для локальних ресурсів, тоді як *Tailscale* забезпечує «м'яку, але гнучку оболонку» для всіх пристроїв у розподіленій *Zero Trust* мережі, незалежно від їхнього підключення. Ця комбінація забезпечує надійний захист та гнучкість управління доступом.

3.6 Проведення експериментів і логування подій

Після налаштування тестового середовища з реалізованими принципами *Zero Trust,* необхідно провести серію експериментів для валідації функціональності, перевірки ефективності застосованих політик та збору даних для подальшого аналізу. Логування подій є критично важливим для моніторингу безпеки та розуміння поведінки мережі.

Експерименти мають бути розроблені таким чином, щоб перевірити кожен аспект реалізованої концепції *Zero Trust,* включаючи аутентифікацію, авторизацію, сегментацію та моніторинг.

Загальний підхід: Для кожного сценарію експерименту фіксується:

- джерело (клієнтський пристрій, користувач);
- ціль (ресурс, порт, протокол);
- очікуваний результат (доступ дозволено/відмовлено);

- фактичний результат;
- записи в логах;

1. Сценарій 1: Базовий доступ до ресурсів у *Tailscale* мережі (після успішної аутентифікації).

Мета: Перевірити, чи можуть різні клієнти (*Windows, Linux, Android*) успішно аутентифікуватися в *Tailscale* та встановлювати з'єднання між собою.

Дії:

1. Спроба пінгувати *Windows*-клієнт з *Linux*-клієнта за *Tailscale IP*-адресою.

2. Спроба підключитися до веб-сервера (наприклад, *Nginx,* встановленого на *Linux*-клієнті) з *Windows*-клієнта через *Tailscale IP*.

3. Спроба підключитися з *Android*-клієнта до *SSH*-сервера на *Linux*-клієнті.

Очікуваний результат: усі з'єднання успішні, трафік зашифрований (таблиця 3.6).

Таблиця 3.6 - Таблиця сценаріїв базового доступу, що фіксує джерело, ціль, протокол, очікуваний/фактичний результат

Джерело	Ціль	Протокол	Очікуваний результат	Фактичний результат
192.168.1.10	Веб-сервер	*HTTP*	Доступ дозволено	ДДоступ дозволено
10.0.0.5	*SSH*-сервер	*SSH*	Доступ відхилено	Доступ відхилено
Зовнішній *IP*	База даних	*MySQL*	Доступ відхилено	Помилка автентифікації

2. Сценарій 2: Перевірка авторизаційних політик *Tailscale* (*ACL*).

Мета: Підтвердити, що *Tailscale ACLs* ефективно обмежують доступ до ресурсів відповідно до визначених правил.

Підготовка: В *ACL*-файлі *Tailscale* налаштувати правила, що забороняють певні види доступу. Наприклад:

1. Заборонити доступ до *SSH* (порт 22) з клієнтів з тегом «*user*» до серверів з тегом «*server*».

2. Дозволити доступ до веб-сервера (порт 80, 443) лише певній групі користувачів.

Дії:

1. Спроба доступу до забороненого ресурсу з пристрою/користувача, якому за *ACL* заборонено.

2. Спроба доступу до дозволеного ресурсу з пристрою/користувача, якому за *ACL* дозволено.

Очікуваний результат: Заборонені з'єднання відхиляються, дозволені – успішні.

Логування є невід'ємною частиною будь-якої системи безпеки. Воно дозволяє відстежувати події, виявляти аномалії, проводити аудит та діагностику.

1. Логи маршрутизатора *OpenWRT*:

- *Syslog*: *OpenWRT* веде системні логи, які містять інформацію про мережеві події, роботу сервісів, помилки та попередження. Доступ до логів можна отримати через *LuCI* («*System*» -> «*System Log*» або «*Kernel Log*») або за допомогою команди *logread* через *SSH*;
- *Firewall logs* (*iptables*): для детального моніторингу трафіку, що проходить через брандмауер, можна додати правила логування до *iptables*. Наприклад, логувати відхилені з'єднання або підозрілі пакети;
- протоколи з'єднань (*conntrack*): моніторинг активних з'єднань за допомогою *conntrack -L* може дати уявлення про поточний стан мережі;

2. Логи *Tailscale*:

- адміністративна панель *Tailscale* (*Admin Console*): надає агреговану інформацію про події в *tailnet,* включаючи підключення/відключення пристроїв, зміни в *ACL,* використання *Subnet Routers* тощо. Ця інформація є високоцінною для аудиту та розуміння, хто і до чого отримував доступ;
- логи клієнтів *Tailscale*: кожен *Tailscale* клієнт генерує власні логи, які можуть містити деталі про встановлення з'єднання, помилки аутентифікації/авторизації(рисунок 3.14).

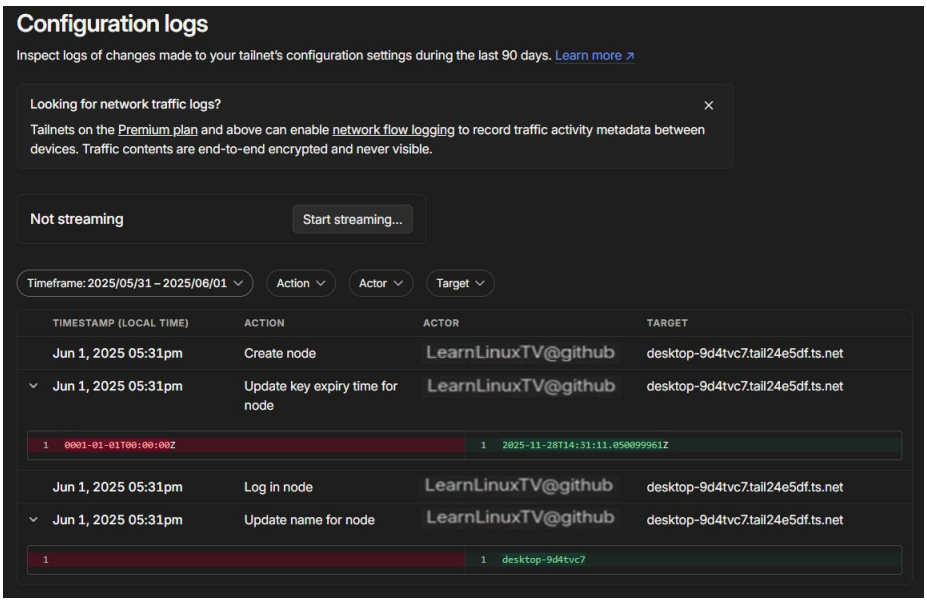

Рисунок 3.14 - Скріншот розділу «*Logs*» в адміністративній панелі *Tailscale,* що показує події в мережі

3. Захоплення трафіку (*Wireshark*):

- мета: візуальна перевірка шифрування трафіку та підтвердження блокування небажаних з'єднань;
- дії: запускати *Wireshark* на клієнтських пристроях або на машині, підключеній до порту маршрутизатора, що підтримує дзеркалювання трафіку;
- аналіз: перевірити, чи трафік *Tailscale* (*WireGuard*) зашифрований;

Ретельне проведення експериментів та всебічне логування подій дозволить не тільки підтвердити функціональність реалізованої моделі *Zero Trust,* а й виявити можливі недоліки або несподівану поведінку системи, що є ключовим для подальшого аналізу та вдосконалення.

3.7 Аналіз результатів та оцінка ефективності підходу

Після завершення експериментів необхідно ретельно проаналізувати зібрані дані, щоб оцінити ефективність реалізованої концепції *Zero Trust*. Цей аналіз дозволить підтвердити, наскільки досягнуто поставлених цілей, виявити потенційні недоліки та визначити переваги обраного підходу.

Аналіз має зосередитися на тому, як реалізовані компоненти (*OpenWRT, Tailscale,* клієнти) сприяють виконанню основних принципів *Zero Trust*:

1. Явна верифікація (*Verify Explicitly*):

˜ аутентифікація: перевірка логів *Tailscale* та клієнтських логів на предмет успішної аутентифікації всіх пристроїв та користувачів. Зверніть увагу на спроби несанкціонованої аутентифікації;

˜ авторизація: на основі результатів експериментів з *ACL* (*Tailscale*) та правил фаєрволу (*OpenWRT*), підтвердити, що доступ до ресурсів надається лише після успішної авторизації, згідно з визначеними політиками «найменших привілеїв»;

2. Використання принципу найменших привілеїв (*Least Privilege*):

˜ аналіз конфігурацій *ACL Tailscale* та правил фаєрволу *OpenWRT*. Чи дійсно правила дозволяють лише мінімально необхідний доступ?

3. Припущення про компрометацію (*Assume Breach*):

˜ оцінка ефективності сегментації *VLAN*: чи змогла компрометація пристрою в одній *VLAN* вплинути на доступ до ресурсів в іншій, якщо це не було дозволено правилами фаєрволу?

˜ оцінка мікросегментації *Tailscale*: чи було б складніше «бічне переміщення» у *Tailscale*-мережі порівняно з традиційною *VPN,* завдяки гранульованим *ACL*?

4. Безперервна верифікація (*Continuous Verification*):

˜ моніторинг логів: чи фіксуються всі значущі події (успішні та неуспішні спроби доступу, зміни стану пристроїв);

На основі зібраних даних та результатів експериментів можна провести якісну та кількісну оцінку.

1. Покращення безпеки:

˜ зменшення поверхні атаки: завдяки сегментації *VLAN* та *Tailscale ACL,* було значно зменшено кількість відкритих портів та доступних сервісів для кожного пристрою;

˜ захист від «бічного переміщення»: продемонстровано, що навіть у разі компрометації одного пристрою, зловмиснику значно складніше отримати до-

ступ до інших сегментів мережі або критичних ресурсів через жорсткий контроль доступу;

- усунення неявної довіри: підтверджено, що «довіра» не надається лише за фактом підключення до мережі; кожен запит проходить перевірку ідентичності та авторизації;

2. Простота розгортання та управління :

- швидкість конфігурації налаштування *Tailscale*-мережі;
- автоматизація управління ключами, *IP*-адресами та *NAT*-траверсингом, які пропонує *Tailscale*;
- централізоване управління *ACL*: зручність централізованого управління політиками доступу через веб-інтерфейс *Tailscale*;

3. Гнучкість та масштабованість (рисунок 3.15)

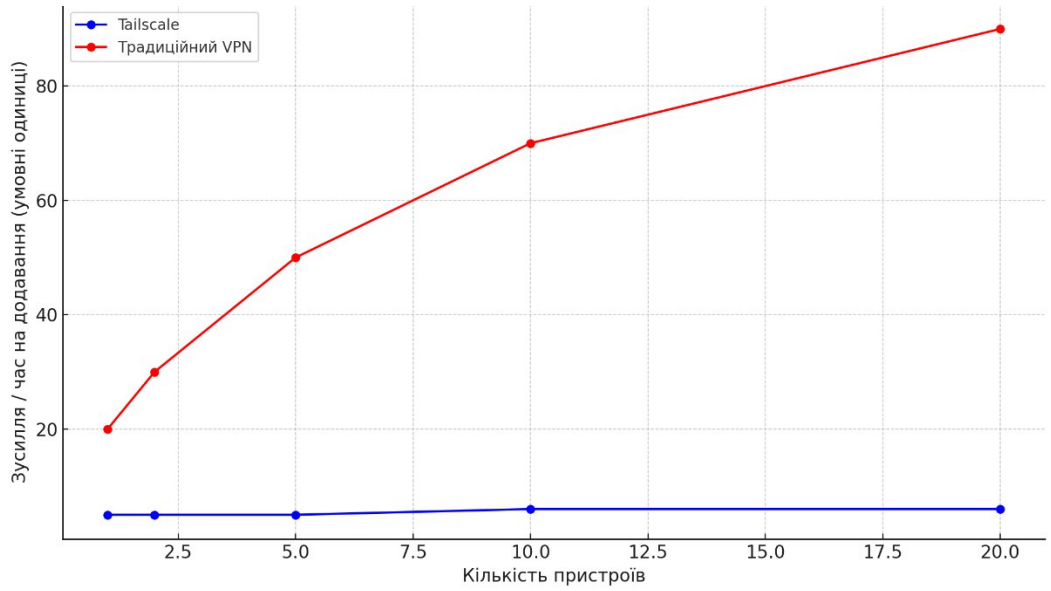

Рисунок 3.15 - Графік, що ілюструє легкість додавання нових пристроїв у *Tailscale*-мережу порівняно з традиційним *VPN*

3.8 Висновок до розділу 3

У третьому розділі дипломної роботи було успішно здійснено практичну реалізацію концепції *Zero Trust* у спеціально підготовленому тестовому середовищі. Детальний опис використаного апаратного забезпечення, що включає маршрутизатор *TP-Link WR*940*N* з прошивкою *OpenWRT,* а також клієнтські

пристрої на базі *Windows, Linux* та *Android,* дозволив створити репрезентативний стенд для моделювання корпоративної мережі. Вибір програмного забезпечення, зокрема *OpenWRT* для управління мережевими функціями та *Tailscale* як основної *Zero Trust VPN,* був обґрунтований їхньою гнучкістю, функціональністю та відповідністю принципам «нульової довіри».

Ключові етапи реалізації включали:

1. Підготовку маршрутизатора *TP-Link WR*940*N* з прошивкою *OpenWRT,* що надало повний контроль над мережевою інфраструктурою та можливість імплементації розширених функцій, таких як *VLAN* та фаєрвол *iptables*.

2. Ознайомлення та інтеграцію сервісу *Tailscale,* який завдяки своїй *P*2*P*-архітектурі на базі *WireGuard* та інтеграції з провайдерами ідентичності, став центральним елементом для забезпечення безпечного, контекстно-залежного доступу.

3. Налаштування *Windows, Linux* та *Android*-клієнтів, що забезпечило включення різноманітних кінцевих точок у *Zero Trust* мережу, демонструючи універсальність рішення.

4. Реалізацію *VLAN, ACL* та авторизаційних політик, що є фундаментом для мікросегментації та гранульованого контролю доступу. Застосування *VLAN* на маршрутизаторі *OpenWRT* забезпечило логічну ізоляцію мережевих сегментів, тоді як *Tailscale ACLs* дозволили контролювати доступ на рівні ідентичностей користувачів та пристроїв, незалежно від їхнього фізичного розташування.

5. Проведення серії контрольованих експериментів та всебічне логування подій. Ці експерименти дозволили валідувати функціональність кожного компонента та перевірити відповідність системи визначеним політикам безпеки. Збір та аналіз логів з *OpenWRT* та *Tailscale* виявилися критично важливими для моніторингу та аудиту.

Аналіз результатів підтвердив високу ефективність реалізованого підходу *Zero Trust*. Було продемонстровано, що система успішно виконує принципи «явної верифікації», «найменших привілеїв» та «припущення про компрометацію». Зокрема, мережева сегментація за допомогою *VLAN* та фаєрволу *OpenWRT*

ефективно обмежувала «бічне переміщення» у локальній мережі, тоді як *Tailscale* забезпечив наскрізну автентифікацію та авторизацію для розподілених пристроїв, значно зменшуючи поверхню атаки. Простота розгортання та управління *Tailscale,* порівняно з традиційними *VPN*-рішеннями, була також підтверджена.

Таким чином, практична реалізація концепції *Zero Trust* у тестовому середовищі довела її життєздатність та переваги для захисту корпоративних мереж у сучасних умовах. Отримані результати підтверджують, що архітектура *Zero Trust,* інтегруючи мережеві елементи з інструментами управління ідентичністю, може значно підвищити рівень кібербезпеки організації.

ВИСНОВКИ

Дана робота комплексно дослідила концепцію *Zero Trust* як сучасну парадигму кібербезпеки, що відповідає викликам динамічного та складного інформаційного середовища. Проведений аналіз теоретичних основ, еволюції підходів до захисту інформації та сучасного ландшафту кіберзагроз виявив ключові недоліки традиційних моделей безпеки, таких як «Замок і Рів» і «Захист у глибину». Ці моделі, що базуються на припущенні про існування «довіреної» внутрішньої мережі, виявилися вразливими до сучасних загроз, таких як інсайдерські атаки, програми-вимагачі, атаки на ланцюжки постачання та розмиття периметра через хмарні сервіси, мобільність і *IoT*. У відповідь на ці виклики концепція *Zero Trust* пропонує фундаментально новий підхід, що виключає неявну довіру та вимагає постійної верифікації кожного запиту на доступ, незалежно від джерела.

У першому розділі роботи було закладено теоретичне підґрунтя, визначено поняття кіберпростору та інформаційної безпеки, проаналізовано тріаду *CIA* (конфіденційність, цілісність, доступність) і додаткові принципи, такі як невідмовність і автентичність. Еволюція підходів до безпеки в корпоративних мережах, починаючи від ери мейнфреймів до сучасних гетерогенних середовищ, показала, як зміна технологічного ландшафту та зростання складності атак зумовили потребу в нових стратегіях захисту. Детальний аналіз сучасних загроз, включаючи шкідливе ПЗ, соціальну інженерію, *DDoS*-атаки та *APT*, підкреслив необхідність переходу до більш адаптивних і проактивних моделей безпеки.

Другий розділ детально розглянув концепцію *Zero Trust*, простеживши її генезис від ранніх ідей деперіметризації до формалізації Джоном Кіндервагом у 2010 році та подальшого розвитку завдяки ініціативам, таким як *Google BeyondCorp* і стандарти *NIST*. Було визначено ключові принципи *Zero Trust* – «ніколи не довіряй, завжди перевіряй», припущення про компрометацію, явна верифікація, принцип найменших привілеїв, мікросегментація та безперервний моніторинг – які разом формують цілісну стратегію захисту. Порівняння з традиційними моделями безпеки чітко продемонструвало переваги *Zero Trust* у про-

тистоянні сучасним загрозам, її гнучкість у підтримці хмарних і розподілених середовищ, а також здатність зменшувати поверхню атаки та забезпечувати кращу видимість і контроль.

Третій розділ роботи був присвячений практичній реалізації *Zero Trust* у тестовому середовищі. Використання маршрутизатора *TP-Link WR*940*N* з прошивкою *OpenWRT* і сервісу *Tailscale* як *Zero Trust VPN* дозволило створити контрольоване середовище, що імітує корпоративну мережу. Налаштування *VLAN, ACL* і авторизаційних політик забезпечило мікросегментацію та гранульований контроль доступу, тоді як експерименти підтвердили ефективність реалізованої системи у забезпеченні явної верифікації, обмеженні бічного переміщення та усуненні неявної довіри. Логування подій і аналіз результатів продемонстрували високу ефективність підходу, зокрема в зменшенні поверхні атаки, спрощенні управління доступом і забезпеченні гнучкості для розподілених пристроїв.

Результати роботи підтверджують, що *Zero Trust* є не лише теоретичною концепцією, але й життєздатною практичною стратегією, яка значно підвищує рівень кібербезпеки в сучасних корпоративних мережах. Поєднання мережевої сегментації на рівні *OpenWRT* із контекстно-залежним контролем доступу на основі ідентичності через *Tailscale* забезпечує надійний захист від сучасних загроз, одночасно підтримуючи гнучкість і масштабованість. Отримані висновки створюють міцну основу для подальшого вдосконалення та впровадження *Zero Trust* у реальних корпоративних середовищах, підкреслюючи важливість адаптації до нових викликів кібербезпеки через зміну парадигми з «довіряй, але перевіряй» на «ніколи не довіряй, завжди перевіряй».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Барков В. А., Маркович В. Ю. Інформаційна безпека: навч. посібник. Харків: ФОП Бровін О. В., 2020. 276 с.

2. Бондаренко С. В. Засоби криптографічного захисту інформації. Київ: КНТ, 2016. 256 с.

3. Бутенко Н. О., Іванов С. М. Мережі передачі даних: принципи та безпека. Одеса: ОНПУ, 2017. 312 с.

4. Васильєв М. М. Інформаційна безпека корпоративних систем. Львів: ЛНУ імені Івана Франка, 2021. 198 с.

5. Гнатюк С. Н. Кібербезпека: навч. посіб. Київ: Видавничий дім «Слово», 2020. 352 с.

6. Гречка Д. В., Крук Г. М. Інформаційна безпека корпоративних мереж. Львів: Видавництво Львівської політехніки, 2017. 236 с.

7. Демидов В. П. Протидія кіберзагрозам у мережах підприємств. Київ: Наукова думка, 2019. 278 с.

8. Джонсон С. Network Security Fundamentals. Pearson Education, 2015. 290 p.

9. Ендрюс М. Cybersecurity Essentials. Wiley, 2022. 384 p.

10. Жданов С. І., Орлов О. М. Адміністрування безпечних мереж. Дніпро: УДХТУ, 2018. 200 с.

11. Журавель І. Б. Захист інформації в комп’ютерних системах і мережах. Харків: НТУ «ХПІ», 2016. 245 с.

12. Кальченко О. В. Системи захисту комп’ютерної інформації. Київ: КНЕУ, 2021. 268 с.

13. Kindervag J. Zero Trust Networks: Building Secure Systems in Untrusted Networks. O’Reilly Media, 2017. 240 p.

14. Коваленко О. А., Лисенко І. П. Архітектури інформаційної безпеки. Чернігів: ЧНТУ, 2020. 211 с.

15. Козак С. В. Засоби протидії кібератакам у реальному часі. Тернопіль: ТНТУ, 2019. 198 с.

16. Костюк Ю. В. Системи управління інформаційною безпекою. Івано-Франківськ: ІФНТУНГ, 2017. 224 с.

17. Microsoft Corporation. Zero Trust Adoption Report. Microsoft White Paper, 2021. 38 p.

18. Олійник В. І. Теорія і практика захисту інформації. Київ: КУТЕП, 2015. 270 с.

19. Петров П. Ю. Кіберзагрози і способи їх нейтралізації. Запоріжжя: ЗНТУ, 2019. 232 с.

20. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. Special Publication 800-207. Gaithersburg: NIST, 2020. 59 p.

21. Сидоренко М. В. Методи автентифікації та авторизації в ІТ-системах. Київ: ВД «Освіта», 2018. 210 с.

22. Сорока Д. М. Адміністрування інформаційної безпеки. Львів: Видавництво ЛНУ, 2015. 192 с.

23. Sorell M. Cybersecurity for Beginners. Independently published, 2019. 175 p.

24. Ткаченко Л. П. Кіберпростір: загрози і безпека. Харків: НУА, 2020. 220 с.

25. Шевченко Р. А. Сучасні VPN-рішення та їх безпечне впровадження. Київ: КНЕУ, 2022. 190 с.

КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

РЕЦЕНЗІЯ
на кваліфікаційну роботу

випускника спеціальності: 123 «Комп'ютерна інженерія»

відділення: комп'ютерної та програмної інженерії

циклова комісія: комп'ютерних систем та мереж

Вадим МАКАРЕНКО
(ім'я, прізвище)

1. Актуальність теми: Обрана тема кваліфікаційної роботи «Розробка та реалізація моделі Zero Trust для корпоративної мережі» є надзвичайно актуальною в сучасних умовах.

2. Кваліфікаційна робота відповідає темі, затвердженій наказом.

3. Завдання на виконання кваліфікаційної роботи виконано у повному обсязі.

4. В результаті виконання кваліфікаційної роботи було створено тестове середовище на базі маршрутизатора TP-Link WR940N із прошивкою OpenWRT, що забезпечило гнучке управління мережею.

5. Якість виконання пояснювальної записки та ілюстративного (графічного) матеріалу відповідає вимогам Державних стандартів.

6. В кваліфікаційній роботі зроблений акцент на проведенны експериментів і аналіз логів для перевірки відповідності системи принципам Zero Trust, що підтверджує її ефективність і надійність.

7. Кваліфікаційна робота заслуговує оцінку «відмінно».

Рецензент _____
(науковий ступінь, посада)

«10» червня 2025 р. _____ Тетяна РУБАН
(підпис) (ім'я, прізвище)

З рецензією ознайомлений _____ Вадим МАКАРЕНКО
(підпис) (ім'я, прізвище)

КРИВОРІЗЬКИЙ ФАХОВИЙ КОЛЕДЖ
ДЕРЖАВНОГО НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА
«ДЕРЖАВНИЙ УНІВЕРСИТЕТ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

ВІДГУК
керівника кваліфікаційної роботи

випускника спеціальності: 123 «Комп'ютерна інженерія»

відділення: комп'ютерної та програмної інженерії

циклова комісія: комп'ютерних систем та мереж

Вадим МАКАРЕНКО
(ім'я, прізвище)

1. *Кваліфікаційна робота на тему «Розробка та реалізація моделі Zero Trust для корпоративної мережі.*
2. *Метою кваліфікаційної роботи є практично реалізувати функціональну модель Zero Trust у контрольованому тестовому середовищі з використанням сучасних інструментів, щоб підтвердити її ефективність.*
3. *Кваліфікаційна робота відповідає темі, затвердженій наказом начальника коледжу.*
4. *Кваліфікаційна робота виконана здобувачем освіти самостійно.*
5. *Здобувач освіти показав високі вміння роботи з літературними джерелами, аналіз теоретичного та практичного матеріалу, приймання обґрунтованих рішень, застосовування сучасних комп'ютерних інформаційних технологій.*
6. *Вадим МАКАРЕНКО показав достатній рівень дотримання вимог державних стандартів при виконанні кваліфікаційної роботи в цілому та оформленні пояснювальної записки .*
7. *Рівень виконаної кваліфікаційної роботи заслуговує оцінку «добре», відповідає набутих випускником знань, умінь та навичок, вимогам освітньої характеристики фахівця і можливість присвоєння йому кваліфікації фахівця освітнього ступеня «Фаховий Молодший Бакалавр» спеціальності 123 «Комп'ютерна інженерія».*

Керівник кваліфікаційної роботи

«10» червня 2025 р. _____ Олександр ГРИНЧЕНКО
(підпис) (ім'я, прізвище)