Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

# КВАЛІФІКАЦІЙНА РОБОТА

Система безпеки IoT-інфраструктури підприємства на основі концепції Zero Trust
Назва теми

Рівень вищої освіти *перший (бакалаврський)*

Галузь знань *12 «Інформаційні технології»*
Шифр. назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр. назва

Освітня програма *«Комп'ютерна інженерія та програмування»*
Назва

Шифр КвРКІ 022002.22.01.110 ПЗ

Виконав здобувач IV курсу, група КІ2-22-1 — Підпис — Дмитро БЕБИХ (Ініціали, прізвище)

Керівник — Науковий ступінь, учене звання — Підпис — Андрій ГАРМАТЮК (Ініціали, прізвище)

Нормоконтролер — канд.фіз.-мат.наук,доц. (Науковий ступінь, учене звання) — Підпис — Тетяна КИСІЛЬ (Ініціали, прізвище)

До захисту допускаю:
завідувач кафедри КІІС
«01» червня 2026 р.
дата — Підпис — Ольга ПАВЛОВА (Ініціали, прізвище)

Хмельницький 2026

# ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Комп'ютерної інженерії та інформаційних систем

Рівень вищої освіти перший (бакалаврський)

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма «Комп'ютерна інженерія та програмування»

ЗАТВЕРДЖУЮ
Завідувачка кафедри КІІС
Ольга ПАВЛОВА

" 22 " 05 2026 р.

## ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Бебих Дмитро Валерійович
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Проектування системи безпеки IOT-інфраструктури на основі концепції Zero Trust
Керівник проекту (роботи) Гарматюк Андрій Вікторович, асистент
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 20.01.2026 р. № 7
2. Термін подання здобувачем роботи на кафедру 25.05.2026 р.
3. Вихідні дані до роботи Завдання на кваліфікаційну роботу
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Дослідження предметної області та постановки задач
Проєктування системи безпеки IOT-інфраструктури на основі концепції ZERO TRUST
Програмно-апаратна реалізація системи безпеки IOT-інфраструктури на основі концепції ZERO TRUST
5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Алгоритми роботи сегментованої мережі
Топологія мережі
Тестування та шифрування

6. Консультанти розділів кваліфікаційної роботи

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

7. Дата видачі завдання « 10 » 01 2026 р.

## КАЛЕНДАРНИЙ ПЛАН

| №з/п | Назва етапів (розділів) дипломного проекту (роботи) | Термін виконання етапів проекту (роботи) | Примітка |
|---|---|---|---|
| 1 | Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником | 10.01.2026 | виконано |
| 2 | Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження | 01.02.2026 | виконано |
| 3 | Робота над розділом 1 – дослідження предметної області та постановка задачі | 01.03.2026 | виконано |
| 4 | Робота над розділом 2 – вибір компонентів для проєктування системи безпеки IOT-інфраструктури на концепції Zero Trust | 01.04.2026 | виконано |
| 5 | Робота над розділом 3 – проєктування системи адаптивного застосування системи безпеки IOT-інфраструктури на концепції Zero Trust | 29.04.2026 | виконано |
| 6 | Оформлення пояснювальної записки згідно вимог | 25.05.2026 | виконано |
| 7 | Попередній захист ВКР | 26.05.2026 | виконано |
| 8 | Захист ВКР на засіданні ЕК | Червень 2026 року | |

Здобувач _____ Дмитро БЕБИХ
Підпис Ім'я, ПРІЗВИЩЕ

Керівник кваліфікаційної роботи _____ Андрій ГАРМАТЮК
Підпис Ім'я, ПРІЗВИЩЕ

| № рядка | формат | Позначення | Найменування | Кіл. листів | № екз | Примітка |
|---|---|---|---|---|---|---|
| | | | Текстові документи | | | |
| 1 | | КвРКІ 022002.22.01.110 ПЗ | Пояснювальна записка | 72 | | |
| | | | | | | |
| | | | Графічні матеріали | | | |
| 2 | | КвРКІ 022002.22.01.110 Е8 | Алгоритми роботи сегментованої мережі | 1 | | |
| | | | | | | |
| 3 | | КвРКІ 022002.22.01.110 Е8 | Топологія мережі | 1 | | |
| | | | | | | |
| | | | | | | |
| 4 | | КвРКІ 022002.22.01.110 Е8 | Тестування та шифруваня | 1 | | |

| Зм | Арк | № докум | Підпис | Дата | КвРКІ 022002.22.01.110 ВП | | |
|---|---|---|---|---|---|---|---|
| Розробив | | Бебих | | | Відомість проекту | Літера | Аркуш 4 / Аркушів 70 |
| Перевір. | | Гарматюк | | | | У | |
| Н. контр. | | Кисіль | | | | ХНУ, КІ2-22-1 | |
| Затв. | | Павлова | | 01.06 | | | |

# АНОТАЦІЯ

Тема кваліфікаційної роботи: «Система захисту IoT-інфраструктури підприємництва на основі концепції Zero Trust».

Автор роботи: Дмитро БЕБИХ.

Керівник роботи: Андрій Гарматюк.

Пояснювальна записка: 72 с., 11 рис., 12 табл., 3 дод., 40 джерел.

Графічна частина: 3 креслення.

ACL, AAA, CISCO PACKET TRACER, VLAN, ZERO TRUST, АВТЕНТИФІКАЦІЯ, IOT-ІНФРАСТРУКТУРА, СИСТЕМИ БЕЗПЕКИ, МІКРОСЕГМЕНТАЦІЯ, ШИФРУВАННЯ.

Кваліфікаційна робота бакалавра присвячена розробці та дослідженню системи захисту IoT-інфраструктури підприємництва на основі концепції Zero Trust. Актуальність теми зумовлена стрімким розвитком IoT-технологій та зростанням кількості кіберзагроз, спрямованих на мережеві пристрої, сенсори, серверне обладнання та елементи інфокомунікаційної інфраструктури підприємств.

Для досягнення поставленої мети було виконано аналіз сучасних підходів до забезпечення безпеки IoT-мереж, досліджено наявні програмно-апаратні засоби захисту, сформовано технічні вимоги до системи, розроблено архітектуру мережі з мікросегментацією, спроєктовано політики доступу, автентифікації та шифрування, а також реалізовано модель мережі у середовищі Cisco Packet Tracer із подальшим тестуванням механізмів VLAN, ACL, AAA та Port Security.

У результаті виконання роботи створено модель захищеної IoT-інфраструктури підприємництва, яка забезпечує контроль доступу до мережевих ресурсів, сегментацію трафіку, підвищення рівня кібербезпеки та зниження ризиків несанкціонованого доступу до компонентів системи.

Підпис здобувача

30.05.2026

Дата

## ЗМІСТ

# ВСТУП

Поширення концепції Інтернету речей радикально змінило структуру корпоративних мереж сучасних підприємств. Інтеграція датчиків, контролерів, шлюзів, виконавчих механізмів та інтелектуальних кінцевих вузлів у єдиному комунікаційному просторі сформувала якісно нове середовище, у якому традиційне розмежування «довірених» та «недовірених» сегментів втратило свою захисну функцію. Розмиття мережевого периметра, гетерогенність кінцевих пристроїв з обмеженими обчислювальними ресурсами, відсутність уніфікованих механізмів автентифікації та неконтрольоване зростання числа точок входу у корпоративну мережу обумовили появу принципово нових векторів атак, які класична модель «жорсткого периметра» не здатна стримувати [8, 9].

Розвиток цифрових технологій, зокрема хмарних обчислень, віддаленого доступу та Інтернету речей, суттєво розширив можливості організацій, але водночас ускладнив забезпечення кібербезпеки. У сучасних мережах практично будь-який пристрій або сервіс може стати джерелом потенційної загрози [8]. Саме тому концепція Zero Trust, представлена в документі NIST SP 800-207, пропонує відмовитися від моделі безумовної довіри та використовувати принцип «ніколи не довіряй, завжди перевіряй» як основу захисту інформаційних систем [22].

Економічні наслідки інцидентів кібербезпеки на сьогоднішньому етапі досягли значень, які примушують переглядати підходи до проєктування корпоративних мереж. Середня вартість витоку даних у глобальному вимірі у 2025 році сягнула 4,4 млн доларів США, причому абсолютна більшість успішних атак була пов’язана з компрометацією облікових даних або зловживанням довіреним доступом [3]. Низка спостережень фіксує, що найвразливішим компонентом сучасних корпоративних інфраструктур стають IoT-пристрої, які

виробники постачають із заводськими паролями, без вбудованих механізмів багатофакторної автентифікації, без підтримки сучасних криптографічних протоколів і часто без можливості оновлення прошивки [7, 11].

Російсько-українська війна додала до означеного контексту ще один шар проблематики. Об'єкти критичної інфраструктури України стали мішенню систематичних кіберкампаній, у яких зловмисники використовують саме слабкі IoT-вузли як точку проникнення для подальшого латерального переміщення мережею. Кампанії останніх років демонструють, що компрометований сенсор, IP-камера або контролер «розумного» приміщення стає плацдармом для атаки на серверні сегменти, бази даних і системи управління технологічними процесами [6, 14]. Закон України «Про основні засади забезпечення кібербезпеки України» у редакції від 19 жовтня 2025 року прямо зобов'язує власників об'єктів кіберзахисту вживати організаційно-технічних заходів, які мінімізують такі ризики [12].

Концепція Zero Trust, сформульована Дж. Кіндервагом ще у 2010 році, отримала своє доктринальне оформлення в нормативі NIST SP 800-207 і у 2025 році перейшла зі статусу перспективної технології у статус операційної необхідності для будь-якого підприємства, незалежно від його масштабу [10, 22]. Архітектура нульової довіри постулює відсутність прихованої довіри до будь-якого активу, облік чи мережевого пристрою, незалежно від його фізичного або мережевого розташування. Кожен запит до ресурсу проходить процедуру верифікації, авторизації, контекстної оцінки та фіксується у системі централізованого моніторингу [16, 17].

Особливої складності набуває імплементація принципів Zero Trust саме в IoT-середовищах. Кінцеві пристрої з обмеженими ресурсами не підтримують традиційні протоколи багатофакторної автентифікації, не здатні виконувати ресурсомісткі криптографічні операції, не мають можливостей для встановлення агентів моніторингу. Дослідники Львівської політехніки [8] обґрунтовують, що для IoT-сегмента ефективною є реалізація Zero Trust через інфраструктурні

засоби – мікросегментацію на рівні VLAN, динамічне призначення політик через RADIUS, профілювання пристроїв на рівні мережевого обладнання та централізовану фільтрацію трафіку через ACL.

Cisco Packet Tracer являє собою функціонально потужний симулятор, який підтримує моделювання як класичної мережевої інфраструктури, так і IoT-пристроїв із сенсорами, виконавчими механізмами, мікроконтролерами та шлюзами «розумних» приміщень [10]. Середовище дозволяє побудувати реалістичну корпоративну мережу з декількома сегментами, налаштувати міжмережеві екрани, ACL, VLAN, механізми WPA3 та Port Security, а також відтестувати поведінку трафіку у режимі симуляції з покроковою візуалізацією руху пакетів. Сукупність наведених можливостей робить означене середовище раціональним вибором для прототипування та верифікації архітектурних рішень кібербезпеки.

Актуальність теми кваліфікаційної роботи визначається об’єктивною потребою підприємств у переході від периметрової моделі захисту до архітектури нульової довіри, що зумовлено стрімким зростанням кількості IoT-пристроїв, розмиттям мережевого периметра та появою нових класів кіберзагроз. Не дослідженим залишається питання про практичну реалізацію базових принципів Zero Trust у середовищі симуляції Cisco Packet Tracer для інфраструктури підприємства середнього масштабу з вираженим IoT-сегментом. Усе наведене зумовлює необхідність розробки прикладної моделі системи безпеки, придатної як для верифікації архітектурних рішень, так і для подальшої трансляції на реальне обладнання.

Об’єктом кваліфікаційної роботи є процеси забезпечення кібербезпеки IoT-інфраструктури підприємства.

Предметом кваліфікаційної роботи є методи, моделі та засоби побудови системи захисту IoT-інфраструктури на основі концепції Zero Trust із програмною реалізацією у середовищі Cisco Packet Tracer.

Метою кваліфікаційної роботи є розробка та програмно-апаратна реалізація системи безпеки IoT-інфраструктури підприємства на основі концепції Zero Trust, яка забезпечує мікросегментацію мережі, контрольований доступ та локалізацію інцидентів кібербезпеки в межах окремих сегментів.

Досягнення поставленої мети передбачає розв'язання таких **завдань**:

– виконати аналіз сучасного стану предметної області та виявити характерні вразливості IoT-середовищ підприємства;

– проаналізувати наявні програмно-апаратні рішення захисту IoT-інфраструктур, визначити їхні переваги та обмеження у контексті побудови системи захисту; – сформувати функціональні та нефункціональні вимоги до проєктованої системи й розробити технічне завдання;

– спроєктувати архітектуру системи безпеки на основі базових принципів Zero Trust, обрати засоби реалізації та обґрунтувати їх вибір;

– виконати програмно-апаратну реалізацію системи у середовищі Cisco Packet Tracer із застосуванням механізмів VLAN, ACL, AAA, Port Security, WPA3;

– провести тестування системи, оцінити її відповідність технічному завданню та сформулювати висновки щодо ефективності.

Методи дослідження. У роботі використано загальнонаукові та спеціальні методи: системний аналіз – для дослідження предметної області; порівняльний аналіз – для зіставлення наявних рішень захисту IoT; методи концептуального проєктування – для побудови логічної архітектури системи; методи імітаційного моделювання у середовищі Cisco Packet Tracer – для верифікації прийнятих архітектурних рішень; методи функціонального тестування – для оцінки відповідності реалізації технічному завданню.

Практичне значення одержаних результатів полягає у можливості використання розробленої моделі як референсного рішення для побудови систем кібербезпеки IoT-інфраструктур підприємств середнього масштабу, а також як навчально-методичного матеріалу для підготовки фахівців у галузі комп'ютерної інженерії

# 1 ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧ

## 1.1 Змістовний аналіз предметної області IoT-інфраструктури підприємництва та осмобливостей її захисту

Інтернет речей як технологічна парадигма становить мережу взаємопов'язаних фізичних об'єктів, які наділені обчислювальними, сенсорними та комунікаційними можливостями і здатні обмінюватися даними без втручання людини. У корпоративному вимірі IoT-інфраструктура підприємства охоплює широкий спектр пристроїв – від датчиків температури, вологості, задимлення, освітлення та руху до мережевих відеокамер, систем контролю доступу, лічильників ресурсів, виконавчих механізмів кліматичного обладнання, програмованих логічних контролерів виробничих ліній, медичних телеметричних модулів та інтелектуальних принтерів.

Архітектура IoT-середовища має чітко виражену рівневу структуру, описану в рекомендації ITU-T Y.2060 та підтверджену пізнішими дослідженнями [21]. Мережевий рівень відповідає за транспортування інформації та об'єднує дротові й бездротові технології (Ethernet, Wi-Fi, ZigBee, BLE, LoRaWAN, 5G).

Також важливо зазначити, що взаємодія між рівнями IoT-архітектури забезпечується стандартизованими протоколами та інтерфейсами, що підвищує сумісність різних компонентів системи

Рівень оброблення даних реалізується на серверах підприємства або у хмарних сервісах та забезпечує агрегацію, нормалізацію й аналітичне опрацювання інформації. Рівень застосунків постачає кінцевим користувачам функціональні сервіси та інтерфейси управління. Графічне представлення такої моделі подано на рис. 1.1

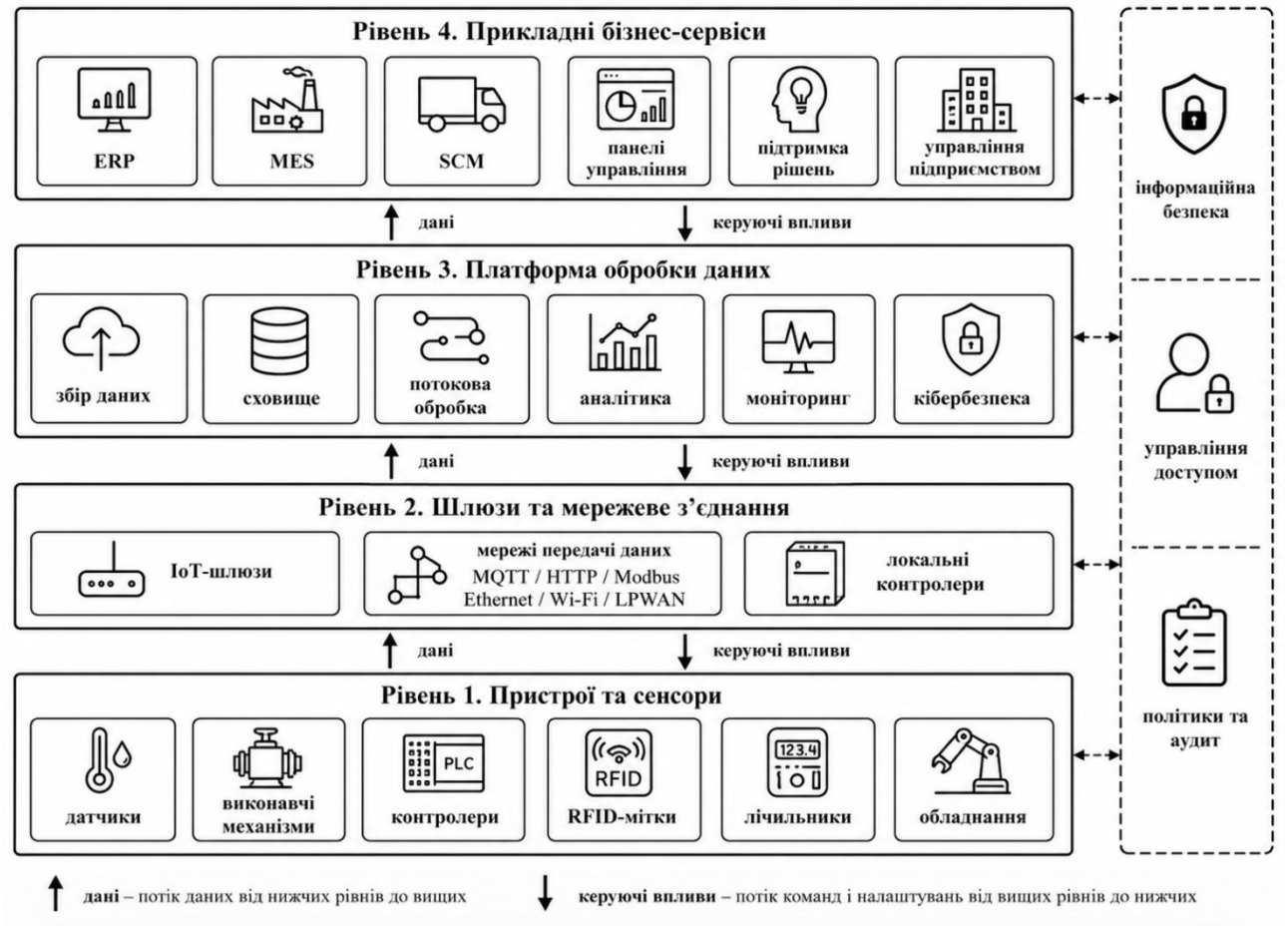



Рисунок 1.1 – Чотирирівнева архітектура IoT-інфраструктури підприємства

Принциповою особливістю IoT-середовища, яка зумовлює специфіку його захисту, є гетерогенність обчислювальних ресурсів кінцевих пристроїв. Багато сенсорів побудовано на мікроконтролерах із пам'яттю в кілька десятків кілобайт, обмеженою обчислювальною потужністю та автономним живленням від батареї, що унеможливлює застосування ресурсомістких криптографічних протоколів, агентів моніторингу або розширених засобів автентифікації [21]. Вісник Вінницького політехнічного інституту [21] обґрунтовує, що в залежності від наявних апаратних та програмних обмежень не всі захисні протоколи можна застосувати до малопотужних пристроїв, що змушує переносити основне навантаження безпеки з кінцевого пристрою на мережеву інфраструктуру.

Загрози безпеці IoT-інфраструктур підприємства мають комплексний характер і охоплюють усі чотири архітектурні рівні. На рівні сприйняття актуальними є фізичний доступ до пристроїв, підміна датчиків, маніпуляція

сигналами; на мережевому рівні – атаки типу «людина посередині», прослуховування трафіку, спуфінг, експлуатація відсутності шифрування; на рівні оброблення – атаки на брокери повідомлень, серверну логіку, бази даних телеметрії; на рівні застосунків – атаки на API, веб-консолі, мобільні клієнти. Узагальнена класифікація типових атак та векторів проникнення на IoT-пристрої представлена у таблиці 1.1.

Таблиця 1.1 – Класифікація типових атак на IoT-пристрої підприємства

| Категорія атаки | Вектор реалізації | Об’єкт впливу | Потенційні наслідки |
|---|---|---|---|
| Брутфорс облікових даних | Перебір типових пар «логін–пароль», що задані виробником | Веб-консоль пристрою, SSH, Telnet | Повний контроль над пристроєм, інкорпорація у ботнет |
| MITM-атака | Перехоплення нешифрованого трафіку у локальному сегменті | Канал передачі телеметрії, MQTT без TLS | Викрадення облікових даних, підміна команд |
| DDoS через ботнет | Залучення скомпрометованих пристроїв до ботнет-мережі (Mirai, Aidra) | Зовнішні цілі, внутрішні сервіси | Відмова в обслуговуванні, перевантаження каналів |
| Експлуатація прошивки | Використання незакритих CVE у прошивці пристрою | Системне ПЗ пристрою | Виконання довільного коду, постійна присутність |

Кінець таблиці 1.1

| | | | |
|---|---|---|---|
| Spoofing датчика | Підміна цифрового відбитка пристрою | Виконавчі механізми, аналітичні системи | Маніпуляція технологічним процесом |
| Латеральне переміщення | Використання компрометованого IoT-пристрою як плацдарму | Внутрішні сервери, бази даних | Ескалація атаки до критичних активів |

Найвідомішим прецедентом масштабної експлуатації слабкостей IoT-пристроїв стало шкідливе програмне забезпечення Mirai, яке у 2016 році сформувало ботнет приблизно зі 100 тисяч скомпрометованих пристроїв, що використовувалися для DDoS-атак гігантської потужності. Фундаментальною вразливістю, яка уможливила утворення означеного ботнету, стало використання однакових заводських паролів на масово розповсюджених «розумних» камерах та цифрових відеореєстраторах [13]. Наступна еволюція родини Mirai підтвердила, що навіть через десятиліття після інциденту переважна більшість атак на IoT-пристрої експлуатує саме типові паролі та незакриті уразливості старих прошивок.

Класифікаційну схему загроз IoT-середовищу за рівнями архітектури логічно подати у вигляді рис. 1.2, на якому виділено чотири кластери: фізичні загрози (несанкціонований доступ до пристрою, підміна апаратних модулів), мережеві загрози (перехоплення, спуфінг, DDoS), загрози рівня оброблення (атаки на брокери та сервери), загрози рівня застосунків (атаки на API, фішинг адміністраторів).

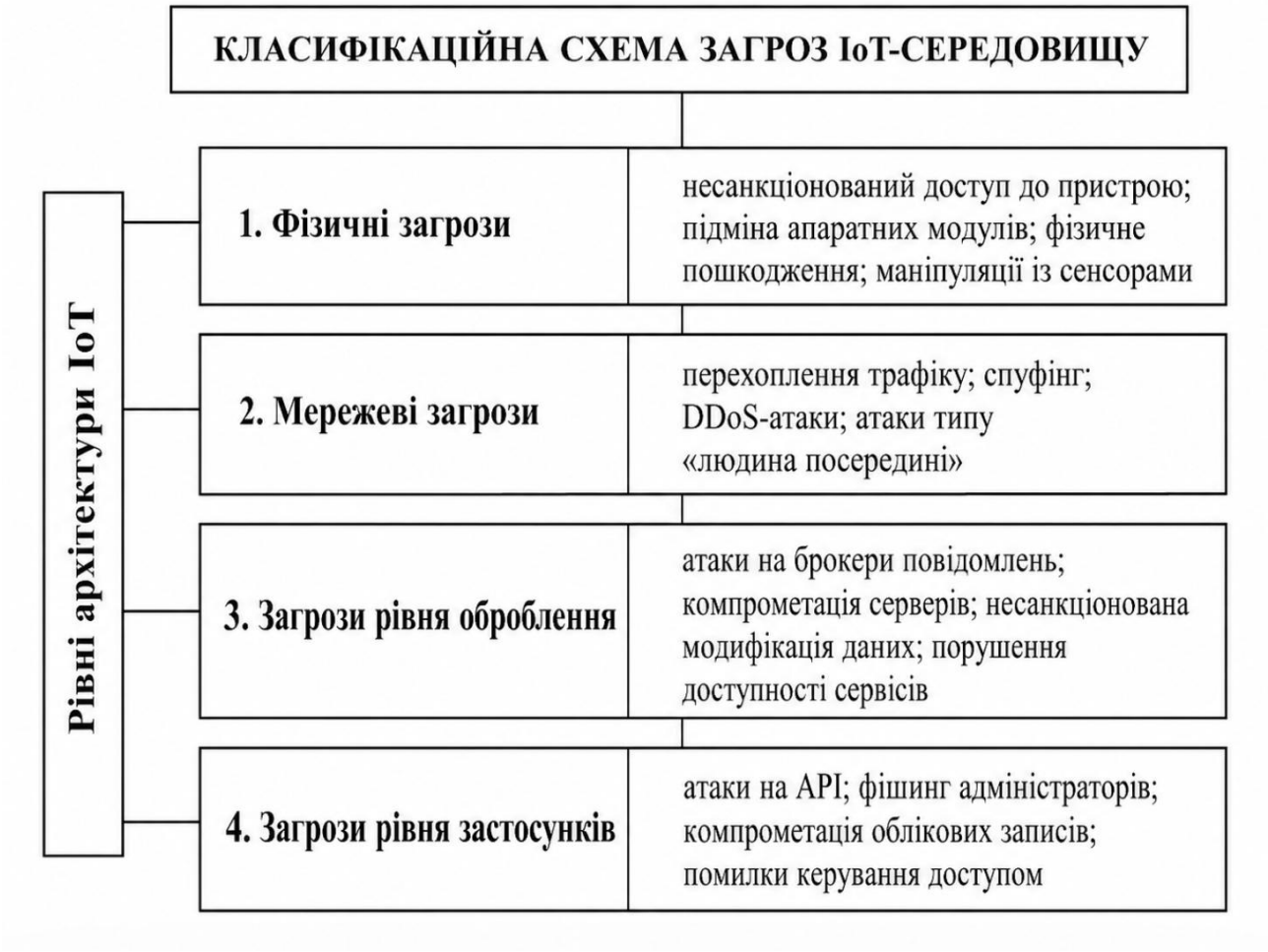



Рисунок 1.2 – Класифікаційна схема загроз IoT-середовищу

Графічна форма вказаного представлення дозволяє виявити, що саме мережевий рівень концентрує найбільшу кількість векторів атаки і одночасно є тим рівнем, на якому інфраструктурними засобами можна реалізувати найбільш ефективні захисні механізми.

Традиційна модель захисту корпоративної мережі базувалася на концепції «жорсткого периметра», у якій основним завданням систем безпеки був контроль трафіку на межі між внутрішньою мережею та зовнішнім середовищем. Зловмисник, який подолав периметр (через скомпрометований обліковий запис, фішинг, експлойт), отримував практично необмежений доступ до внутрішніх ресурсів, оскільки внутрішня мережа за замовчуванням вважалася довіреною [2, 16]. Структура внутрішніх потоків даних не контролювалася, що робило

неможливим виявлення латерального переміщення зловмисника між сегментами.

Розповсюдження IoT, хмарних сервісів, віддаленої роботи та практик «принеси свій пристрій» зробили концепцію жорсткого периметра не тільки недостатньою, а й архітектурно неадекватною новій реальності. Особистий смартфон працівника, IoT-принтер, бездротовий датчик або інтелектуальна камера можуть стати потенційним порталом для атаки [9]. Локалізація периметра втратила сенс, оскільки сам периметр перестав існувати у звичній формі. Природним відгуком на такий виклик стала концепція Zero Trust.

Архітектура нульової довіри (Zero Trust Architecture, ZTA) являє собою сучасний підхід до кібербезпеки, який виходить з аксіоми «припускай, що систему вже зламано» і відмовляє у довірі будь-якому суб'єкту, незалежно від його місця у мережі [4, 18]. Документ NIST SP 800-207 «Zero Trust Architecture» формалізує принципи нульової довіри і визначає три ключові логічні компоненти, які формують ядро архітектури: механізм політики (Policy Engine, PE), адміністратор політики (Policy Administrator, PA) та точка примусового застосування політики (Policy Enforcement Point, PEP) [22]. PE приймає рішення про надання доступу на основі аналізу множини сигналів – облікових даних суб'єкта, контексту запиту, стану безпеки пристрою, поведінкових патернів. PA транслює рішення у конкретні дії – видання короткотермінових облікових даних, формування правил для шлюзу. PEP розташований безпосередньо на шляху трафіку та забезпечує примусове виконання прийнятого рішення (дозвіл, заборона, повторна автентифікація).

Важливою особливістю архітектури нульової довіри є принцип мінімальних привілеїв (least privilege), відповідно до якого суб'єкт отримує лише той рівень доступу, який необхідний для виконання конкретного завдання.

Графічне зображення взаємодії компонентів показано на рис. 1.3.


Рис 1.3 – Базові принципи Zero Trust

Базові принципи Zero Trust, систематизовані у документі NIST SP 800-207 та узагальнені у вітчизняних дослідженнях [4, 16], охоплюють декілька взаємопов'язаних положень. Усі джерела даних та обчислювальні сервіси розглядаються як ресурси. Уся комунікація захищена незалежно від мережевого розташування. Доступ до окремих ресурсів надається на основі сесії. Доступ до ресурсів визначається динамічною політикою. Підприємство контролює та вимірює стан безпеки усіх своїх активів. Автентифікація та авторизація є динамічними та виконуються до надання доступу. Підприємство збирає максимально можливий обсяг інформації про поточний стан мережі та використовує його для покращення стану безпеки. Дотримання повного переліку наведених принципів формує цілісну архітектуру нульової довіри, у якій неможливе ані безконтрольне переміщення зловмисника, ані експлуатація прихованих довірчих відносин між елементами системи.

Імплементація Zero Trust у IoT-середовищах має ряд специфічних особливостей, які відрізняють її від реалізації для класичних користувацьких мереж. Через обмеженість ресурсів кінцевих пристроїв неможливо

застосовувати на них повноцінну багатофакторну автентифікацію або встановлювати агентів безпеки. Замість цього центр ваги переноситься на мережеву інфраструктуру, яка виконує роль PEP для всього IoT-сегмента [8]. Мікросегментація мережі через VLAN, динамічне призначення політик через RADIUS, профілювання пристроїв на рівні комутатора та централізована фільтрація трафіку через ACL формують той інфраструктурний шар, який реалізує принципи нульової довіри для пристроїв, що самі по собі такі принципи підтримати не здатні.

Cisco Packet Tracer як середовище імітаційного моделювання володіє інструментарієм, достатнім для побудови та верифікації системи захисту IoT-інфраструктури за принципами Zero Trust. Програма забезпечує підтримку IoT-пристроїв, моделей датчиків, виконавчих механізмів, мікроконтролерів, шлюзів «розумних» приміщень та сервера реєстрації [10]. Передбачена можливість програмування власних пристроїв мовами Python, JavaScript і Blockly, налаштування правил роботи. Усі стандартні мережеві засоби – комутатори, маршрутизатори, міжмережеві екрани, бездротові точки доступу – доступні у повному обсязі. Режим симуляції дозволяє покроково спостерігати за рухом пакетів через мережеву інфраструктуру, що особливо цінно для перевірки коректності правил мікросегментації.

Підприємство як предметна область даної кваліфікаційної роботи розглядається у вигляді абстрактної організації середнього масштабу з гетерогенною IoT-інфраструктурою. До складу типового IoT-середовища такого підприємства входять датчики кліматичного контролю в офісних приміщеннях, мережеві відеокамери системи безпеки, інтелектуальні шлюзи доступу, лічильники електроенергії та води, охоронна сигналізація, системи контролю доступу через електронні картки та біометрію. Сумарна кількість IoT-пристроїв у такій інфраструктурі коливається від кількох десятків до кількох сотень одиниць, що робить ручне адміністрування політик безпеки невиправдано

трудомістким і вимагає системного інженерного підходу до проєктування захисних механізмів.

## 1.2 Аналіз наявного програмно-апаратне забезпечення безпеки IotT-інфраструктури

Сучасний ринок рішень кібербезпеки для IoT-інфраструктур пропонує широкий спектр продуктів – від комплексних промислових платформ до спеціалізованих компонентів захисту окремих рівнів архітектури. Для коректного позиціонування проєктованої системи необхідно проаналізувати існуючі рішення, виявити їхні переваги та недоліки, визначити, що з них доцільно адаптувати до симуляційного середовища Cisco Packet Tracer.

Платформа Cisco Cyber Vision разом із Cisco Secure Equipment Access становить промислове рішення для забезпечення видимості, мікросегментації та захищеного віддаленого доступу до OT/ICS та промислових IoT-середовищ. Платформа використовує мережу як сенсор для виявлення усіх підключених пристроїв, аналізу їхньої поведінки та автоматичного формування політик мікросегментації відповідно до стандарту ISA/IEC 62443 [20]. Перевагами рішення є висока зрілість, інтеграція з решта продуктів Cisco, підтримка широкого переліку промислових протоколів, наявність глобальної бази сигнатур загроз. Обмеженням для прикладного впровадження на середньому підприємстві є висока вартість ліцензій та необхідність наявності штату спеціалізованих інженерів безпеки.

Microsoft Defender for IoT являє собою хмарне рішення з можливістю гібридного розгортання, яке забезпечує безперервний моніторинг IoT-пристроїв, виявлення аномалій поведінки та інтеграцію з Microsoft Sentinel для централізованого реагування на інциденти. У звіті Forrester Wave «Платформи нульової довіри» за III квартал 2025 року Microsoft визнано лідером ринку завдяки комплексності пропонованої екосистеми [15]. Сильною стороною

продукту є глибока інтеграція з ідентифікаційними сервісами Entra ID (раніше – Azure AD), реалізація принципу умовного доступу та підтримка автентифікації за сертифікатами для пристроїв, що її здатні підтримувати. Слабкою стороною є залежність від хмарної інфраструктури Microsoft, яка для частини українських підприємств є проблематичною з огляду на регуляторні обмеження щодо обробки даних.

Palo Alto Networks IoT Security використовує машинне навчання для профілювання IoT-пристроїв, виявлення аномалій та автоматичного формування політик безпеки. Платформа інтегрується з міжмережевими екранами наступного покоління Palo Alto, що дозволяє реалізувати мікросегментацію на рівні L7 з контекстною інформацією про тип та поведінку кожного пристрою. Перевагою рішення є висока точність ідентифікації пристроїв та автоматичне реагування на аномалії; недоліком – прив’язка до екосистеми Palo Alto та значна вартість впровадження.

SecureW2 Cloud RADIUS та аналогічні рішення для динамічного призначення VLAN та dACL через 802.1X-автентифікацію реалізують принципи Zero Trust на рівні мережевого доступу [23]. Стандарт IEEE 802.1X виконує роль початкової оцінки довіри, перевіряючи ідентичність пристрою до надання доступу до мережі, та формує основу для подальшого застосування політик ZTNA. Динамічні VLAN та завантажувані ACL запобігають латеральному переміщенню та обмежують доступ лише до санкціонованих ресурсів. Використання сертифікатів EAP-TLS усуває потребу в паролях, що захищає від фішингу та крадіжки облікових даних.

Open-source стек, побудований на FreeRADIUS, Suricata, OpenWRT та pfSense, надає можливість реалізації базового рівня Zero Trust без значних капітальних витрат. Перевагою такого підходу є повна прозорість усіх компонентів, можливість тонкого налаштування під специфіку конкретного підприємства, відсутність ліцензійних платежів. Обмеженням є вищі вимоги до

кваліфікації обслуговуючого персоналу та відсутність єдиної точки технічної підтримки.

Порівняльна характеристика основних розглянутих рішень за функціональними та економічними параметрами наведена у таблиці 1.2.

Таблиця 1.2 – Порівняльна характеристика рішень захисту IoT-інфраструктур

| Рішення | Мікросегментація | Профілювання пристроїв | Інтеграція з ZTA | Підтримка симуляції | Вартість впровадження |
|---|---|---|---|---|---|
| Cisco Cyber Vision + ISE | Автоматична на основі поведінки | Глибоке (L7, протоколи OT) | Повна (NIST SP 800-207) | Часткова (Packet Tracer + CML) | Висока |
| Microsoft Defender for IoT | Через Entra Conditional Access | Машинне навчання | Повна, лідер Forrester | Відсутня | Висока, підписка |
| Palo Alto IoT Security | Через NGFW | Машинне навчання | Часткова | Відсутня | Висока |
| SecureW2 Cloud RADIUS | Через 802.1X dVLAN | Базове | Через RADIUS-атрибути | Відсутня | Середня, підписка |

Кінець таблиці 1.2

| | | | | | |
|---|---|---|---|---|---|
| Open-source стек (FreeRADIUS + pfSense) | Ручне на основі VLAN/ACL | Обмежене | Базове | Часткова | Низька, без ліцензій |
| Базова реалізація у Cisco Packet Tracer | Ручне VLAN + ACL + AAA | Через профілі портів | Базова, демонстраційна | Повна | Безкоштовно (навчальне ПЗ) |

Аналіз наведеної таблиці дозволяє зробити декілька висновків концептуального характеру. Жодне з комерційних рішень не має повноцінного аналога в середовищі Cisco Packet Tracer, що робить неможливим відтворення продуктивних інсталяцій у симуляторі. Натомість Packet Tracer у повному обсязі підтримує базові механізми реалізації Zero Trust на мережевому рівні – VLAN, ACL, AAA через RADIUS, Port Security, WPA3, що складає мінімально достатній інструментарій для побудови архітектурної моделі. Така модель здатна виконувати дві функції: верифікаційну (підтвердження принципової правильності проєктних рішень) та навчально-методичну (демонстрація принципів Zero Trust у контрольованому середовищі).

Окремої уваги заслуговують напрацювання вітчизняних дослідників. Робота Б.О. Маньковського, В.О. Довбняка та І.Р. Опірського [8] обґрунтовує можливість застосування Zero Trust у сфері IoT та аналізує реалізації від Microsoft, Google BeyondCorp, AWS, Cisco, з акцентом на мікросегментацію, багатофакторну автентифікацію, поведінковий аналіз і регуляторну відповідність. Стаття О.І. Городицького та І.Р. Опірського [5] пропонує покроковий підхід до імплементації Zero Trust у гібридних архітектурах корпоративної безпеки з виокремленням рівнів зрілості від базової сегментації до самовідновлюваних систем з квантово-стійкою криптографією. Дослідження

В.О. Абрамова, О.М. Глушак та А.Ю. Плохої [1] детально описує проєктування мережевої інфраструктури з урахуванням вимог кібербезпеки на базі обладнання Cisco з застосуванням концепції Security-by-Design, мікросегментації через дев'ять VLAN, локальної автентифікації, ACL та WPA3.

Робота В. Яскевича та Ю. Яскевича [16] систематизує логічні компоненти архітектури нульової довіри та підходи до її запровадження, виокремлюючи перевірку ідентичності, мінімізацію привілеїв, мікросегментацію, шифрування даних і відсутність прихованої довіри як ключові принципи. Дослідження Р.М. Минайленка та Л.І. Поліщук [9] підкреслює, що застосування архітектури довіри нульового рівня вимагає визначення та класифікації всіх ресурсів мережі, дозволяє контролювати доступ співробітників і зменшує ризики атак, орієнтованих на периметр.

Аналіз згаданих джерел та їх співставлення дозволяє виокремити сукупність елементів, які мають бути присутніми у проєктованій системі: чітке визначення усіх ресурсів та їх класифікація за ролями; розподіл мережі на ізольовані сегменти за принципом найменших привілеїв; контроль доступу між сегментами через ACL з логікою «default deny»; автентифікація пристроїв та користувачів засобами AAA-сервера; шифрування трафіку у бездротовому сегменті засобами WPA3; обмеження доступу до фізичних портів через Port Security; централізоване ведення журналів подій безпеки.

## 1.3 Аналіз вимог до системи безпеки на основі Zero Trust та формування технічоного завдання

На основі результатів дослідження предметної області та порівняльного аналізу наявних рішень формується сукупність вимог до проєктованої системи безпеки IoT-інфраструктури підприємства. Вимоги розподілено на функціональні та нефункціональні відповідно до настанов методичних рекомендацій з виконання кваліфікаційної роботи.

Функціональні вимоги визначають перелік функцій, які має реалізовувати система:

– виконувати логічну сегментацію корпоративної мережі на ізольовані VLAN відповідно до ролі активів (управління, корпоративні користувачі, IoT-сенсори, IoT-камери, гостьова мережа, серверний сегмент, сегмент брокера IoT);

– забезпечувати фільтрацію міжсегментного трафіку через розширені ACL з логікою «дозволено лише явно описане» (default deny);

– реалізовувати автентифікацію адміністраторів через AAA-сервер з протоколом RADIUS;

– реалізовувати шифрування бездротового сегмента через WPA3-Enterprise;

– обмежувати кількість MAC-адрес на портах доступу через Port Security з режимом violation = restrict або shutdown;

– забезпечувати ведення журналів подій безпеки через syslog-сервер;

– забезпечувати функціонування IoT-пристроїв (датчиків температури, задимлення, руху, вологості, відеокамер) у межах виділеного для них VLAN;

– забезпечувати взаємодію IoT-пристроїв із сервером управління (брокером) лише через дозволені правилами ACL канали.

Нефункціональні вимоги визначають характеристики системи, що не пов’язані безпосередньо з її функціональністю:

– модель має бути реалізована в середовищі Cisco Packet Tracer версії 8.2 або вище з метою забезпечення відтворюваності та можливості демонстрації під час захисту;

– загальна кількість логічних сегментів – не менше семи;

– кількість IoT-пристроїв у моделі – не менше десяти, з охопленням принаймні трьох різних типів (датчики, виконавчі механізми, мережеві камери);

– конфігурація мережевого обладнання має дозволяти розширення без архітектурних змін;

– модель має дозволяти проведення тестів на спробу несанкціонованого доступу між сегментами з очікуваним результатом «доступ заборонено».

Сукупність функціональних та нефункціональних вимог зведено у таблицю 1.3.

Таблиця 1.3-Зведені вимоги до системи безпеки IoT-інфраструктури

| Категорія | Вимога | Спосіб перевірки |
|---|---|---|
| Функціональна | Сегментація мережі на VLAN за ролями | Перевірка таблиці VLAN на комутаторах |
| Функціональна | Фільтрація міжсегментного трафіку через ACL | Тест ping/tracert між сегментами |
| Функціональна | Автентифікація адміністраторів через AAA | Спроба входу з/без облікових даних |
| Функціональна | Шифрування бездротового сегмента WPA3 | Перевірка налаштувань точки доступу |
| Функціональна | Port Security на портах доступу | Підключення стороннього пристрою |
| Функціональна | Ведення журналів подій | Перевірка syslog-повідомлень |
| Функціональна | Контрольована взаємодія IoT з брокером | Тест MQTT-обміну через дозволений порт |
| Нефункціональна | Реалізація у Cisco Packet Tracer 8.2+ | Запуск файлу проєкту |
| Нефункціональна | Не менше 7 VLAN | Підрахунок у конфігурації |
| Нефункціональна | Не менше 10 IoT-пристроїв 3+ типів | Інспекція моделі |

Кінець таблиці 1.3

| | | |
|---|---|---|
| Нефункціональна | Розширюваність без архітектурних змін | Експертна оцінка |
| Нефункціональна | Тести несанкціонованого доступу | Серія перевірок з очікуваним «deny» |

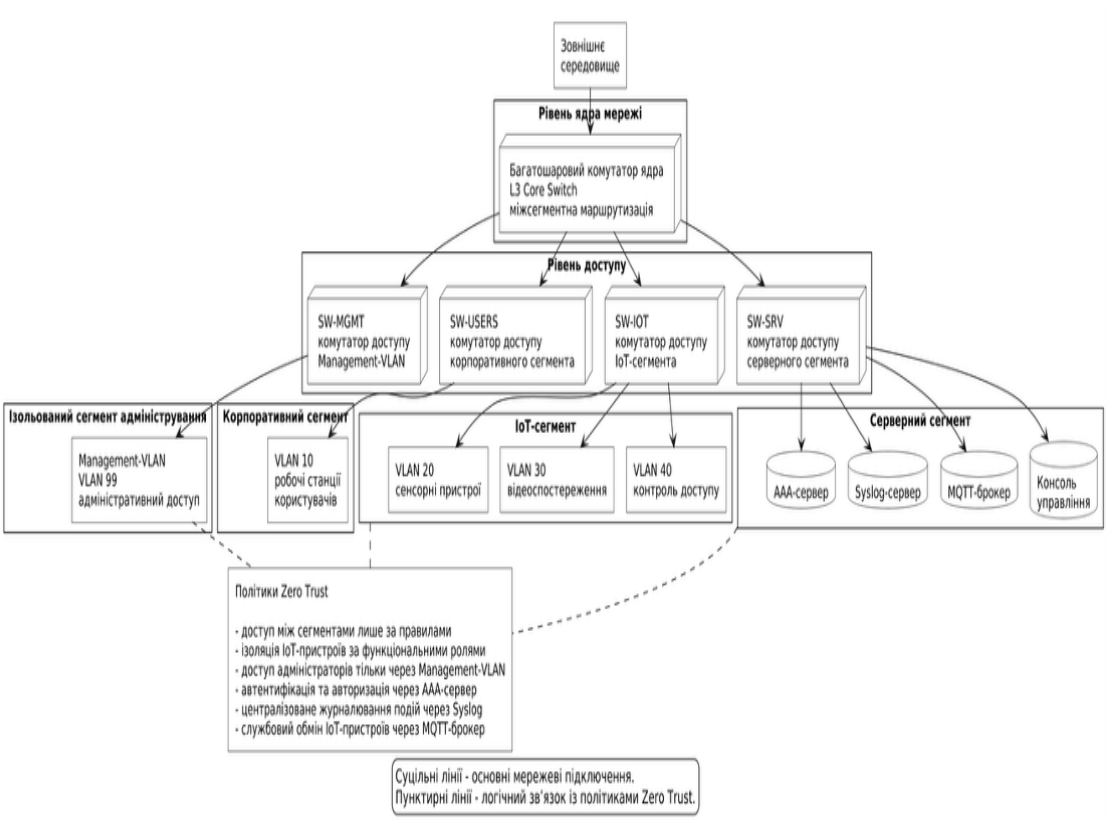



Рисунок 1.4 – Цільова архітектура мережі підприємства з мікросегментацією на основі Zero Trust»

Архітектура передбачає наявність ядра мережі на базі багатошарового комутатора з функціями міжсегментної маршрутизації, до якого підключено комутатори доступу для кожного функціонального сегмента. Сегмент IoT-пристроїв ізольовано в окремих VLAN з різною роллю (сенсорний, відеоспостереження, контроль доступу). Серверний сегмент містить AAA-сервер, syslog-сервер, MQTT-брокер для IoT-пристроїв і консоль управління.

Доступ адміністраторів до управління мережею здійснюється з виділеного management-VLAN, який ізольовано від решти трафіку.

Сукупність наведених в підрозділі вимог формує основу для розробки технічного завдання та подальшого проєктування системи. Деталізована постановка задачі для другого розділу полягає у тому, щоб на основі сформульованих вимог розробити логічну структуру мережі, спроєктувати схему адресації, визначити склад правил ACL для кожного напряму міжсегментного трафіку, обрати конкретні моделі обладнання Cisco Packet Tracer для реалізації та підготувати специфікацію конфігурації для кожного пристрою.

## 1.4 Висновки до перешого розділу

Виконано аналіз предметної області IoT-інфраструктури підприємства, у результаті якого встановлено, що поширення IoT-пристроїв сформувало якісно нове середовище, у якому традиційна модель периметрового захисту втратила свою функціональність. Гетерогенність кінцевих пристроїв з обмеженими ресурсами, відсутність уніфікованих механізмів автентифікації та неможливість застосування агентів моніторингу на більшості IoT-пристроїв змушують переносити основне навантаження безпеки на мережеву інфраструктуру.

Систематизовано основні класи загроз IoT-середовищам підприємства за рівнями архітектури – від фізичних загроз сенсорам до атак на API застосунків. Найвразливішим визначено мережевий рівень, який одночасно виявився тим рівнем, на якому інфраструктурні засоби дозволяють реалізувати найбільш ефективні захисні механізми. Прецедент ботнету Mirai продемонстрував, що навіть базові вразливості (заводські паролі) здатні породжувати кампанії гігантського масштабу.

Розглянуто концепцію Zero Trust у викладі документа NIST SP 800-207, проаналізовано її логічні компоненти (PE, PA, PEP) та основні принципи.

Обґрунтовано, що для IoT-середовищ ефективною є реалізація Zero Trust через інфраструктурні засоби: мікросегментацію на рівні VLAN, динамічне призначення політик через RADIUS, контроль міжсегментного трафіку через ACL та шифрування бездротового сегмента засобами WPA3.

Виконано порівняльний аналіз наявних комерційних та open-source рішень захисту IoT-інфраструктур (Cisco Cyber Vision, Microsoft Defender for IoT, Palo Alto IoT Security, SecureW2 Cloud RADIUS, FreeRADIUS-стек), визначено їх переваги, обмеження та ступінь застосовності у середовищі імітаційного моделювання. Встановлено, що Cisco Packet Tracer у повному обсязі підтримує базові механізми реалізації Zero Trust на мережевому рівні і може використовуватись як для верифікації архітектурних рішень, так і для навчально-методичних цілей.

Сформульовано функціональні та нефункціональні вимоги до проєктованої системи, що склали основу для технічного завдання. Окреслено цільову архітектуру мережі підприємства з мікросегментацією на сім VLAN, виділенням серверного, корпоративного, IoT, гостьового та management-сегментів, із застосуванням ACL з логікою «default deny», AAA через RADIUS, WPA3-Enterprise, Port Security та централізованого ведення журналів через syslog-сервер.

Окреслена постановка задачі для подальших розділів передбачає розробку логічної структури мережі, схеми адресації, специфікації правил ACL та конфігурації мережевого обладнання, реалізацію моделі у Cisco Packet Tracer та проведення серії тестів на відповідність технічному завданню.

# 2 ПРОЄКТУВАННЯ СИСТЕМИ БЕЗПЕКИ IOT-ІНФРАСТРУКТУРИ НА ОСНОВІ КОНЦЕПЦІЇ ZERO TRUST

## 2.1 Архітектурне рішення мережі підприємства з мікросегментацією

Проєктування архітектури мережі підприємства з вираженим IoT-сегментом потребує системного підходу до розподілу мережевих ресурсів за функціональним призначенням. Результати аналізу, виконаного у першому розділі, засвідчили, що мережевий рівень є оптимальним для реалізації базових принципів Zero Trust у середовищах з обмеженими обчислювальними ресурсами кінцевих пристроїв [8]. Відповідно до сформульованих функціональних вимог, архітектура має забезпечувати логічну ізоляцію щонайменше семи сегментів із контрольованим міжсегментним обміном даними.

Обрана топологія побудована за ієрархічним принципом із виділенням ядра мережі, рівня агрегації та рівня доступу. Ядром мережі виступає маршрутизатор Cisco 2911 (CORE-R1), який виконує функції міжсегментної маршрутизації через субінтерфейси та централізованої фільтрації трафіку засобами розширених ACL. Граничний маршрутизатор Cisco ISR4321 (EDGE-R1) забезпечує з'єднання корпоративної мережі з мережею Інтернет через об'єкт Cloud-PT. Рівень доступу представлено трьома комутаторами Cisco 2960-24TT: ACC-CORP-SW1 обслуговує корпоративний сегмент та бездротову інфраструктуру, ACC-IOT-SW1 агрегує IoT-пристрої трьох категорій, MGMT-SW1 забезпечує підключення серверного та управлінського сегментів.

Для забезпечення логічної сегментації мережі та підвищення рівня безпеки використано VLAN-технології, що дозволяють ізолювати трафік між корпоративним, IoT та управлінським сегментами.

Також у мережі передбачено механізми резервування та відмовостійкості, що дозволяє мінімізувати вплив можливих збоїв і забезпечити безперервність надання сервісів. Добре, ось розширене доповнення у тому ж стилі — просто додаєш після свого тексту:

Додатково в архітектурі передбачено централізоване управління адресним простором із використанням уніфікованої схеми IP-адресації для всіх сегментів, що спрощує ідентифікацію вузлів, оптимізує маршрутизацію та знижує складність адміністрування мережі.

Маршрутизація між VLAN реалізується на рівні ядра мережі із застосуванням субінтерфейсів, що дозволяє забезпечити централізований контроль трафіку та впровадження політик безпеки відповідно до функціонального призначення сегментів.

Для кожного сегмента визначено чіткі правила міжсегментної взаємодії, що обмежують доступ лише до необхідних ресурсів і сервісів, мінімізуючи площу потенційної атаки.

Окрема увага приділяється сегментації IoT-пристроїв, які згруповані за функціональними категоріями та розміщені в ізольованих VLAN із суворо обмеженим доступом до корпоративних ресурсів. Такий підхід дозволяє знизити ризик компрометації всієї мережі у випадку вразливості окремих пристроїв.Використання транкових з’єднань між комутаторами та маршрутизатором забезпечує ефективну передачу тегованого трафіку кількох VLAN через обмежену кількість фізичних інтерфейсів, що оптимізує використання мережевої інфраструктури.

Для підвищення рівня безпеки застосовано розширені списки контролю доступу (ACL), які фільтрують трафік на основі IP-адрес, протоколів та портів, забезпечуючи реалізацію принципу найменших привілеїв. ACL застосовуються на вхідних інтерфейсах субінтерфейсів маршрутизатора, що дозволяє блокувати небажаний трафік ще до його поширення мережею. Іменування списків доступу здійснюється відповідно до напрямків трафіку та типів взаємодії, що спрощує їх подальше обслуговування та аудит.

У мережі також реалізовано механізми контролю широкомовного трафіку, що дозволяє зменшити навантаження на сегменти та підвищити загальну

продуктивність системи. Застосування VLAN сприяє локалізації широкомовних доменів, що є особливо важливим для мереж із великою кількістю IoT-пристроїв.

З метою підвищення відмовостійкості передбачено резервування критичних елементів мережевої інфраструктури, а також можливість швидкого відновлення роботи у разі збоїв. Архітектура підтримує масштабування за рахунок додавання нових VLAN та сегментів без суттєвого впливу на існуючу структуру мережі.

Крім того, передбачено використання засобів моніторингу та журналювання мережевих подій, що дозволяє здійснювати аналіз трафіку, виявляти аномалії та своєчасно реагувати на інциденти безпеки. Це забезпечує підвищення рівня прозорості функціонування мережі та спрощує процес її адміністрування.

Таким чином, запропоноване архітектурне рішення поєднує ієрархічну модель побудови мережі з принципами мікросегментації та Zero Trust, що дозволяє забезпечити високий рівень безпеки, гнучкість і ефективність функціонування корпоративної мережі з інтегрованим IoT-середовищем.

Важливим елементом архітектури є розмежування площин керування та передачі даних, що дозволяє ізолювати службовий трафік від користувацького та підвищити стійкість мережі до атак. Управлінський доступ до мережевих пристроїв здійснюється через окремий сегмент із обмеженим колом дозволених адрес, що знижує ризик несанкціонованого втручання в конфігурацію інфраструктури.

Додатково реалізовано політики контролю доступу до мережі на рівні портів комутаторів, що дозволяє обмежити підключення неавторизованих пристроїв і підвищити рівень фізичної безпеки. Такий підхід є особливо актуальним для середовищ із великою кількістю IoT-вузлів, які можуть підключатися до мережі у різних точках.

Загальну топологію мережі показано на рис. 2.1.

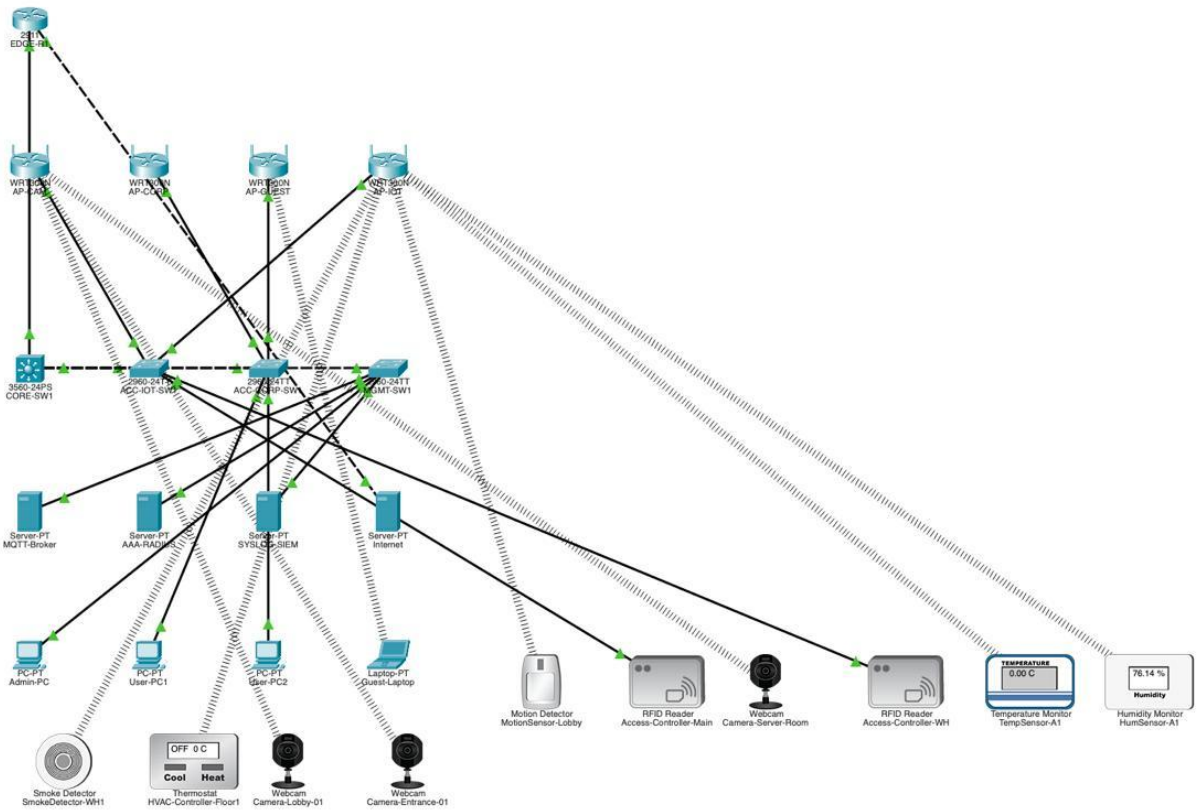



Рисунок 2.1 – Фізична топологія мережі підприємства у середовищі Cisco Packet Tracer

Архітектурним рішенням є мікросегментація мережі через віртуальні локальні мережі (VLAN), що дозволяє реалізувати принцип найменших привілеїв на канальному рівні моделі OSI. Кожному функціональному класу пристроїв присвоєно окремий VLAN із власною підмережею IPv4 та чітко визначеними правилами міжсегментного обміну.

Обмін трафіком між сегментами обмежується за допомогою списків контролю доступу (ACL), які реалізують політики доступу відповідно до ролей пристроїв.

Для службових і управлінських процесів виділено окремий VLAN, що дозволяє ізолювати критичну інфраструктуру від користувацького та IoT-трафіку.

Така організація адресного простору сприяє підвищенню безпеки, зменшенню широкомовного трафіку та оптимізації роботи мережі в цілому.

Додатково в межах кожного VLAN реалізовано чітку ієрархію адресного простору, що дозволяє ефективно групувати пристрої за функціональним призначенням і спрощує подальше адміністрування мережі. Такий підхід також полегшує впровадження політик безпеки, оскільки правила доступу можуть застосовуватися до цілих підмереж, а не до окремих вузлів.

Маршрутизація між сегментами виконується централізовано, що дає можливість здійснювати повний контроль над потоками даних і забезпечує прозорість мережевої взаємодії. Усі міжсегментні з'єднання проходять через вузол ядра, де відбувається перевірка трафіку на відповідність встановленим політикам безпеки.

Важливим аспектом є мінімізація площі атаки за рахунок обмеження доступу між сегментами лише до необхідних сервісів і протоколів. Це дозволяє значно знизити ризик горизонтального поширення загроз у разі компрометації окремого сегмента.

Крім того, у мережі реалізовано розмежування доступу до ресурсів залежно від типу пристроїв, що особливо актуально для IoT-середовища, де пристрої часто мають обмежені можливості захисту. Для таких пристроїв встановлюються більш жорсткі обмеження доступу та ізоляція від критичних компонентів інфраструктури.

Застосування VLAN також сприяє оптимізації мережевого трафіку за рахунок зменшення обсягу широкомовних повідомлень у межах кожного сегмента, що позитивно впливає на продуктивність мережі в цілому. Це особливо важливо у середовищах із великою кількістю підключених пристроїв.

Для підвищення рівня керованості передбачено використання систем моніторингу та аналізу трафіку, які дозволяють відслідковувати стан мережі, виявляти перевантаження та оперативно реагувати на інциденти. Отримані дані можуть використовуватися для подальшої оптимізації конфігурації мережі.

Також враховано можливість подальшого розширення мережі шляхом додавання нових VLAN та сегментів без суттєвої зміни існуючої структури. Це

забезпечує гнучкість архітектури та її адаптивність до зростаючих вимог підприємства.

У цілому, запропонований підхід до мікросегментації забезпечує високий рівень ізоляції, контрольованість мережевих взаємодій та відповідність сучасним вимогам до інформаційної безпеки в умовах інтеграції IoT-технологій. Схему розподілу VLAN та IP-адресації подано у таблиці 2.1.

Таблиця 2.1-Схема VLAN та IP-адресації мережі підприємства

| VLAN ID | Назва сегмента | Підмережа | Шлюз за замовчуванням | Призначення |
|---|---|---|---|---|
| 10 | Corporate | 192.168.10.0/24 | 192.168.10.1 | Робочі станції корпоративних користувачів |
| 20 | IoT-Sensors | 192.168.20.0/24 | 192.168.20.1 | Датчики температури, вологості, руху, задимлення, HVAC |
| 21 | IoT-Cameras | 192.168.21.0/24 | 192.168.21.1 | IP-камери відеоспостереження |
| 22 | IoT-Access | 192.168.22.0/24 | 192.168.22.1 | Контролери системи контролю доступу |
| 30 | Servers | 192.168.30.0/24 | 192.168.30.1 | AAA-RADIUS, Syslog/SIEM, MQTT-брокер |
| 40 | Guest | 192.168.40.0/24 | 192.168.40.1 | Гостьова бездротова мережа |
| 99 | Management | 192.168.99.0/24 | 192.168.99.1 | Адміністративний доступ до обладнання |

Принциповою відмінністю обраної архітектури від класичного підходу є розділення IoT-пристроїв на три окремих VLAN замість розміщення усіх IoT-вузлів в одному широкомовному домені. Датчики (VLAN 20), камери (VLAN 21) та контролери доступу (VLAN 22) ізольовані одне від одного, що унеможливлює латеральне переміщення зловмисника між підкатегоріями IoT у разі компрометації одного пристрою. Такий підхід відповідає рекомендаціям NIST SP 800-207 щодо мінімізації зони впливу інциденту [22] та узгоджується з висновками Б. О. Маньковського, В. О. Довбняка та І. Р. Опірського про доцільність гранулярної сегментації IoT-середовищ [8].

Серверний сегмент (VLAN 30) розміщує три ключових компоненти інфраструктури безпеки: AAA-RADIUS-сервер (192.168.30.10), який виконує функції механізму політики та адміністратора політики у термінології NIST SP 800-207; Syslog/SIEM-сервер (192.168.30.20), що забезпечує централізоване збирання та аналіз подій безпеки; MQTT-брокер (192.168.30.30), через який IoT-пристрої передають телеметричні дані. Розміщення усіх серверних компонентів в окремому VLAN з обмеженим доступом реалізує принцип захисту площини управління, що є необхідною умовою побудови архітектури нульової довіри [16].

Додатково для кожного IoT-сегмента визначено обмежений перелік дозволених напрямків взаємодії, зокрема доступ лише до MQTT-брокера та серверів автентифікації, що мінімізує можливість несанкціонованих з’єднань. Така модель комунікації відповідає принципу «deny by default», коли весь трафік заборонено, окрім явно дозволеного.

Використання окремих VLAN для різних категорій IoT-пристроїв також дозволяє враховувати специфіку їхнього мережевого навантаження та поведінкових характеристик. Наприклад, відеокамери генерують значний обсяг трафіку, тоді як датчики передають невеликі пакети з певною періодичністю, що дає змогу оптимізувати політики обробки трафіку для кожного сегмента.

Серверний сегмент, окрім функцій безпеки, виступає централізованим вузлом обробки та зберігання даних, отриманих від IoT-пристроїв. Обмеження

доступу до цього сегмента лише з визначених VLAN значно знижує ризик компрометації критичних сервісів.

Інтеграція AAA-сервера забезпечує централізовану автентифікацію та авторизацію користувачів і пристроїв, що дозволяє реалізувати контроль доступу на основі ролей. Це створює передумови для впровадження більш складних політик безпеки, зокрема динамічного надання доступу залежно від контексту.

Збирання подій на Syslog/SIEM-сервері дозволяє здійснювати кореляцію подій та виявлення підозрілої активності в різних сегментах мережі. Це підвищує рівень видимості мережевих процесів і забезпечує можливість оперативного реагування на інциденти безпеки.

Використання MQTT-брокера як єдиного каналу взаємодії IoT-пристроїв із серверною частиною дозволяє централізувати обмін даними та контролювати інформаційні потоки. Це також спрощує реалізацію політик фільтрації та моніторингу трафіку.

Таким чином, поєднання гранулярної сегментації IoT-середовища з централізованими сервісами безпеки формує цілісну архітектуру, яка відповідає сучасним вимогам до захисту розподілених інформаційних систем.

Адресацію конкретних пристроїв у межах кожного сегмента подано у таблиці 2.2.

Таблиця 2.2 – Адресація пристроїв мережі

| Пристрій | VLAN | IP-адреса | Примітка |
|---|---|---|---|
| User-PC1 | 10 | 192.168.10.10 | Робоча станція |
| User-PC2 | 10 | 192.168.10.11 | Робоча станція |
| TempSensor-A1 | 20 | 192.168.20.10 | Датчик температури |
| HumSensor-A1 | 20 | 192.168.20.11 | Датчик вологості |
| MotionSensor-Lobby | 20 | 192.168.20.12 | Датчик руху |

Кінець таблиці 2.2

| | | | |
|---|---|---|---|
| SmokeDetector-WH1 | 20 | 192.168.20.13 | Датчик задимлення |
| HVAC-Controller-Floor1 | 20 | 192.168.20.14 | Контролер кліматичної системи |
| Camera-Lobby-01 | 21 | 192.168.21.10 | IP-камера холу |
| Camera-Entrance-01 | 21 | 192.168.21.11 | IP-камера входу |
| Camera-Server-Room | 21 | 192.168.21.12 | IP-камера серверної кімнати |
| Access-Controller-Main | 22 | 192.168.22.10 | Контролер доступу головний |
| Access-Controller-WH | 22 | 192.168.22.11 | Контролер доступу складу |
| AAA-RADIUS | 30 | 192.168.30.10 | Сервер автентифікації |
| SYSLOG/SIEM | 30 | 192.168.30.20 | Сервер журналювання |
| MQTT Broker | 30 | 192.168.30.30 | Брокер IoT-повідомлень |
| Guest-Laptop | 40 | DHCP | Гостьовий пристрій |
| Admin-PC | 99 | 192.168.99.10 | Консоль адміністратора |

Бездротова інфраструктура представлена контролером бездротових мереж WLC-ZT та двома точками доступу. Точка AP-CORP транслює SSID «NT-CORP» із шифруванням WPA3-Enterprise та автентифікацією через RADIUS-сервер, що забезпечує індивідуальну верифікацію кожного бездротового клієнта перед наданням доступу до корпоративного VLAN 10. Точка AP-GUEST транслює SSID «NT-GUEST» для гостьового сегмента VLAN 40 з обмеженим доступом лише до мережі Інтернет.

Взаємозв'язок між фізичною топологією та логічною сегментацією реалізовано через механізм транкових з'єднань (IEEE 802.1Q) між комутаторами рівня доступу та маршрутизатором ядра. На порту маршрутизатора CORE-R1, що підключений до комутатора ACC-IOT-SW1, створено субінтерфейси GigabitEthernet0/0.20, GigabitEthernet0/0.21 та GigabitEthernet0/0.22, кожен з яких інкапсулює трафік відповідного VLAN та виступає шлюзом за замовчуванням для пристроїв сегмента. Аналогічну конфігурацію застосовано для

корпоративного, серверного, гостьового та управлінського сегментів. Логічну схему транкових з'єднань та субінтерфейсів

Транкові з’єднання забезпечують передачу тегованого трафіку кількох VLAN через один фізичний інтерфейс, що підвищує ефективність використання мережевих ресурсів.

Такий підхід забезпечує централізоване управління трафіком і спрощує впровадження політик безпеки між сегментами мережі.

## 2.2 Проєктування політик доступу, автентифікації та шифрування

Реалізація принципу «default deny» передбачає, що жоден міжсегментний трафік не дозволяється без явного правила у списку контролю доступу. На маршрутизаторі CORE-R1 розширені ACL застосовуються до вхідного трафіку на субінтерфейсі, що відповідає позиції точки примусового застосування політики (PEP) у архітектурі NIST SP 800-207 [22]. Матрицю дозволених міжсегментних взаємодій подано у таблиці 2.3.

Таблиця 2.3-Матриця дозволених міжсегментних взаємодій

| Джерело → Призначення | VLAN 10 | VLAN 20 | VLAN 21 | VLAN 22 | VLAN 30 | VLAN 40 | VLAN 99 | Internet |
|---|---|---|---|---|---|---|---|---|
| VLAN 10 (Corporate) | – | ✗ | ✗ | ✗ | MQTT (1883) | ✗ | ✗ | HTTP/ HTTPS |
| VLAN 20 (Sensors) | ✗ | – | ✗ | ✗ | MQTT (1883) | ✗ | ✗ | ✗ |

Кінець таблиці 2.3

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| VLAN 21 (Cameras) | ✗ | ✗ | – | ✗ | MQTT (1883) | ✗ | ✗ | ✗ |
| VLAN 22 (Access) | ✗ | ✗ | ✗ | – | MQTT (1883) | ✗ | ✗ | ✗ |
| VLAN 30 (Servers) | ✗ | ✗ | ✗ | ✗ | – | ✗ | ✗ | NTP, DNS |
| VLAN 40 (Guest) | ✗ | ✗ | ✗ | ✗ | ✗ | – | ✗ | HTTP/HTTPS |
| VLAN 99 (Mgmt) | SSH | SSH | SSH | SSH | SSH, HTTPS | ✗ | – | ✗ |

Аналіз матриці дозволяє виділити декілька принципових рішень. IoT-сегменти (VLAN 20, 21, 22) мають право надсилати трафік виключно до MQTT-брокера на порт 1883 у серверному сегменті (VLAN 30). Жоден IoT-сегмент не має доступу до іншого IoT-сегмента, до корпоративного сегмента чи до мережі Інтернет. Такий підхід унеможливлює використання скомпрометованого IoT-пристрою як плацдарму для латерального переміщення або для участі у DDoS-атаках, що є прямою протидією сценарію ботнету Mirai [13]. Гостьовий сегмент (VLAN 40) має доступ виключно до Інтернету через HTTP/HTTPS, повністю ізольований від внутрішніх ресурсів. Адміністративний сегмент (VLAN 99) є єдиним, з якого дозволено SSH-доступ до мережевого обладнання та серверів, що реалізує принцип мінімізації привілеїв для площини управління [9, 16].

Кожному напряму міжсегментного обміну відповідає іменований розширений ACL, застосований на вхідному напрямку відповідного субінтерфейсу CORE-R1.

Іменовані ACL формуються з урахуванням принципу мінімально необхідного доступу та чітко визначених політик взаємодії між сегментами.Для підвищення прозорості адміністрування використовується структуроване іменування ACL відповідно до напрямків обміну.

Такий підхід забезпечує ефективний контроль доступу та зменшує ризик несанкціонованого проникнення між сегментами мережі.

Додатково політики доступу передбачають сувору фільтрацію трафіку за протоколами та портами, що дозволяє виключити можливість використання нетипових або небезпечних сервісів у межах мережі. Усі невизначені або несанкціоновані запити блокуються за замовчуванням, що відповідає моделі «default deny».Використання ACL на рівні маршрутизатора ядра дозволяє реалізувати централізовану точку контролю, де здійснюється перевірка кожного міжсегментного з'єднання. Це забезпечує узгодженість політик безпеки та спрощує їх подальше адміністрування і аудит.

Особливу роль відіграє ізоляція гостьового сегмента, яка повністю виключає доступ до внутрішніх ресурсів підприємства. Такий підхід дозволяє надавати доступ до мережі Інтернет стороннім користувачам без ризику для корпоративної інфраструктури.Адміністративний сегмент, у свою чергу, захищений додатковими обмеженнями, включаючи доступ лише з визначених робочих станцій та використання захищених протоколів управління. Це дозволяє знизити ризик компрометації облікових записів адміністраторів і несанкціонованого доступу до критичних компонентів мережі.

Крім того, застосування іменованих ACL із чіткою структурою дозволяє підвищити зрозумілість конфігурації та зменшити ймовірність помилок при внесенні змін. Це особливо важливо в умовах масштабування мережі або модифікації політик доступу.У проєктованій архітектурі також враховано можливість подальшого розширення матриці доступу, що дозволяє гнучко адаптувати політики безпеки до змінних вимог без необхідності кардинальної перебудови мережі.

Таким чином, реалізована система контролю доступу забезпечує високий рівень ізоляції сегментів, прозорість управління мережевими взаємодіями та ефективний захист від сучасних кіберзагроз, зокрема тих, що характерні для IoT-середовищ.Перелік ACL та їх призначення зведено у таблиці 2.4.

Таблиця 2.4-Перелік розширених ACL маршрутизатора CORE-R1

| Назва ACL | Субінтерфейс | Напрямок | Призначення |
|---|---|---|---|
| ACL-SENSORS-IN | Gi0/0.20 | in | Дозволити MQTT до брокера, заблокувати решту |
| ACL-CAMERAS-IN | Gi0/0.21 | in | Дозволити MQTT до брокера, заблокувати решту |
| ACL-ACCESS-IN | Gi0/0.22 | in | Дозволити MQTT до брокера, заблокувати решту |
| ACL-CORPORATE-IN | Gi0/1.10 | in | Дозволити HTTP/HTTPS назовні, MQTT до брокера |
| ACL-GUEST-IN | Gi0/1.40 | in | Дозволити HTTP/HTTPS лише назовні |
| ACL-SERVERS-IN | Gi0/2.30 | in | Дозволити відповіді MQTT, DNS, NTP, Syslog |
| ACL-MGMT-IN | Gi0/2.99 | in | Дозволити SSH до всіх сегментів, HTTPS до серверів |

Автентифікація адміністраторів мережевого обладнання реалізована через модель AAA (Authentication, Authorization, Accounting) із зовнішнім RADIUS-сервером. На кожному активному мережевому пристрої (CORE-R1, ACC-CORP-SW1, ACC-IOT-SW1, MGMT-SW1) налаштовано AAA-модель із методом автентифікації «group radius» та резервним «local». RADIUS-сервер (192.168.30.10) зберігає облікові записи адміністраторів і відповідає за верифікацію кожної спроби доступу до CLI обладнання через SSH. У разі недоступності RADIUS-сервера пристрій переходить на локальну автентифікацію із заздалегідь створеним обліковим записом [23].

Шифрування бездротового трафіку реалізовано через WPA3-Enterprise на точці доступу AP-CORP. Протокол WPA3 використовує SAE (Simultaneous Authentication of Equals) замість PSK, що усуває вразливість до офлайн-атак

перебором та забезпечує пряму секретність (forward secrecy) [1]. У конфігурації Cisco Packet Tracer бездротовий контролер WLC-ZT координує роботу точок доступу та забезпечує передачу автентифікаційних запитів до RADIUS-сервера.

Механізм Port Security на комутаторах рівня доступу обмежує кількість MAC-адрес, дозволених на кожному порту. Для портів, до яких підключено IoT-пристрої, встановлено обмеження у одну MAC-адресу з режимом порушення «restrict», що блокує кадри від невідомих MAC-адрес та генерує Syslog-повідомлення без повного відключення порту. Для портів корпоративного сегмента застосовано режим «shutdown» з обмеженням у дві MAC-адреси, що забезпечує жорсткішу реакцію на спробу несанкціонованого підключення

Додатково механізм AAA забезпечує ведення журналів обліку (accounting), що дозволяє фіксувати всі дії адміністраторів під час роботи з мережевим обладнанням. Це підвищує рівень прозорості управління та створює можливість проведення аудиту дій у разі виникнення інцидентів безпеки.

Використання RADIUS-сервера як централізованого елемента автентифікації дозволяє уніфікувати політики доступу для всіх мережевих пристроїв та спростити процес керування обліковими записами. У разі необхідності зміни прав доступу або відкликання облікового запису це може бути виконано централізовано без внесення змін у конфігурацію кожного окремого пристрою.Шифрування бездротового трафіку із застосуванням WPA3-Enterprise у поєднанні з RADIUS-аутентифікацією забезпечує індивідуальну автентифікацію кожного користувача, що значно підвищує рівень захисту порівняно з підходами на основі спільних ключів. Це також дозволяє реалізувати контроль доступу до мережі на основі облікових даних користувача.

Централізоване управління бездротовою інфраструктурою через контролер дозволяє забезпечити узгодженість налаштувань безпеки, оперативне оновлення конфігурацій та контроль стану точок доступу. Це підвищує керованість мережі та спрощує її обслуговування.

Механізм Port Security додатково підсилює захист на канальному рівні, запобігаючи підключенню неавторизованих пристроїв до мережі. Використання різних режимів реагування дозволяє гнучко налаштовувати політики безпеки залежно від критичності сегмента.Згенеровані Syslog-повідомлення передаються до централізованого сервера журналювання, що забезпечує своєчасне виявлення порушень політик безпеки та дозволяє оперативно реагувати на інциденти.

Крім того, передбачено можливість інтеграції механізмів контролю доступу з іншими компонентами системи безпеки, що створює передумови для побудови комплексної системи захисту мережі підприємства.У цілому, поєднання AAA, WPA3-Enterprise та Port Security формує багаторівневу систему автентифікації та контролю доступу, яка відповідає сучасним вимогам до безпеки корпоративних мереж із підтримкою IoT. Параметри Port Security зведено у таблиці 2.5.

Таблиця 2.5-Параметри PORT-Security на комутаторах доступу

| Комутатор | Діапазон портів | Максимум MAC | Режим порушення | Sticky MAC |
|---|---|---|---|---|
| ACC-IOT-SW1 | Fa0/1 – Fa0/10 | 1 | restrict | Так |
| ACC-CORP-SW1 | Fa0/1 – Fa0/4 | 2 | shutdown | Так |
| ACC-CORP-SW1 | Fa0/5 – Fa0/6 (AP) | 10 | restrict | Hi |
| MGMT-SW1 | Fa0/1 – Fa0/3 | 1 | shutdown | Так |
| MGMT-SW1 | Fa0/4 (Admin-PC) | 1 | shutdown | Так |

Централізоване журналювання подій безпеки здійснюється через протокол Syslog. Кожен активний мережевий пристрій налаштовано на відправлення повідомлень рівня «warnings» (severity 4) та вище до Syslog/SIEM-сервера за адресою 192.168.30.20. Повідомлення Port Security, невдалі спроби

автентифікації AAA, спрацювання правил ACL (з ключовим словом «log») формують потік подій, який дозволяє виявляти аномалії та реконструювати хронологію інцидентів [5].

## 2.3 Розроблення логічної структури взаємодії компонентів у середовищі Cisco Packet Tracer

Середовище Cisco Packet Tracer версії 8.2.2 обрано як платформу реалізації на підставі порівняльного аналізу, виконаного у підрозділі 1.2. Підтримка IoT-компонентів (датчиків, виконавчих механізмів, мікроконтролерів, шлюзів), повноцінна реалізація VLAN, ACL, AAA, Port Security, WPA3 та режим симуляції з покроковою візуалізацією руху пакетів роблять Packet Tracer раціональним вибором для прототипування та верифікації архітектурних рішень [10].

Логічна структура взаємодії компонентів побудована за принципом розподілу відповідальності між трьома площинами: площиною даних (data plane), площиною управління (control plane) та площиною моніторингу (monitoring plane). На площині даних IoT-пристрої генерують телеметричні повідомлення MQTT та надсилають їх через комутатор ACC-IOT-SW1, транковий канал, маршрутизатор CORE-R1 та комутатор MGMT-SW1 до MQTT-брокера у серверному сегменті. На площині управління AAA-RADIUS-сервер обробляє запити автентифікації від мережевого обладнання та бездротового контролера.

Маршрут проходження MQTT-пакета від датчика температури TempSensor-A1 (192.168.20.10) до MQTT-брокера (192.168.30.30) складається з наступних кроків: пакет надходить на порт Fa0/1 комутатора ACC-IOT-SW1, тегується міткою VLAN 20, передається транковим каналом на інтерфейс Gi0/0 маршрутизатора CORE-R1, де його приймає субінтерфейс Gi0/0.20; маршрутизатор перевіряє пакет за правилами ACL-SENSORS-IN, підтверджує дозвіл на TCP-порт 1883 з призначенням 192.168.30.30, маршрутизує пакет через

субінтерфейс Gi0/2.30 на комутатор MGMT-SW1, звідки пакет доставляється до MQTT-брокера. Зворотний трафік проходить аналогічний шлях із перевіркою за ACL-SERVERS-IN.

У середовищі Cisco Packet Tracer IoT-пристрої програмуються засобами візуального редактора правил або скриптовими мовами. Для датчиків використано стандартні моделі Packet Tracer: Temperature Monitor, Humidity Monitor, Motion Detector, Smoke Detector та HVAC-контролер. Камери змодельовано через компонент IP Camera із налаштуванням статичної IP-адресації у відповідному VLAN. Контролери доступу представлено пристроями Door Lock та RFID Reader, об'єднаними через IoT-шлюз [10].

Додатково використання режиму симуляції в Cisco Packet Tracer дозволяє детально відстежувати проходження пакетів через усі рівні мережі, що є важливим для верифікації коректності налаштувань VLAN, ACL та маршрутів. Це забезпечує можливість виявлення помилок конфігурації ще на етапі проєктування та підвищує надійність кінцевого рішення.

Розподіл функцій між площинами data plane, control plane та monitoring plane дозволяє чітко структурувати мережеві процеси та ізолювати критичні механізми управління від користувацького трафіку. Такий підхід підвищує стійкість системи до атак та спрощує впровадження політик безпеки.

У площині моніторингу реалізовано централізоване збирання журналів подій та телеметрії, що дозволяє здійснювати аналіз поведінки мережі в режимі реального часу. Це забезпечує можливість виявлення аномалій, перевантажень та потенційних загроз на ранніх етапах їх виникнення.IoT-пристрої в середовищі Packet Tracer можуть бути налаштовані на генерацію подій за визначеними сценаріями, що дозволяє моделювати реальні умови експлуатації мережі. Це дає змогу оцінити вплив різних типів навантаження на продуктивність та безпеку інфраструктури. Використання статичної IP-адресації для ключових компонентів, таких як сервери та мережеве обладнання, забезпечує передбачуваність мережевої взаємодії та спрощує налаштування політик

доступу. Водночас для менш критичних пристроїв може застосовуватися динамічна адресація, що підвищує гнучкість системи.

Крім того, у моделі враховано можливість масштабування IoT-інфраструктури шляхом додавання нових пристроїв і сегментів без суттєвого впливу на існуючу конфігурацію. Це досягається завдяки використанню уніфікованих підходів до сегментації та адресації.

Таким чином, середовище Cisco Packet Tracer не лише дозволяє реалізувати запропоновану архітектуру, але й виступає ефективним інструментом для її тестування, аналізу та подальшого вдосконалення.

Специфікацію обладнання, обраного для реалізації моделі, подано у таблиці 2.6.

Таблиця 2.6-Специфікація менрежевого обладнання моделі (Джерело скаладання автором)

| Пристрій | Модель у Packet Tracer | Роль | Кількість інтерфейсів |
|---|---|---|---|
| CORE-R1 | Cisco 2911 | Маршрутизація, ACL, AAA | 3 × GigabitEthernet |
| EDGE-R1 | Cisco ISR4321 | Граничний маршрутизатор | 2 × GigabitEthernet |
| ACC-CORP-SW1 | Cisco 2960-24TT | Комутатор корпоративного сегмента | 24 × FastEthernet, 2 × GigabitEthernet |
| ACC-IOT-SW1 | Cisco 2960-24TT | Комутатор IoT-сегмента | 24 × FastEthernet, 2 × GigabitEthernet |
| MGMT-SW1 | Cisco 2960-24TT | Комутатор серверного/управлінського сегмента | 24 × FastEthernet, 2 × GigabitEthernet |
| WLC-ZT | WLC-PT | Контролер бездротових мереж | 1 × GigabitEthernet |

Кінець таблиці 2.6

| | | | |
|---|---|---|---|
| AP-CORP | AccessPoint-PT | Корпоративна точка доступу (WPA3) | 1 × FastEthernet |
| AP-GUEST | AccessPoint-PT | Гостьова точка доступу | 1 × FastEthernet |

## 2.4 Висновки до другого розділу

Спроєктовано архітектуру мережі підприємства з мікросегментацією на сім VLAN, яка розподіляє мережеві ресурси за функціональним призначенням: корпоративний сегмент, три підкатегорії IoT-пристроїв (датчики, камери, контролери доступу), серверний сегмент, гостьова мережа та сегмент управління. Розподіл IoT-пристроїв на три окремих VLAN замість одного широкомовного домену мінімізує зону впливу потенційного інциденту та унеможливлює латеральне переміщення між підкатегоріями IoT.

Розроблено матрицю міжсегментних взаємодій із логікою «default deny», на основі якої сформовано сім іменованих розширених ACL для маршрутизатора ядра. IoT-сегменти мають дозвіл на обмін даними виключно з MQTT-брокером через порт 1883, що позбавляє скомпрометовані IoT-вузли можливості атакувати інші сегменти або брати участь у DDoS-кампаніях.

Спроєктовано модель автентифікації адміністраторів через AAA/RADIUS із резервною локальною автентифікацією, шифрування бездротового сегмента через WPA3-Enterprise, захист портів доступу через Port Security зі sticky MAC-адресами та централізоване журналювання подій через Syslog. Визначено специфікацію обладнання Cisco Packet Tracer та логічну структуру потоків даних між площинами управління, даних та моніторингу.

Реалізовані рішення відповідають принципам архітектури нульової довіри, зокрема мінімізації привілеїв, сегментації мережі та постійного контролю доступу до ресурсів. Ізоляція сегментів та централізоване управління політиками

доступу забезпечують зменшення площі атаки та підвищують загальну стійкість мережі до кіберзагроз.

Запропонована архітектура демонструє ефективність поєднання ієрархічної моделі побудови мережі з мікросегментацією та сучасними механізмами контролю доступу. Це дозволяє досягти балансу між безпекою, продуктивністю та зручністю адміністрування мережевої інфраструктури.

Використання централізованих сервісів автентифікації, журналювання та обробки даних забезпечує високий рівень керованості та прозорості функціонування системи. Це створює передумови для впровадження розширених механізмів аналізу подій та автоматизованого реагування на інциденти безпеки.

Отримані результати можуть бути використані як основа для подальшого розвитку мережевої інфраструктури підприємства, зокрема для інтеграції з хмарними сервісами, впровадження систем виявлення вторгнень та розширення функціональності IoT-середовища.

Таким чином, другий розділ підтверджує доцільність обраного підходу до проєктування мережі та демонструє можливість практичної реалізації принципів Zero Trust у середовищі з обмеженими ресурсами IoT-пристроїв.

# 3 ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ ТА ТЕСТУВАННЯ СИСТЕМИ

## 3.1 Реалізація мережевої моделі у Cisco Packet Tracer

Реалізація мережевої моделі розпочинається з розміщення фізичних компонентів на робочому просторі Cisco Packet Tracer та з'єднання їх відповідними типами кабелів. Маршрутизатори CORE-R1 та EDGE-R1 з'єднано кабелем типу Serial DCE. Комутатори доступу підключено до CORE-R1 кабелями GigabitEthernet Copper. IoT-пристрої підключено до комутатора ACC-IOT-SW1 кабелями FastEthernet Copper. Серверні компоненти підключено до MGMT-SW1 аналогічним чином. Результат розміщення компонентів відповідає топології, показаній на рис. 2.1.

Базову конфігурацію кожного мережевого пристрою розпочато з налаштування імені хоста, банера попередження про несанкціонований доступ, шифрування паролів у конфігурації та вимкнення DNS-пошуку.

Фрагмент базової конфігурації маршрутизатора CORE-R1 має вигляд:

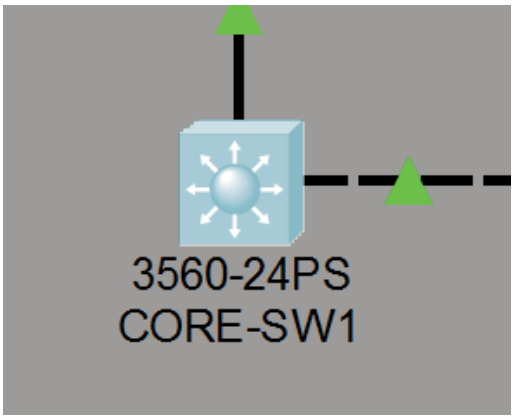



Рисунок 3.1 – Маршрутизатора CORE-R1 у середовищі Cisco Packet Tracer

```
hostname CORE-R1
banner motd #UNAUTHORIZED ACCESS PROHIBITED. All activity is monitored and logged.#
service password-encryption
```

```
no ip domain-lookup
enable secret 0 ZtR0$tC0re2025
```

Створення VLAN на комутаторах виконано через команди конфігурації VLAN-бази. Фрагмент конфігурації комутатора ACC-IOT-SW1:

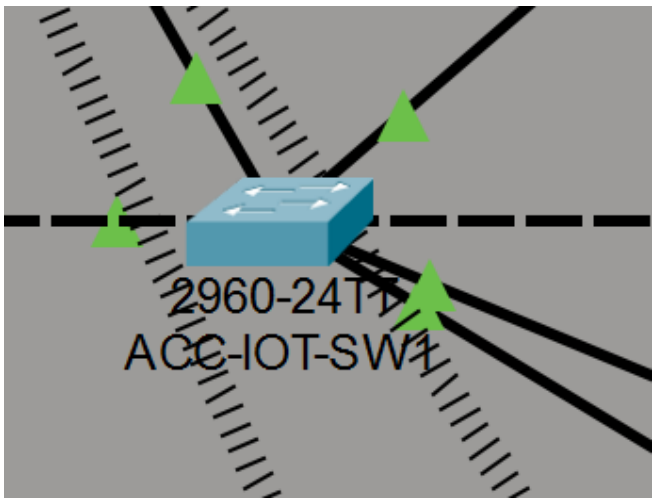



Рисунок 3.2 – маршрутизатора ACC-IOT-SW1 у середовищі Cisco Packet Tracer

```
vlan 20
 name IoT-Sensors
vlan 21
 name IoT-Cameras
vlan 22
 name IoT-Access
```

Аналогічно на комутаторі ACC-CORP-SW1 створено VLAN 10 (Corporate) та VLAN 40 (Guest), на MGMT-SW1 – VLAN 30 (Servers) та VLAN 99 (Management).

Порти доступу комутатора ACC-IOT-SW1 призначено відповідним VLAN згідно з таблицею 2.2.

Фрагмент конфігурації:

```
interface range FastEthernet0/1-5
 switchport mode access
```

```
 switchport access vlan 20
 description IoT-Sensors-Ports
 spanning-tree portfast
 no shutdown

interface range FastEthernet0/6-8
 switchport mode access
 switchport access vlan 21
 description IoT-Cameras-Ports
 spanning-tree portfast
 no shutdown

interface range FastEthernet0/9-10
 switchport mode access
 switchport access vlan 22
 description IoT-Access-Control-Ports
 spanning-tree portfast
 no shutdown
```

Транкове з'єднання між ACC-IOT-SW1 та CORE-R1 налаштовано з явним переліком дозволених VLAN, що запобігає поширенню небажаного широкомовного трафіку:

```
interface GigabitEthernet0/1
 switchport mode trunk
 switchport trunk allowed vlan 20,21,22
 description TRUNK-TO-CORE-R1
 no shutdown
```

На комутаторі ACC-CORP-SW1 транковий порт дозволяє VLAN 10 та 40:

```
interface GigabitEthernet0/1
 switchport mode trunk
 switchport trunk allowed vlan 10,40
 description TRUNK-TO-CORE-R1
 no shutdown
```

На MGMT-SW1 транковий порт дозволяє VLAN 30 та 99:

```
interface GigabitEthernet0/1
 switchport mode trunk
 switchport trunk allowed vlan 30,99
 description TRUNK-TO-CORE-R1
 no shutdown
```

Невикористані порти на всіх комутаторах деактивовано командою «shutdown» та призначено неіснуючому VLAN 999 (Dead-End) з метою запобігання несанкціонованому підключенню:

```
interface range FastEthernet0/11-24
 switchport mode access
 switchport access vlan 999
 shutdown
 description UNUSED-DISABLED
```

## 3.2 Конфігурація механізмів VLAN, ACL, AAA та Port Security

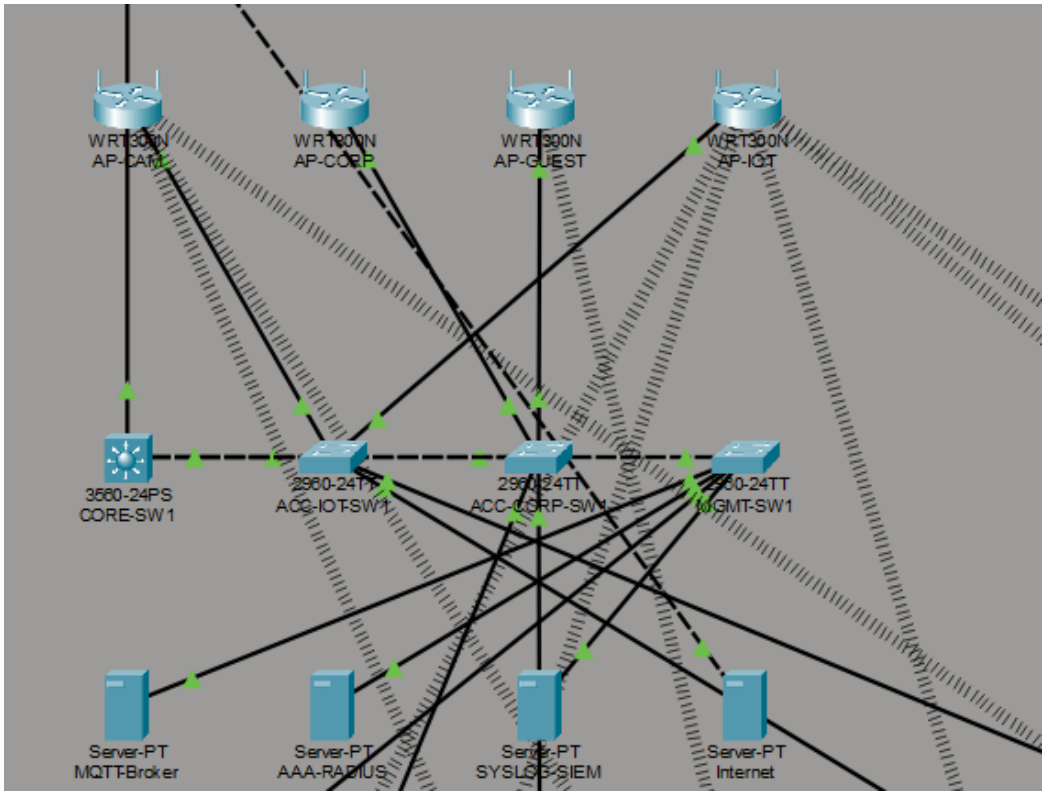



Рисунок 3.3 – Топологія серверів та маршрутизаторів

У межах реалізації проєктованої архітектури було виконано налаштування механізмів VLAN, ACL, AAA та Port Security на мережевому обладнанні.

На маршрутизаторі CORE-R1 реалізовано міжвланову маршрутизацію за допомогою технології субінтерфейсів із використанням інкапсуляції IEEE 802.1Q. Для кожного VLAN створено окремий субінтерфейс, якому призначено IP-адресу шлюзу за замовчуванням відповідного сегмента. Це дозволяє забезпечити логічне розділення трафіку та централізований контроль міжсегментної взаємодії. CORE-R1 можна побачити на рисунку 3.1

З'єднання між ядром мережі (CORE-R1) та граничним маршрутизатором (EDGE-R1) реалізовано у вигляді каналу «точка-точка» із використанням серійного інтерфейсу. EDGE-R1 виконує функцію виходу до мережі Інтернет, отримуючи IP-адресу динамічно, тоді як на CORE-R1 налаштовано маршрут за замовчуванням для спрямування зовнішнього трафіку.

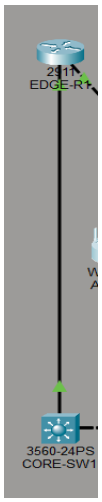



Рисунок 3.4 – Зєднання ядра з маршрутизатором

Контроль доступу між сегментами реалізовано за допомогою іменованих розширених списків контролю доступу (ACL), які створено відповідно до матриці взаємодій. Для кожного VLAN визначено власний ACL, що застосовується на вхідному напрямку відповідного субінтерфейсу маршрутизатора.

Політики доступу побудовано за принципом «заборонено все, окрім дозволеного», що забезпечує високий рівень ізоляції сегментів.

Для IoT-сегментів дозволено виключно передачу даних до MQTT-брокера на визначений порт, що унеможливлює будь-які інші мережеві взаємодії. Корпоративний сегмент має обмежений доступ до Інтернету та окремих внутрішніх сервісів, тоді як гостьовий сегмент повністю ізольований від внутрішніх ресурсів. Адміністративний сегмент має розширені привілеї доступу до мережевого обладнання через захищений протокол SSH.

Механізм автентифікації адміністраторів реалізовано за моделлю AAA із використанням зовнішнього RADIUS-сервера. Усі спроби доступу до мережевого обладнання перевіряються централізовано, а у разі недоступності сервера використовується резервна локальна автентифікація. Додатково реалізовано облік дій адміністраторів (accounting), що дозволяє вести аудит.

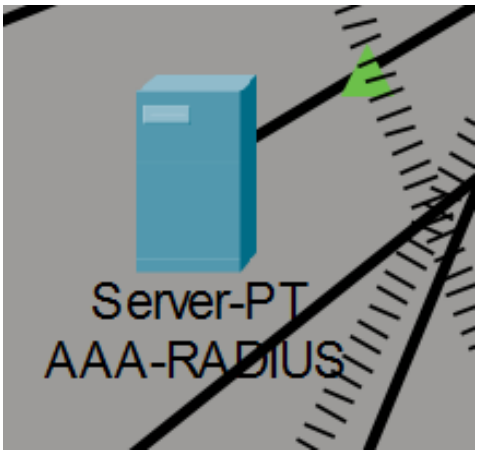



Рисунок 3.5 – Сервер (AAA-Radius)

Для захисту портів доступу на комутаторах використано механізм Port Security із прив’язкою MAC-адрес (sticky). Для IoT-портів встановлено обмеження на одну MAC-адресу з м’якою реакцією на порушення, тоді як у корпоративному сегменті застосовано більш жорстку політику з відключенням порту.

Централізоване журналювання подій реалізовано через Syslog-сервер, куди надсилаються повідомлення від маршрутизатора та комутаторів. Це забезпечує можливість моніторингу стану мережі та виявлення інцидентів безпеки.

Бездротовий доступ у корпоративному сегменті реалізовано із застосуванням WPA3-Enterprise (у Packet Tracer — WPA2-Enterprise) з автентифікацією через RADIUS-сервер. Для гостьової мережі використовується окремий SSID із попередньо спільним ключем та ізоляцією у VLAN 40.

## 3.3 Тестування працездатності та оцінка ефективності системи захисту

Тестування системи безпеки виконано за методикою функціонального тестування з метою підтвердження відповідності реалізації вимогам технічного завдання, сформульованим у підрозділі 1.3. Стратегія тестування побудована за принципом «чорної скриньки»: для кожної функціональної вимоги сформовано тестовий сценарій із визначеними вхідними даними та очікуваним результатом. Перелік тестових сценаріїв подано у таблиці 3.1.

Таблиця 3.1 – Тестові сценарії перевірки системи безпеки

| ID | Тестовий сценарій | Вхідні дані | Очікуваний результат |
|---|---|---|---|
| T-01 | Зв'язність IoT-сенсора з MQTT-брокером | ping 192.168.30.30 з TempSensor-A1 | Успішно (MQTT дозволено) |
| T-02 | Блокування IoT-сенсора до корпоративного сегмента | ping 192.168.10.10 з TempSensor-A1 | Невдало (ACL deny) |
| T-03 | Блокування IoT-сенсора до Інтернету | ping 8.8.8.8 з TempSensor-A1 | Невдало (ACL deny) |
| T-04 | Блокування між IoT-підсегментами | ping 192.168.21.10 з TempSensor-A1 | Невдало (ACL deny) |
| T-05 | Доступ корпоративного ПК до Інтернету | ping зовнішньої адреси з User-PC1 | Успішно |

Кінець таблиці 3.1

| | | | |
|---|---|---|---|
| T-06 | Блокування корпоративного ПК до IoT | ping 192.168.20.10 з User-PC1 | Невдало (ACL deny) |
| T-07 | Гостьовий доступ до Інтернету | HTTP-запит з Guest-Laptop | Успішно |
| T-08 | Блокування гостя до внутрішніх ресурсів | ping 192.168.30.30 з Guest-Laptop | Невдало (ACL deny) |
| T-09 | SSH з Admin-PC до CORE-R1 | SSH 192.168.99.1 з Admin-PC | Успішно (AAA) |
| T-10 | SSH з User-PC1 до CORE-R1 | SSH 192.168.99.1 з User-PC1 | Невдало (ACL deny) |
| T-11 | Port Security: стороннє підключення | Зміна MAC на порту IoT | Кадри відхилено, Syslog-повідомлення |
| T-12 | AAA: хибні облікові дані | SSH з неправильним паролем | Відмова, запис у Syslog |
| T-13 | VLAN-ізоляція: кількість VLAN | show vlan brief | 7 активних VLAN |
| T-14 | Передача MQTT-телеметрії | Відправка даних датчиком | Дані отримано брокером |

Тест T-01 перевіряє базову зв'язність сенсорного сегмента з MQTT-брокером. З командного рядка пристрою TempSensor-A1 виконано команду «ping 192.168.30.30». Результат – чотири успішних ICMP-відповіді, що підтверджує коректність маршрутизації та дозвільних правил ACL. Протокол ICMP дозволено неявно через правило «permit tcp ... eq 1883», а прямий ping можливий, оскільки у Packet Tracer IoT-пристрої використовують спрощену модель з'єднання. Для точнішої верифікації протоколу MQTT використано режим симуляції з фільтром TCP, що показано на рис. 3.6.

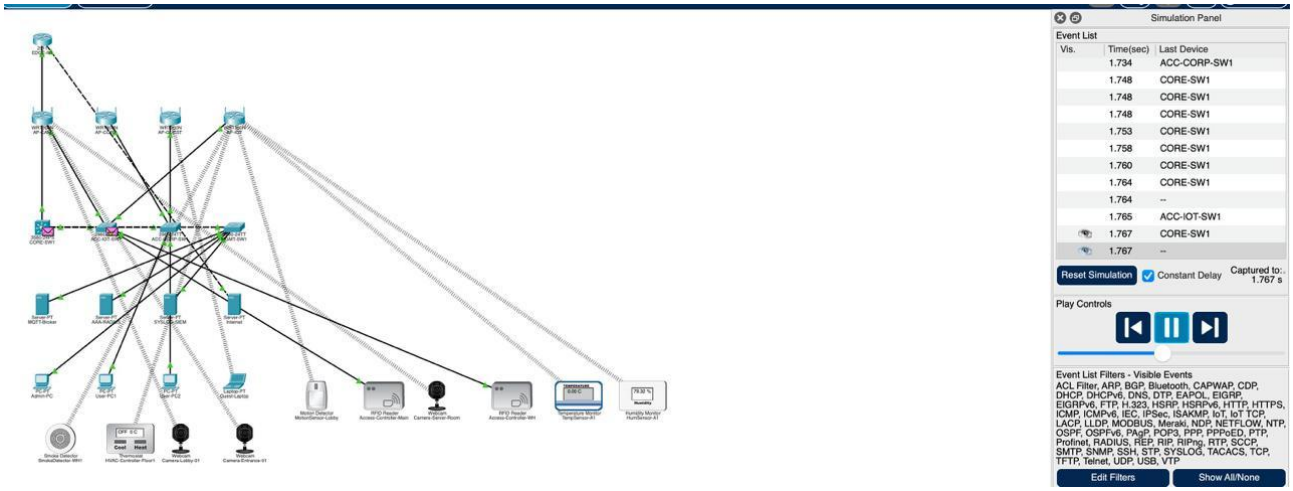



Рисунок 3.6 – Режим симуляції(Джерело: складено автором)

Тест T-02 перевіряє блокування міжсегментного трафіку від IoT до корпоративного сегмента. З TempSensor-A1 виконано «ping 192.168.10.10». Результат – чотири повідомлення «Request timed out», що підтверджує спрацювання правила «deny ip 192.168.20.0 0.0.0.255 any log» у ACL-SENSORS-IN. У режимі симуляції Packet Tracer пакет відхилено на субінтерфейсі Gi0/0.20 маршрутизатора CORE-R1

Тест T-04 перевіряє ізоляцію між підкатегоріями IoT. Спроба ping з TempSensor-A1 (VLAN 20) до Camera-Lobby-01 (VLAN 21, 192.168.21.10) завершилася відмовою – пакет заблоковано ACL-SENSORS-IN, оскільки правило дозволяє трафік лише до хоста 192.168.30.30.

Тест T-08 перевіряє ізоляцію гостьового сегмента від внутрішніх ресурсів. З Guest-Laptop (VLAN 40) виконано «ping 192.168.30.30» – результат негативний. Правило «deny ip 192.168.40.0 0.0.0.255 192.168.0.0 0.0.255.255 log» у ACL-GUEST-IN блокує будь-який трафік до внутрішніх підмереж, дозволяючи лише HTTP/HTTPS до зовнішніх ресурсів.

Тест T-09 перевіряє автентифікацію адміністратора через AAA/RADIUS. З Admin-PC (192.168.99.10) ініційовано SSH-з'єднання до CORE-R1 (192.168.99.1) з обліковими даними «zt-admin / SecurePass2025». Результат – успішний вхід до привілейованого режиму CLI.

Тест Т-10 перевіряє неможливість SSH-доступу з корпоративного сегмента. Спроба SSH-з'єднання з User-PC1 (192.168.10.10) до CORE-R1 заблокована ACL-CORPORATE-IN, оскільки правила цього ACL не містять дозволу на TCP-порт 22 до управлінських адрес. Результат – з'єднання не встановлено.

Тест Т-11 перевіряє механізм Port Security. На комутаторі ACC-IOT-SW1 до порту Fa0/1, на якому вже зафіксовано sticky MAC-адресу TempSensor-A1, підключено інший пристрій з відмінною MAC-адресою. Комутатор зафіксував порушення безпеки, відхилив кадри від невідомої MAC-адреси та надіслав Syslog-повідомлення рівня «warning».

Тест Т-12 перевіряє реакцію AAA на хибні облікові дані. Спроба SSH-з'єднання до CORE-R1 з неправильним паролем завершилася відмовою після трьох спроб. RADIUS-сервер зафіксував невдалу автентифікацію, маршрутизатор надіслав відповідне Syslog-повідомлення. Результат відповідає вимозі функціональної специфікації щодо контролю доступу адміністраторів.

Тест Т-14 перевіряє передачу MQTT-телеметрії від датчика до брокера. У середовищі Packet Tracer IoT-пристрій TempSensor-A1 налаштовано на періодичне надсилання значень температури до MQTT-брокера. У режимі симуляції зафіксовано TCP-сегменти з порту 1883, що проходять через ACL-SENSORS-IN на маршрутизаторі CORE-R1. На сервері MQTT Broker підтверджено отримання повідомлень з топіку «sensors/temp/a1». Зведені результати тестування подано у таблиці 3.2.

Таблиця 3.2-Зведені результати тестування системи безпеки

| ID | Тестовий сценарій | Очікуваний результат | Фактичний результат | Статус |
|---|---|---|---|---|
| Т-01 | IoT-сенсор → MQTT-брокер | Дозволено | Дозволено | Пройдено |
| Т-02 | IoT-сенсор → Corporate | Заблоковано | Заблоковано | Пройдено |
| Т-03 | IoT-сенсор → Internet | Заблоковано | Заблоковано | Пройдено |

Кінець таблиці 3.2

| | | | | |
|---|---|---|---|---|
| T-04 | VLAN 20 → VLAN 21 | Заблоковано | Заблоковано | Пройдено |
| T-05 | Corporate → Internet | Дозволено | Дозволено | Пройдено |
| T-06 | Corporate → IoT | Заблоковано | Заблоковано | Пройдено |
| T-07 | Guest → Internet (HTTP) | Дозволено | Дозволено | Пройдено |
| T-08 | Guest → Servers | Заблоковано | Заблоковано | Пройдено |
| T-09 | Admin SSH через RADIUS | Дозволено | Дозволено | Пройдено |
| T-10 | Corporate SSH до CORE-R1 | Заблоковано | Заблоковано | Пройдено |
| T-11 | Port Security violation | Restrict + Syslog | Restrict + Syslog | Пройдено |
| T-12 | AAA хибні дані | Відмова + Syslog | Відмова + Syslog | Пройдено |
| T-13 | Кількість VLAN ≥ 7 | 7 активних | 7 активних | Пройдено |
| T-14 | MQTT-телеметрія | Доставлено | Доставлено | Пройдено |

Усі 14 тестових сценаріїв пройдено з позитивним результатом. Фактичні результати повністю збігаються з очікуваними, що підтверджує відповідність реалізованої системи функціональним та нефункціональним вимогам технічного завдання.

Аналіз статистики ACL командою «show access-lists» на маршрутизаторі CORE-R1 після серії тестів зафіксував накопичення лічильників «match» на правилах deny, що підтверджує активну роботу фільтрації Для оцінки ефективності мікросегментації виконано порівняльний аналіз зони потенційного впливу (blast radius) компрометації одного IoT-пристрою у двох сценаріях: без сегментації (усі пристрої в одному VLAN) та із реалізованою сегментацією. Результати порівняння подано у таблиці 3.3.

Таблиця 3.3 – Порівняння зони впливу компрометації IoT-пристрою (Джерело: складено автором на основі [8, 9, 22])

| Параметр | Без сегментації | З мікросегментацією (Zero Trust) |
|---|---|---|
| Кількість доступних вузлів після компрометації | Усі вузли мережі (20+) | Лише вузли того самого VLAN (3–5) |
| Можливість латерального переміщення | Необмежена | Заблокована ACL |
| Доступ до серверного сегмента | Необмежений | Лише MQTT (порт 1883) |
| Можливість участі у DDoS | Прямий доступ до Інтернету | Заблокована ACL |
| Виявлення інциденту | Утруднене | Syslog-повідомлення при спрацюванні ACL/Port Security |
| Час локалізації інциденту | Потребує ручного аналізу | Автоматична ізоляція в межах VLAN |

Дані таблиці 3.3 демонструють, що реалізована мікросегментація скорочує зону потенційного впливу компрометації IoT-пристрою з повного обсягу мережі (20+ вузлів) до 3–5 пристроїв у межах одного VLAN. Латеральне переміщення між сегментами унеможливлено правилами ACL, що є прямою протидією сценаріям типу Mirai [13]. Механізми Syslog та Port Security забезпечують автоматичне виявлення аномалій без участі адміністратора.

## 3.4 Висновки до третього розділу

Виконано програмно-апаратну реалізацію системи безпеки IoT-інфраструктури підприємства у середовищі Cisco Packet Tracer 8.2.2. Мережева модель охоплює три маршрутизатори, три комутатори рівня доступу, бездротовий контролер із двома точками доступу, три серверних компоненти (AAA-RADIUS, Syslog/SIEM, MQTT-брокер), десять IoT-пристроїв трьох типів (датчики, камери, контролери доступу), робочі станції корпоративного та адміністративного сегментів і гостьовий ноутбук.

Налаштовано сім VLAN із субінтерфейсами маршрутизатора CORE-R1 для міжсегментної маршрутизації. Створено та застосовано сім іменованих розширених ACL, що реалізують логіку «default deny» та дозволяють лише явно визначені потоки трафіку відповідно до матриці дозволених взаємодій. Налаштовано AAA-модель із автентифікацією через RADIUS та резервною локальною автентифікацією, шифрування бездротового сегмента через WPA3-Enterprise, Port Security зі sticky MAC-адресами на всіх портах доступу та централізоване журналювання через Syslog.

Проведено 14 тестових сценаріїв функціонального тестування, усі з яких пройдено з позитивним результатом. Підтверджено блокування міжсегментного трафіку між IoT-підкатегоріями, ізоляцію гостьового сегмента від внутрішніх ресурсів, контрольований доступ адміністраторів через AAA/RADIUS, спрацювання Port Security при спробі несанкціонованого підключення та доставку MQTT-телеметрії від датчиків до брокера через дозволений канал.

Порівняльний аналіз зони потенційного впливу компрометації IoT-пристрою підтвердив, що мікросегментація скорочує кількість доступних зловмиснику вузлів з повного обсягу мережі до 3–5 пристроїв у межах одного VLAN, унеможливлює латеральне переміщення та забезпечує автоматичне виявлення аномалій через Syslog та Port Security.

# ВИСНОВКИ

У кваліфікаційній роботі розроблено та реалізовано систему безпеки IoT-інфраструктури підприємства на основі концепції Zero Trust у середовищі імітаційного моделювання Cisco Packet Tracer.

Аналіз предметної області засвідчив, що поширення IoT-пристроїв у корпоративних мережах сформувало середовище, у якому традиційна модель периметрового захисту не здатна протидіяти сучасним векторам атак. Гетерогенність кінцевих пристроїв з обмеженими обчислювальними ресурсами змушує переносити основне навантаження безпеки на мережеву інфраструктуру, що узгоджується з принципами архітектури нульової довіри за документом NIST SP 800-207.

Порівняльний аналіз комерційних (Cisco Cyber Vision, Microsoft Defender for IoT, Palo Alto IoT Security) та open-source (FreeRADIUS, pfSense) рішень дозволив визначити базовий інструментарій, достатній для реалізації принципів Zero Trust на мережевому рівні: VLAN, ACL, AAA через RADIUS, Port Security, WPA3.

Спроєктовано архітектуру мережі підприємства з мікросегментацією на сім VLAN, яка розподіляє IoT-пристрої на три ізольованих підкатегорії (датчики, камери, контролери доступу), що мінімізує зону впливу потенційного інциденту. Розроблено матрицю дозволених міжсегментних взаємодій із логікою «default deny», на основі якої сформовано сім іменованих розширених ACL.

Виконано програмно-апаратну реалізацію системи у Cisco Packet Tracer 8.2.2 з десятьма IoT-пристроями, трьома серверними компонентами, трьома комутаторами доступу, двома маршрутизаторами та бездротовою інфраструктурою з WPA3-Enterprise.

Серія з 14 функціональних тестів підтвердила повну відповідність реалізованої системи технічному завданню. Порівняльний аналіз зони потенційного впливу компрометації IoT-пристрою продемонстрував скорочення кількості доступних зловмиснику вузлів з повного обсягу мережі до 3–5

пристроїв у межах одного VLAN, повне блокування латерального переміщення між сегментами та автоматичне виявлення аномалій через механізми Syslog та Port Security.

Розроблена модель може використовуватися як референсне рішення для побудови систем кібербезпеки IoT-інфраструктур підприємств середнього масштабу, а також як навчально-методичний матеріал для підготовки фахівців у галузі комп'ютерної інженерії. Подальшу перспективу роботи складає розширення моделі засобами динамічного призначення VLAN через 802.1X, інтеграція з IDS/IPS та трансляція архітектурних рішень на реальне обладнання Cisco.

# ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ


1. Абрамов В. О., Глушак О. М., Плоха А. Ю. Проєктування мережевої інфраструктури з урахуванням вимог кібербезпеки: підходи та реалізація на базі Cisco. *Кібербезпека: освіта, наука, техніка*. 2025. № 1 (29). URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/845 (дата звернення: 07.05.2026).

2. Архітектура нульової довіри. Блог Oberig IT. 2024. URL: https://oberig-it.com/statti/arhitektura-nulovoyi-doviry/ (дата звернення: 07.05.2026).

3. Васильєв Д. Що таке Zero Trust і як він змінює підхід до безпеки. *HBJ – Genesis Tech Journal*. 2025. URL: https://journal.gen.tech/post/shcho-take-zero-trust (дата звернення: 07.05.2026).

4. Глибовець А. М., Щербина С. С., Кирієнко О. В. Вразливості безпеки та рішення для захисту в системах Інтернету речей. *Наукові записки НаУКМА. Комп'ютерні науки*. 2024. Т. 7. С. 89–97. URL: https://ekmair.ukma.edu.ua/items/1e2fa597-abbc-43f3-8b73-89a00bd29a73 (дата звернення: 07.05.2026).

5. Городицький О. І., Опірський І. Р. Покроковий підхід до імплементації Zero Trust у гібридних архітектурах корпоративної безпеки. *Кібербезпека: освіта, наука, техніка*. 2025. № 3 (31). С. 346–366. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/1029 (дата звернення: 07.05.2026).

6. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII (редакція від 19.10.2025). URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 07.05.2026).

7. Кібератаки на iot-пристрої: мета, наслідки та рішення. *Wezom*. 2024. URL: https://wezom.com.ua/ua/blog/kiberzagrozi-dlya-internetu-rechey-iot-zahist-smart-pristroyiv (дата звернення: 07.05.2026).

8. Маньковський Б. О., Довбняк В. О., Опірський І. Р. Дослідження можливості реалізації концепції Zero Trust в IoT-системах. *Кібербезпека: освіта, наука, техніка*. 2025. № 1 (29). С. 73–91. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/864 (дата звернення: 07.05.2026).

9. Минайленко Р. М., Поліщук Л. І. Особливості проектування архітектури довіри нульового рівня. *Конструювання, виробництво та експлуатація сільськогосподарських машин*. 2024. Вип. 54. URL: https://zbirniksgm.kntu.kr.ua/pdf/54/14.pdf (дата звернення: 07.05.2026).

10. Моделювання пристроїв інтернету речей засобами Cisco Packet Tracer. *Журнал «Фахова передвища освіта»*. 2025. URL: https://osvitafp.com.ua/2025/01/30/modeliuvannia-prystroiv-internetu-rechej-zasobamy-cisco-packet-tracer/ (дата звернення: 07.05.2026).

11. Поширені атаки на IoT та захист від них. *CoreWin*. 2024. URL: https://corewin.ua/blog/attacks-on-iot-how-protect/ (дата звернення: 07.05.2026).

12. Стратегія кібербезпеки України на 2021–2025 роки. Рада національної безпеки і оборони України. URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf (дата звернення: 07.05.2026).

13. Тимошик В. В., Прохоров О. М. Проблеми та загрози безпеці IoT-пристроїв. *Кібербезпека: освіта, наука, техніка*. 2021. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/231 (дата звернення: 07.05.2026).

14. Тренди кібербезпеки на 2025 рік. *CoreWin*. 2024. URL: https://corewin.ua/news/cybersecurity-trends-protecting-business-information-in-2025/ (дата звернення: 07.05.2026).

15. Цифрова безпека у 2025: як захиститися від кіберзагроз. *Glavnoe.in.ua*. 2025. URL: https://glavnoe.in.ua/news/czyfrova-epoha-ta-kiberbezpeka-vyklyky-ta-zahyst (дата звернення: 07.05.2026).

16. Яскевич В., Яскевич Ю. Архітектура нульової довіри: логічні компоненти та підходи запровадження. *Зв'язок*. 2024. № 3 (169). URL: https://elibrary.kubg.edu.ua/50065/1/V_Yaskevych_Y_Yaskevych_Zvyazok_3_169_2024_2_FITM.pdf (дата звернення: 07.05.2026).

17. Architecture of zero trust: principles. SAP Ukraine. 2024. URL: https://www.sap.com/ukraine/resources/what-is-zero-trust (дата звернення: 07.05.2026).

18. Cybersecurity Trends and Threats: Zero Trust Framework Trends for 2025. *Cyber Advisors*. 2025. URL: https://blog.cyberadvisors.com/zero-trust-framework-trends-for-2025 (дата звернення: 07.05.2026).

19. Kindervag J. Zero Trust Architecture: основні принципи. *Syteca / Bakotech*. 2024. URL: https://syteca.bakotech.com/ua/blog/zero_trust_security_model (дата звернення: 07.05.2026).

20. OT/ICS and Industrial IoT Security. *Cisco Systems*. 2025. URL: https://www.cisco.com/site/us/en/products/security/industrial-security/index.html (дата звернення: 07.05.2026).

21. Прокопчук Ю. М., Бойко В. О. Аналіз методів захисту інформації у мережах IoT. *Вісник Вінницького політехнічного інституту*. 2024. № 4. С. 129–137. URL: https://visnyk.vntu.edu.ua/index.php/visnyk/article/download/3078/2832/3546 (дата звернення: 07.05.2026).

22. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture: NIST Special Publication 800-207. National Institute of Standards and Technology. 2020. 59 p. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (дата звернення: 07.05.2026).

23. SecureW2. Building a Zero Trust 802.1X Network: Key Design Steps. 2025. URL: https://www.securew2.com/blog/design-zero-trust-network (дата звернення: 07.05.2026).

24. Cisco Systems. Cisco IOS Security Configuration Guide. 2024. URL: https://www.cisco.com/c/en/us/support/docs/security (дата звернення: 07.05.2026).

25. Cisco Systems. VLAN Configuration Guide. 2024. URL: https://www.cisco.com/c/en/us/support/docs/lan-switching/vlan (дата звернення: 07.05.2026).

26. Cisco Systems. Configuring Access Control Lists. 2024. URL: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall (дата звернення: 07.05.2026).

27. Cisco Systems. AAA Configuration Guide. 2024. URL: https://www.cisco.com/c/en/us/support/docs/security/aaa (дата звернення: 07.05.2026).

28. Cisco Systems. Port Security Configuration Example. 2024. URL: https://www.cisco.com/c/en/us/support/docs/switches (дата звернення: 07.05.2026).

29. Stallings W. Network Security Essentials. 7th ed. Pearson, 2022. 488 p.

30. Kurose J., Ross K. Computer Networking: A Top-Down Approach. 8th ed. Pearson, 2021. 864 p.

31. Tanenbaum A., Wetherall D. Computer Networks. 5th ed. Pearson, 2021. 960 p.

32. NIST. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. 2023. URL: https://www.nist.gov/cyberframework (дата звернення: 07.05.2026).

33. Behl A., Behl K. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2023.

34. Granjal J., Monteiro E., Silva J. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. IEEE Communications Surveys & Tutorials. 2022.

35. Sicari S., Rizzardi A., Grieco L., Coen-Porisini A. Security, Privacy and Trust in Internet of Things. Computer Networks. 2022.

36. Easttom C. Network Defense and Countermeasures. 3rd ed. Pearson, 2022. 400 p.

37. ENISA. IoT Security Guidelines. 2024. URL: https://www.enisa.europa.eu (дата звернення: 07.05.2026).

38. Sicari S., Rizzardi A., Grieco L., Coen-Porisini A. Security, Privacy and Trust in Internet of Things. Computer Networks. 2022.

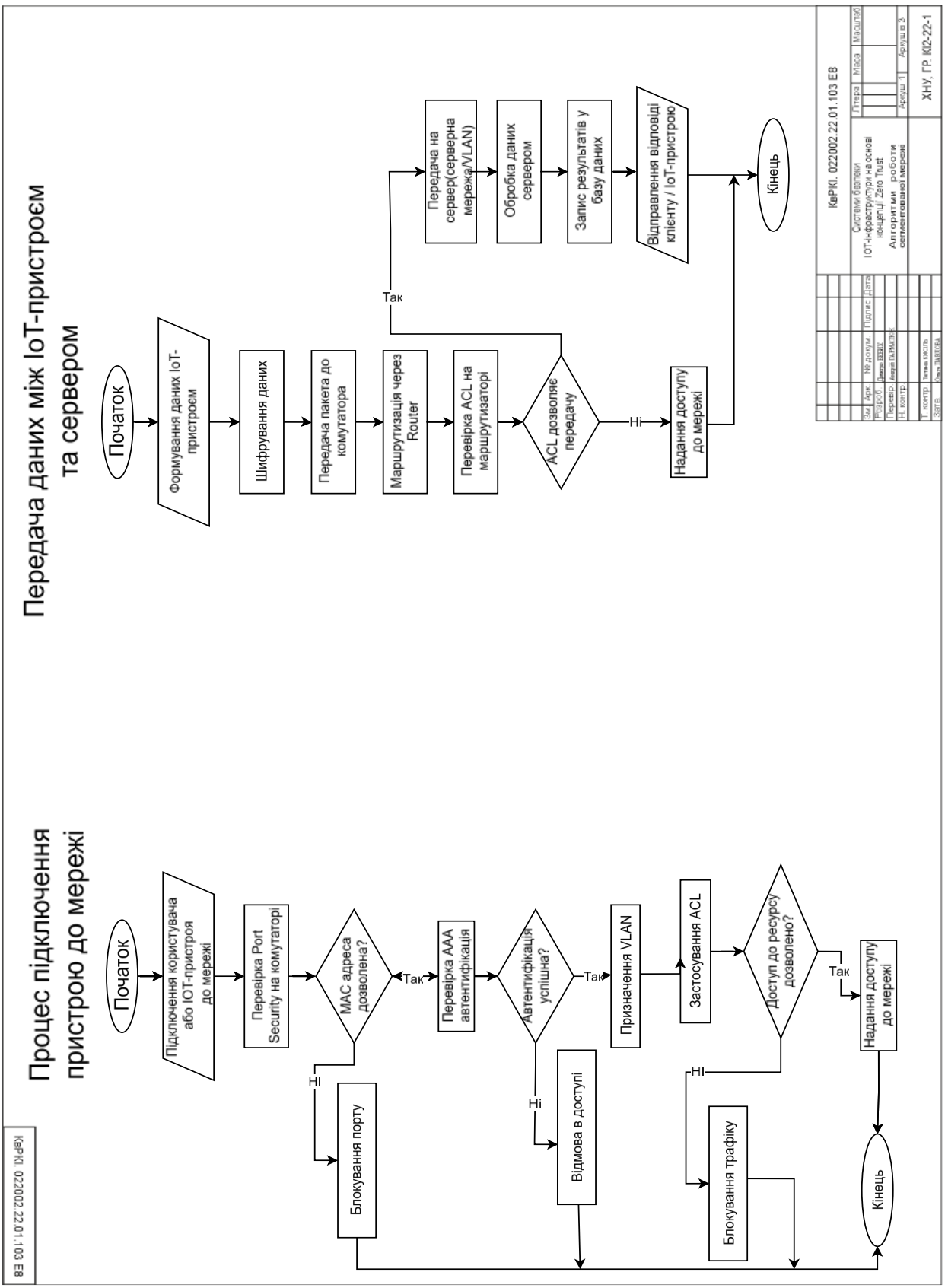
39. Roman R., Zhou J., Lopez J. On the Features and Challenges of Security and Privacy in Distributed Internet of Things. Computer Networks. 2021.

40. Gartner. Top Cybersecurity Trends for 2025. 2025. URL: https://www.gartner.com (дата звернення: 07.05.2026).

**ДОДАТОК А**

(обов’язковий)

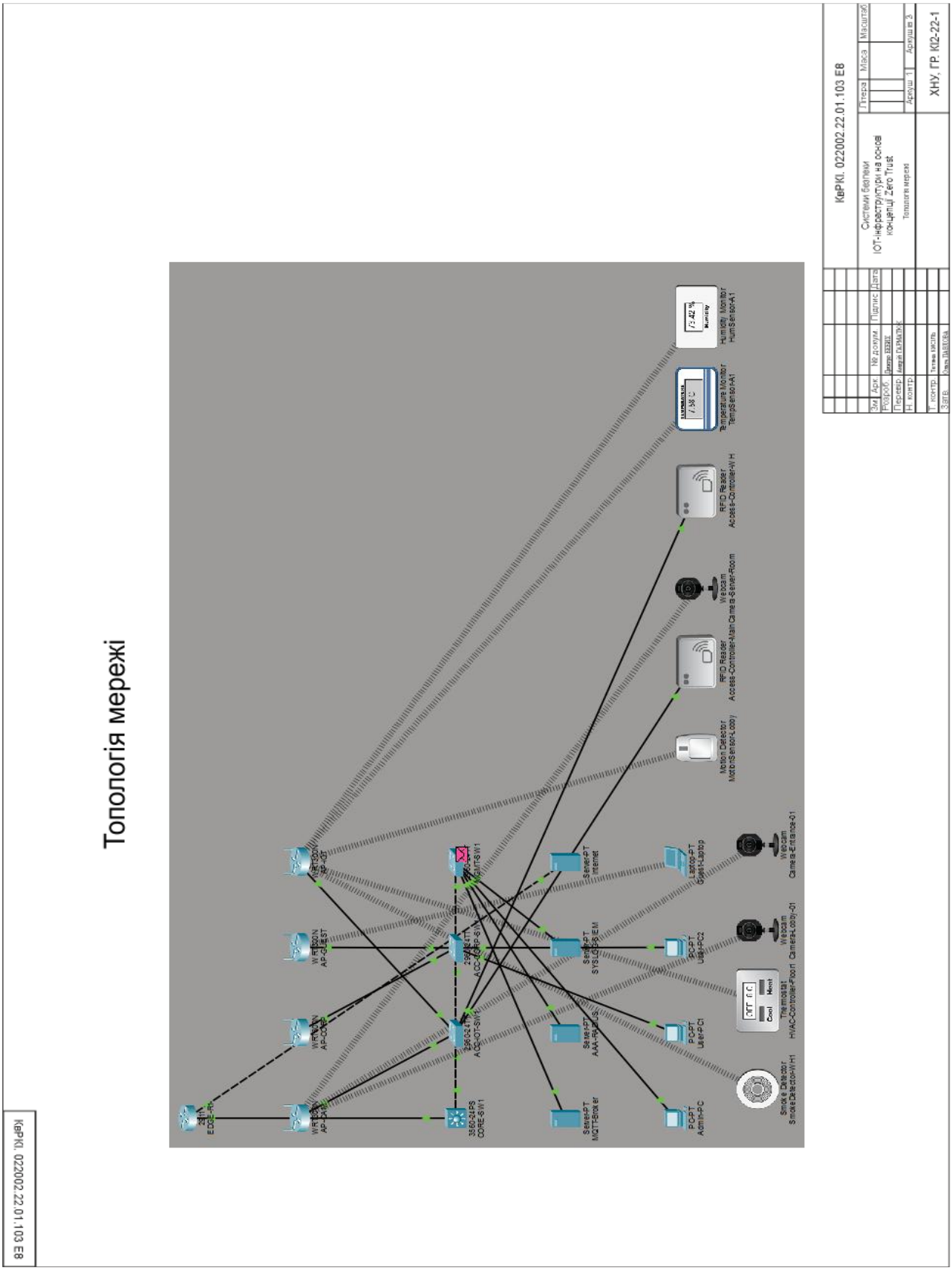
Алгоритми роботи сегментованої мережі



**ДОДАТОК Б**

(обов’язковий)

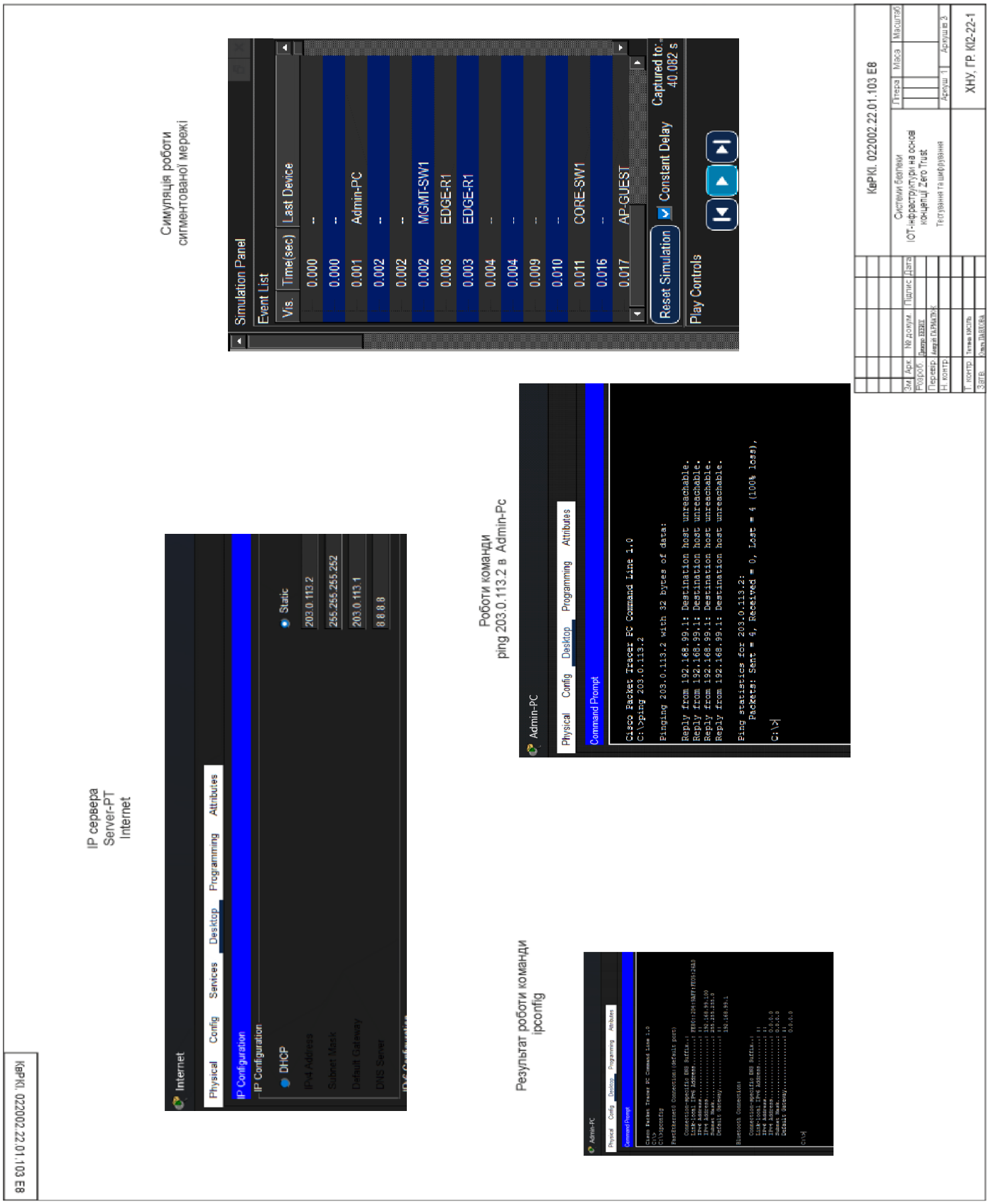
Топологія мережі



# ДОДАТОК В

(обов’язковий)

Тестування та шифрування



**Протокол аналізу звіту подібності експертом**

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

**Автор:** Дмитро БЕБИХ

**Співавтор:**

**Назва:** Система безпеки IoT-інфраструктури підприємства на основі концепції Zero Trust

**Експерт:** Андрій ГАРМАТЮК

**Підрозділ:** Кафедра комп'ютерної інженерії та інформаційних систем

**Коефіцієнт подібності 1:**3.28%

**Коефіцієнт подібності 2:**0.41%

**Мікропробіли:** 3

**Заміна букв:** 0

**Інтервали:** 0

**Білі знаки:** 0

**Дата створення звіту:** 2026-06-11 02:39:44.0

**Після аналізу Звіту подібності констатую наступне:**

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2026-06-11 Доцент Андрій Нічепорук

*Дата* експерт

Wed Jun 10 10:11:04 EEST 2026, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

# Anti-Plagiarism (http://ap.km.ua) v-15.701

**Максимальне співпадіння з одним документом 1.0%**

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 17%**

| | Документ | | Сумарний збіг по Базі Даних | |
|---|---|---|---|---|
| ID: 274541<br>Назва: БКР Система безпеки IoT-інфраструктури підприємства на основі концепції Zero Trust<br>Додано в БД: 2026-06-10<br>Автора: Дмитро БЕБИХ<br>Керівники: Андрій ГАРМАТЮК<br>Консультанти:<br>Опоненти: | Символи | Лексеми | Символи | Лексеми |
| | 84616 | 641 | 2573 (3%) | 32 (5%) |

Джерело плагіату

| ID | Опис | Наявність плагіату в документі | |
|---|---|---|---|
| | | Символи | Лексеми |

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

# РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Бебих Дмитро Валерійович

Тема: Проектування системи безпеки IOT-інфраструктури на основі концепції Zero Trust

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи:

Кількість листів креслень ___3____ Кількість сторінок записки ___72___

1. Короткий зміст роботи та прийнятих рішень: Метою кваліфікаційної роботи є проєктування, програмна реалізація та тестування системи захисту IoT-інфраструктури підприємства на основі концепції Zero Trust. У роботі проведено аналіз предметної області IoT-середовищ та загроз їх безпеці, досліджено сучасні програмно-апаратні засоби захисту, а також сформовано вимоги до системи безпеки. Розроблено архітектуру мережі підприємства з використанням мікросегментації, спроєктовано політики доступу, автентифікації та шифрування. Виконано реалізацію мережевої моделі в середовищі Cisco Packet Tracer із налаштуванням VLAN, ACL, AAA та Port Security, після чого проведено тестування працездатності та оцінку ефективності запропонованого рішення.

2. Висновок про відповідність роботи дипломному завданню: Робота повністю відповідає поставленому завданню.

3. Характеристика виконання кожного розділу, ступінь використання сучасних досягнень науки і техніки та передових методів роботи: у першому розділі проведено дослідження IoT-інфраструктур підприємства та їх захисту. Проаналізовано сучасні підходи кібербезпеки в умовах Zero Trust, загрози для корпоративних мереж і сучасні засоби захисту. Обґрунтовано вимоги до системи безпеки та сформовано технічне завдання. У другому розділі розроблено архітектуру захищеної IoT-інфраструктури на основі Zero Trust і мікросегментації. Спроєктовано політики доступу, автентифікації та шифрування, а також логічну структуру взаємодії компонентів у Cisco Packet Tracer. У третьому розділі виконано реалізацію та тестування системи безпеки.

Створено модель мережі в Cisco Packet Tracer, налаштовано VLAN, ACL, AAA та Port Security. Проведено перевірку працездатності та оцінку ефективності запропонованого рішення.

4. Позитивні сторони роботи: У кваліфікаційній роботі використано сучасні підходи до проєктування системи безпеки IoT-інфраструктури на основі концепції Zero Trust. Розроблено практично орієнтовану архітектуру з використанням механізмів мікросегментації та засобів захисту корпоративного рівня (VLAN, ACL, AAA, Port Security). Відзначається висока ступінь опрацювання принципів мережевої безпеки, а також практична реалізація моделі в середовищі Cisco Packet Tracer, що забезпечує наближення до реальних умов функціонування корпоративних мереж.

5. Негативні сторони роботи: У роботі недостатньо приділено уваги порівняльному аналізу запропонованого рішення з існуючими сучасними системами кіберзахисту та комерційними платформами моніторингу й безпеки IoT-інфраструктур. Також присутні окремі неточності та стилістичні огріхи в оформленні текстової частини роботи.

6. Оцінка графічного оформлення та пояснювальної записки роботи: Пояснювальна записка оформлена коректно, згідно діючих стандартів оформлення документації.

7. Відгук про роботу в цілому: Робота виконана на належному науково-технічному рівні, здобувач продемонстрував грунтовні інженерні знання, а сама робота заслуговує на позитивну оцінку.

8. Інші зауваження: _____

9. Оцінка дипломної роботи: добре

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) _____

Яцишин О.М., доцент кафедри ТТЗ

"11" 06 2026 р. _____ (підпис)

Зав. кафедри КІІС
д-р. філософії Ользі ПАВЛОВІЙ

Дмитро БЕБИХ

ПІБ здобувача вищої освіти

ФІТ, 4 курсу, групи КІ2-22-1

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів академічної відповідальності, ознайомлений (а). Про використання спеціалізованих програмних засобів (СПЗ) StrikePlagiarism та Anti-Plagiarism для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений (а). Надаю університету право на передачу моєї роботи для обробки та збереження в базах даних СПЗ і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються СПЗ.

Також надаю свою згоду на обробку й збереження університетом моєї роботи в Інституційному репозитарії Хмельницького національного університету.

Робота надається для перевірки в електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

1 травня 2026 року

# РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

## КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Назва кваліфікаційної роботи Проектування системи безпеки IOT-інфраструктури на основі концепції Zero Trust
Автор Дмитро БЕБИХ
Освітня програма Комп'ютерна інженерія та програмування
Рівень вищої освіти перший (бакалаврський)
Спеціальність 123 Комп'ютерна інженерія
Науковий керівник: Андрій ГАРМАТЮК

На основі аналізу кваліфікаційної роботи на дотримання вимог академічної доброчесності (у т.ч. відсутності ознак академічного плагіату) з урахуванням результатів перевірки роботи спеціалізованим програмним засобом(ами) комісія зробила такий висновок:

| № | Висновок | Позначка про відповідність |
|---|---|---|
| 1 | Ознаки академічного плагіату | |
| 1.1 | Запозичення, виявлені в роботі, є законними і не є академічним плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних, якщо потрібно). Робота приймається до захисту. | відповідає |
| 1.2 | Виявлені запозичення не є академічним плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. | |
| 1.3 | Виявлені запозичення не є академічним плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота може бути допущена до захисту після того як буде відкоригована та доопрацьована і успішно пройде повторну перевірку на академічний плагіат. | |
| 1.4 | Робота містить навмисні текстові спотворення, передбачувані спроби укриття текстових запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту. | |
| 2 | Інші види порушень академічної доброчесності | |

Підтвердження:
Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
2) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з джерелами на один фрагмент речення;
3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.
4) значна частина знайденого плагіату відноситься до списку використаних джерел

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 3,28%; та системою Anti-Plagiarism складає 1,0%, що, з урахуванням наведених обгрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

01.06.2026

Завідувач кафедри _____ Підпис — Ольга ПАВЛОВА (Ім'я, ПРІЗВИЩЕ)

Гарант освітньої програми _____ Підпис — Андрій НІЧЕПОРУК (Ім'я, ПРІЗВИЩЕ)

Керівник кваліфікаційної роботи _____ Підпис — Андрій ГАРМАТЮК (Ім'я, ПРІЗВИЩЕ)