

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»**

Навчально-науковий Інститут телекомунікаційних систем

Кафедра електронних комунікацій та інтернету речей

«До захисту допущено»

Завідувач кафедри

_____ Анатолій МАКАРЕНКО

« ____ » _____ 20 ____ р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Особливості забезпечення кібербезпеки в мережах IoT»

Виконав:

студент IV курсу, групи ТС-22

Мельник Максим Сергійович _____

Керівник:

Доцент кафедри ЕКІР, к.т.н. доцент,

Григоренко Олена Григорівна _____

Рецензент:

Доцент каф. Інформаційної безпеки НН ФТІ, доц., к.т.н.

Репа Федір Михайлович _____

Засвідчую, що у цій дипломній роботі немає
запозичень з праць інших авторів без
відповідних посилань.

Студент _____

Київ – 2026 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий Інститут телекомунікаційних систем
Кафедра електронних комунікацій та інтернету речей

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 Телекомунікації та радіотехніка

Освітня програма – «Системи електронних комунікацій та Інтернету речей»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Анатолій МАКАРЕНКО

«__» _____ 20__ р.

ЗАВДАННЯ

на дипломну роботу студенту
Мельнику Максиму Сергійовичу

1. Тема роботи «Особливості забезпечення кібербезпеки в мережах IoT», керівник роботи Григоренко Олена Григорівна, кандидат технічних наук, доцент кафедри ЕКІР, затверджені наказом по університету від «26» травня 2026 р. №1912 – с.
2. Термін подання студентом роботи 13 червня 2026 р.
3. Вихідні дані до роботи
4. Зміст роботи
 1. Проаналізувати архітектуру мереж Інтернету речей та здійснити класифікацію основних загроз і вразливостей, що виникають через специфіку IoT-обладнання.
 2. Обґрунтувати вибір методів та засобів захисту мережевої інфраструктури на каналному та мережевому рівнях моделі OSI, а також середовища імітаційного моделювання.
 3. Розробити топологію захищеної мережі та реалізувати комплекс механізмів захисту.
 4. Провести експериментальну перевірку ефективності запропонованих рішень шляхом імітації сценаріїв типових кібератак та аналізу реакції системи захисту.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

Плакат №1 (слайд) Тема роботи;

Плакат №2 (слайд) Мета роботи, об'єкт, предмет та актуальність дослідження;

Плакат №3 (слайд) Основні поняття та принципи IoT;

Плакат №4 (слайд) Аналіз загроз та вразливостей в мережах Інтернету речей;

Плакат №5 (слайд) Огляд методів та протоколів захисту IoT-систем;

Плакат №6 (слайд) Схема модельованої мережі в середовищі Cisco Packet Tracer;

Плакат №7 (слайд) Реалізація механізмів захисту канального рівня (Port Security, DHCP Snooping, DAI);

Плакат №8 (слайд) Сегментація та фільтрація трафіку на мережевому рівні (VLAN, ACL, SSH);

Плакат №9 (слайд) Оцінка ефективності запропонованих рішень;

Плакат №10 (слайд) Загальні висновки по роботі;

6. Дата видачі завдання 28.01.2026 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	28.01.2026	виконано
2	Підбір та опрацювання літератури за темою	10.02.2026	виконано
3	Аналіз архітектури мереж IoT та класифікація загроз і вразливостей	23.03.2026	виконано
4	Аналіз наслідків кібератак на IoT-інфраструктуру, формулювання наукової проблеми	10.04.2026	виконано
5	Огляд підходів до захисту та обґрунтування вибору технологій	18.04.2026	виконано
6	Порівняльний аналіз та вибір середовища імітаційного моделювання	08.05.2026	виконано
7	Проектування топології та реалізація механізмів захисту в Cisco Packet Tracer	20.05.2026	виконано
8	Імітаційне моделювання атак та тестування ефективності системи захисту	30.05.2026	виконано
9	Формулювання висновків, оформлення роботи відповідно до вимог	02.06.2026	виконано

Студент

Максим МЕЛЬНИК

Керівник роботи

Олена ГРИГОРЕНКО

РЕФЕРАТ

Кваліфікаційна робота: **75 стор., 13 рис., 19 джерел.**

Мета роботи — підвищення рівня захищеності мережевої інфраструктури Інтернету речей шляхом обґрунтування та впровадження комплексних методів захисту на каналному та мережевому рівнях моделі OSI.

Об'єкт дослідження — процес передачі даних та функціонування розподіленої мережевої інфраструктури Інтернету речей.

Предмет дослідження — методи та програмно-апаратні засоби забезпечення конфіденційності, цілісності та доступності інформаційних потоків у мережах IoT.

Короткий зміст роботи

У першому розділі проаналізовано концепцію та архітектурну будову мереж Інтернету речей, простежено еволюцію архітектурних підходів від базової трирівневої до семирівневої моделі. Здійснено класифікацію загроз та вразливостей IoT-систем за рівнями архітектури з опорою на тріаду конфіденційності, цілісності та доступності. Розглянуто домінуючі вектори сучасних кібератак на IoT-середовища, серед яких атаки відмови в обслуговуванні, експлуатація облікових даних за замовчуванням, атаки «людина посередині» та зараження ботнетами.

У другому розділі обґрунтовано вибір методів та засобів захисту мережевої інфраструктури Інтернету речей. Доведено доцільність застосування мережецентричного підходу як єдиного способу компенсації внутрішніх вразливостей кінцевих пристроїв. Сформовано інтегрований комплекс захисних механізмів, що включає сегментацію через VLAN, розширені списки контролю доступу, технологію Port Security, а також зв'язку DHCP Snooping та Dynamic ARP Inspection. Здійснено порівняльний аналіз середовищ моделювання мереж та обґрунтовано вибір симулятора Cisco Packet Tracer як оптимального інструмента для практичної реалізації.

У третьому розділі спроектовано та реалізовано в середовищі імітаційного моделювання комплексну топологію захищеної мережі розумного офісу із сегментацією на чотири ізольовані віртуальні локальні мережі. Налаштовано повний цикл механізмів захисту канального та мережевого рівнів, включно з протоколом Secure Shell версії 2 для безпечного адміністрування. Проведено імітаційне тестування ефективності розробленої системи за трьома сценаріями кібератак: фізичне неавторизоване підключення, підміна MAC-адреси з переміщенням та атака «людина посередині» через розгортання нелегітимного DHCP-сервера. Експериментально підтверджено практичну цінність архітектури ешелонованої оборони та доведено ефективність запропонованого комплексу засобів захисту.

КЛЮЧОВІ СЛОВА: ІНТЕРНЕТ РЕЧЕЙ, КІБЕРБЕЗПЕКА, МЕРЕЖЕВА ІНФРАСТРУКТУРА, CISCO PACKET TRACER, СЕГМЕНТАЦІЯ МЕРЕЖІ, VLAN, ACL, PORT SECURITY, ЕШЕЛОНОВАНА ОБОРОНА, НУЛЬОВА ДОВІРА.

ABSTRACT

The qualification work consists of **75 pages, 13 figures, 19 references.**

The purpose of the work is to enhance the security level of the Internet of Things network infrastructure through the substantiation and implementation of comprehensive protection methods at the data link and network layers of the OSI model.

The object of research is the process of data transmission and the functioning of the distributed network infrastructure of the Internet of Things.

The subject of research is methods and software-hardware means of ensuring confidentiality, integrity, and availability of information flows in IoT networks.

Summary

The first chapter analyzes the concept and architectural structure of Internet of Things networks and traces the evolution of architectural approaches from the basic three-layer to the seven-layer model. A classification of threats and vulnerabilities of IoT systems by architectural levels is carried out based on the triad of confidentiality, integrity, and availability. The dominant vectors of modern cyberattacks on IoT environments are considered, including denial-of-service attacks, exploitation of default credentials, man-in-the-middle attacks, and botnet infections.

The second chapter substantiates the choice of methods and means of protecting the Internet of Things network infrastructure. The feasibility of applying a network-centric approach as the only way to compensate for the internal vulnerabilities of end devices is proven. An integrated complex of protective mechanisms is formed, which includes VLAN segmentation, extended access control lists, Port Security technology, as well as the combination of DHCP Snooping and Dynamic ARP Inspection. A comparative analysis of network modeling environments is carried out, and the choice of the Cisco Packet Tracer simulator as the optimal tool for practical implementation is justified.

The third chapter presents the design and implementation of a comprehensive topology of a secure smart office network with segmentation into four isolated virtual

local area networks within the simulation environment. A full cycle of data link and network layer protection mechanisms is configured, including the Secure Shell protocol version 2 for secure administration. Simulation testing of the developed system's effectiveness is conducted across three cyberattack scenarios: unauthorized physical connection, MAC address spoofing with lateral movement, and a man-in-the-middle attack through the deployment of a rogue DHCP server. The practical value of the defense-in-depth architecture is experimentally confirmed, and the effectiveness of the proposed set of protection means is proven.

KEYWORDS: INTERNET OF THINGS, CYBERSECURITY, NETWORK INFRASTRUCTURE, CISCO PACKET TRACER, NETWORK SEGMENTATION, VLAN, ACL, PORT SECURITY, DEFENSE IN DEPTH, ZERO TRUST

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ ...	10
ВСТУП.....	11
1 АНАЛІЗ ПРОБЛЕМАТИКИ КІБЕРБЕЗПЕКИ В СИСТЕМАХ ІОТ	13
1.1 Концепція та архітектура мереж Інтернету речей.....	13
1.2 Класифікація загроз та вразливостей ІоТ-систем	18
1.3 Аналіз наслідків кібератак на ІоТ-інфраструктуру.....	23
1.4 Висновки до розділу 1	27
2 ОБҐРУНТУВАННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ.....	29
2.1 Огляд сучасних підходів до забезпечення безпеки ІоТ.....	29
2.2 Обґрунтування вибору технологій для реалізації.....	32
2.3 Вибір середовища моделювання	38
2.4 Висновки до розділу 2	42
3 ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗАХИСТУ В CISCO PACKET TRACER	44
3.1 Проектування та базова конфігурація мережі.....	44
3.2 Реалізація механізмів захисту на каналному рівні	51
3.2.1 Логічна сегментація та управління неактивними портами.....	51
3.2.2 Налаштування безпеки портів (Port Security).....	54
3.2.3 Впровадження захисту від атак типу «людина посередині»	55
3.3 Налаштування безпеки мережевого рівня та фільтрації трафіку.....	57
3.3.1 Впровадження списків контролю доступу.....	58
3.3.2 Налаштування захищеного віддаленого керування (SSH)	59
3.4 Імітаційне моделювання атак та тестування ефективності системи захисту	61
3.4.1 Сценарій 1: Фізичне проникнення та спроба неавторизованого підключення	62
3.4.2 Сценарій 2: Атака підміни ідентифікатора (MAC Spoofing) та спроба поширення загроз мережею.....	63
3.4.3 Сценарій 3: Атаки типу «Людина посередині»	65

3.4.4 Аналіз результатів моделювання та загальна оцінка надійності.....	67
3.5 Висновки до розділу 3	68
ВИСНОВКИ.....	71
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	73

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, СКОРОЧЕНЬ І ТЕРМІНІВ

ACL	Access Control List — список контролю доступу
ARP	Address Resolution Protocol — протокол визначення адрес
DAI	Dynamic ARP Inspection — динамічна інспекція ARP
DDoS	Distributed Denial of Service — розподілена відмова в обслуговуванні
DHCP	Dynamic Host Configuration Protocol — протокол динамічної конфігурації хоста
DNS	Domain Name System — система доменних імен
GNS3	Graphical Network Simulator-3 — графічний мережевий симулятор третього покоління
IEEE	Institute of Electrical and Electronics Engineers — Інститут інженерів з електротехніки та електроніки
IoT	Internet of Things — Інтернет речей
IP	Internet Protocol — міжмережевий протокол
L2	Data Link Layer — канальний рівень моделі OSI
L3	Network Layer — мережевий рівень моделі OSI
MAC	Media Access Control — управління доступом до середовища
MitM	Man-in-the-Middle — атака «людина посередині»
NIST	National Institute of Standards and Technology — Національний інститут стандартів і технологій
OSI	Open Systems Interconnection — взаємодія відкритих систем
OT	Operational Technology — операційні технології
RSA	Rivest-Shamir-Adleman — криптографічний алгоритм Рівеста, Шаміра, Адлемана
SSH	Secure Shell — протокол захищеної оболонки
VLAN	Virtual Local Area Network — віртуальна локальна мережа
ZTA	Zero Trust Architecture — архітектура нульової довіри

ВСТУП

Еволюція глобальної мережі призвела до виникнення феномену Інтернету речей (Internet of Things – IoT), який фундаментально змінює підходи до генерації та обробки інформації. Якщо в класичних мережах ініціатором трафіку зазвичай виступав користувач, то в екосистемі IoT обмін даними відбувається автономно, без прямого втручання людини. Це призводить до експоненційного зростання кількості кінцевих вузлів мережі, яке вже вимірюється мільярдами активних з'єднань.

Ключовою відмінністю IoT-пристроїв від традиційних комп'ютерних систем є їх обмежені обчислювальні ресурси та енергозалежність. Більшість кінцевих вузлів не здатні підтримувати важкі механізми шифрування або повноцінні операційні системи з вбудованими засобами захисту. Це створює парадоксальну ситуацію: найбільш масовий сегмент мережі Інтернет є водночас і найбільш вразливим.

Впровадження IoT-рішень дозволяє оптимізувати робочі процеси, впроваджувати аналітику та знижувати вплив людського фактору. Проте, враховуючи, що IoT-пристрої часто стають вхідною точкою для масштабних кібератак на корпоративні та приватні мережі, виникає гостра потреба у розробці методів захисту на рівні мережевої інфраструктури, зокрема на каналному та мережевому рівнях моделі OSI, де можливо реалізувати централізований контроль та аналіз трафіку.

Метою роботи є підвищення рівня захищеності мережевої інфраструктури IoT шляхом обґрунтування та впровадження комплексних методів захисту на рівнях комутації та маршрутизації.

Для досягнення поставленої мети необхідно вирішити такі завдання:

1. Проаналізувати архітектуру мереж Інтернету речей та класифікувати основні вектори кіберзагроз, що виникають через специфіку IoT-обладнання.

2. Здійснити порівняльний аналіз існуючих методів захисту та обґрунтувати вибір технологій для забезпечення безпеки на каналному та мережевому рівнях.

3. Провести експериментальну перевірку ефективності запропонованих рішень шляхом імітації поширених кібератак.

Важливою складовою роботи є практична реалізація теоретичних напрацювань, що передбачає розробку топології захищеної мережі та моделювання її роботи в середовищі імітаційного моделювання Cisco Packet Tracer. Завершальним етапом дослідження стане перевірка ефективності запропонованих рішень шляхом імітації сценаріїв типових мережевих атак та аналізу реакції системи захисту на несанкціоноване втручання.

В якості об'єкта дослідження в роботі розглядається процес передачі даних та функціонування розподіленої мережевої інфраструктури, що об'єднує різноманітні пристрої Інтернету речей в єдину систему, яка створює потенційні ризики для інформаційної безпеки.

Предметом дослідження виступають безпосередньо методи та програмно-апаратні засоби забезпечення конфіденційності, цілісності та доступності інформаційних потоків у мережах IoT.

Методологічну основу дослідження складають методи системного аналізу, що застосовуються для класифікації загроз, методи порівняльного аналізу для вибору оптимальних засобів захисту, а також метод імітаційного моделювання для побудови та верифікації захищеної мережевої інфраструктури.

1 АНАЛІЗ ПРОБЛЕМАТИКИ КІБЕРБЕЗПЕКИ В СИСТЕМАХ ІОТ

1.1 Концепція та архітектура мереж Інтернету речей

Розуміння природи вразливостей та специфіки захисту Інтернету речей неможливе без детального аналізу його концептуальної будови та архітектурної ієрархії. На рівні архітектури ці особливості формалізуються через специфічні моделі взаємодії компонентів. Сутність ІоТ виходить за межі простого підключення пристроїв до мережі, дослідники визначають цю технологію як глобальну інфраструктуру, що дозволяє фізичним та віртуальним об'єктам взаємодіяти, створюючи нові сервіси та застосунки. Часто проводиться аналогія між ІоТ та соціальними мережами, де замість людей комунікацію здійснюють розумні об'єкти, формуючи мережу речей, яка функціонує автоматично, віддалено та безперервно [1].

Функціонування цієї екосистеми базується на складній взаємодії кількох фундаментальних елементів, які забезпечують перетворення фізичних параметрів у цифрові дані. Першочерговим елементом є ідентифікація, яка гарантує, що кожен об'єкт у мережі має унікальне ім'я або адресу, наприклад, через використання протоколу IPv6 або електронного коду продукту. Наступним критичним компонентом є процес відчуття (sensing), що передбачає збір даних із навколишнього середовища за допомогою різноманітних датчиків, смарт-тегів або носимих пристроїв, які згодом передаються у централізовані бази даних або хмарні сховища. Ключову роль відіграє комунікація, яка об'єднує різноманітні об'єкти для обміну інформацією, використовуючи широкий спектр технологій від Wi-Fi та Bluetooth до NFC та RFID. Обробка зібраної інформації покладається на обчислювальні елементи, що виступають мозком системи, виконуючи команди та керуючи потужностями через апаратні платформи та операційні системи реального часу [3].

Зазначені елементи інтегруються у сервіси, які можуть варіюватися від простого збору даних до складних семантичних операцій, і врешті-решт формують концепцію повсюдних сервісів (Ubiquitous Services). Ця концепція

передбачає здатність системи не лише збирати інформацію, але й самостійно приймати рішення щодо реакції на зміни у середовищі, що є основою автоматизації у розумних середовищах [3]. Проте така різноманітність пристроїв та протоколів створює значні архітектурні виклики. На відміну від традиційних комп'ютерних мереж, для IoT досі не існує єдиного, жорстко стандартизованого еталону архітектури. Це зумовлено тим, що пристрої можуть кардинально відрізнятися за функціоналом: від мініатюрних сенсорів до потужних серверів обробки даних. У науковій спільноті найбільш поширеними є підходи, що базуються на розподілі функцій за рівнями [1].

Базовою та найстарішою моделлю, яка заклала фундамент для розуміння будови IoT, є трирівнева архітектура. Вона залишається актуальною для опису загальних принципів роботи системи, хоча й вважається недостатньою для глибокого аналізу сучасних аспектів безпеки. Структуру трирівневої архітектури IoT наведено на рис. 1.1.



Рисунок 1.1 — Трирівнева архітектура IoT [3]

Нижній рівень цієї моделі називають рівнем сприйняття, або фізичним рівнем. Він виконує функцію, аналогічну органам чуття людини: ідентифікує об'єкти та збирає інформацію про фізичний світ. Саме на цьому рівні розташовані датчики, камери, RFID-мітки та виконавчі механізми. Основною проблемою цього рівня, що безпосередньо впливає на безпеку, є те, що пристрої тут часто розміщуються у відкритому, фізично доступному середовищі та мають вкрай обмежені обчислювальні ресурси, що ускладнює впровадження складних криптографічних алгоритмів безпосередньо на кінцевих точках [1, 3].

Зібрані дані передаються на наступний рівень — мережевий, який також називають транспортним. Цей рівень виступає мостом, що забезпечує транзит інформації від рівня сприйняття до рівня обробки та додатків. Він функціонує через різноманітні бездротові та дротові технології зв'язку, включаючи 3G/4G/5G, Wi-Fi, Bluetooth та інфрачервоні канали. Саме на цьому етапі відбувається маршрутизація пакетів даних, і саме тут виникають специфічні загрози, такі як атаки на відмову в обслуговуванні (Denial of Service, DoS) або перехоплення даних [1, 3]. Верхнім рівнем базової моделі є рівень додатків, або прикладний рівень, який надає кінцевому користувачеві інтерфейс для взаємодії з системою. Цей рівень відповідає за надання конкретних сервісів, таких як моніторинг розумного будинку, управління трафіком у розумному місті або контроль параметрів здоров'я пацієнта. Він консолідує дані та перетворює їх у корисну інформацію [3].

Однак розвиток технологій та зростання вимог до надійності систем призвели до еволюції архітектурних поглядів. Трирівнева модель часто критикується за відсутність виділених механізмів обробки та безпеки, оскільки в ній дані можуть передаватися від сенсорів до додатків без належної перевірки. У відповідь на це була запропонована чотирирівнева архітектура, яка вводить додатковий проміжний рівень — рівень підтримки (Support Layer) або Middleware. Цей рівень розміщується між мережевим рівнем та рівнем додатків і відіграє критичну роль у забезпеченні безпеки та сумісності. У той час як у трирівневій моделі інформація може надсилатися безпосередньо, рівень підтримки виконує

процеси автентифікації, гарантуючи, що лише авторизовані суб'єкти мають доступ до системи. Крім того, цей рівень часто реалізує функціонал хмарних обчислень, забезпечуючи потужності для зберігання та аналізу великих масивів даних, які не можуть бути оброблені на периферії [2, 3].

Подальше ускладнення бізнес-процесів та необхідність монетизації IoT-рішень спонукали до розробки п'ятирівневої архітектури. Ця модель розширює попередні, додаючи верхівку — бізнес-рівень. Його завдання полягає не в технічному забезпеченні зв'язку, а в управлінні всією екосистемою: створенні бізнес-моделей, аналізі поведінки користувачів, формуванні графіків та діаграм на основі отриманих даних. Бізнес-рівень відповідає за стратегічне прийняття рішень та контроль за дотриманням політик конфіденційності, що є критичним аспектом в умовах обробки персональних даних [3]. У цій моделі також часто виділяють окремий рівень обробки, який фокусується на управлінні великими даними (Big Data), відсіюючи зайву інформацію та зберігаючи лише релевантну, що дозволяє оптимізувати навантаження на мережу [3].

Існують й альтернативні погляди на п'ятирівневу структуру, які фокусуються на топології мережі. Деякі дослідники пропонують виділяти рівень кінцевого користувача, граничний мережевий рівень (Edge Network), базовий мережевий рівень (Core Network), рівень сервісів та рівень управління. Такий підхід підкреслює важливість граничних обчислень (Edge Computing), де первинна обробка даних відбувається на краю мережі, ближче до джерел даних, що зменшує затримки та розвантажує центральні магістралі [1].

З огляду на тематику даного дослідження, особливої уваги заслуговують архітектурні моделі, розроблені спеціально з урахуванням вимог кібербезпеки. Найбільш деталізованою в цьому контексті є семирівнева архітектура. Вона базується на п'ятирівневій моделі, але додатково інтегрує два критично важливі шари. По-перше, це MAC-рівень, який забезпечує управління доступом до середовища передачі, запобігає колізіям та надає механізми ідентифікації пристроїв на каналному рівні. По-друге, це спеціалізований рівень безпеки даних та активів. Введення цього рівня підкреслює, що безпека не може бути лише

функцією окремих додатків або мережевих протоколів; вона повинна бути інтегрована в архітектуру як окрема сутність, що відповідає за захист чутливих даних, боротьбу з вірусами та управління надійністю паролів [3].

Різноманітність архітектурних підходів супроводжується використанням широкого спектра комунікаційних протоколів, що функціонують на різних рівнях моделі. На рівні додатків домінують протоколи, адаптовані для веб-взаємодії та обміну повідомленнями, такі як HTTP, CoAP (Constrained Application Protocol — протокол обмеженого застосування), MQTT та XMPP. Для представлення даних використовуються формати XML або JSON. На мережевому рівні ключову роль відіграє протокол IPv6, зокрема його адаптація для малопотужних мереж — 6LoWPAN, а також протоколи маршрутизації, такі як RPL (Routing Protocol for Low-Power and Lossy Networks — протокол маршрутизації для малопотужних мереж із втратами). Канальний та фізичний рівні характеризуються використанням стандартів IEEE 802.15.4, Bluetooth Low Energy (BLE), Wi-Fi, а також технологій мобільного зв'язку LTE та 5G [1].

Така багаторівнева та гетерогенна структура Інтернету речей створює унікальний ландшафт загроз. Кожен рівень архітектури — від фізичного сприйняття до бізнес-логіки — має свої специфічні вразливості. Наприклад, рівень сприйняття вразливий до фізичного захоплення вузлів, мережевий рівень — до атак на маршрутизацію, а рівень додатків — до шкідливого програмного забезпечення та фішингу. Відсутність єдиної стандартизованої архітектури ускладнює розробку універсальних методів захисту, змушуючи фахівців з кібербезпеки адаптувати стратегії оборони під конкретну реалізацію системи та обраний архітектурний стек [1, 2]. Саме тому аналіз проблематики кібербезпеки вимагає чіткого розуміння того, на якому архітектурному рівні функціонує той чи інший компонент системи та які протоколи забезпечують його взаємодію з іншими елементами інфраструктури.

1.2 Класифікація загроз та вразливостей IoT-систем

Складність та різноманітність архітектури Інтернету речей, детально розглянута у попередньому підрозділі, формує унікальний ландшафт загроз, який суттєво відрізняється від традиційних комп'ютерних мереж. Якщо архітектура визначає структуру взаємодії, то аналіз вразливостей дозволяє зрозуміти, яким чином злоумисники можуть порушити цілісність, конфіденційність або доступність системи. У науковій літературі класифікація загроз часто прив'язується до тривірневої моделі безпеки, відомої як тріада CIA: конфіденційність (Confidentiality), цілісність (Integrity) та доступність (Availability). Порушення конфіденційності в контексті IoT означає несанкціонований доступ до даних, що збираються датчиками або передаються мережею. Порушення цілісності передбачає модифікацію даних під час їх передачі або зберігання, що може призвести до прийняття хибних рішень автоматизованими системами управління. Атаки на доступність, своєю чергою, спрямовані на те, щоб зробити сервіси або пристрої недоступними для легітимних користувачів, що є критичним для систем реального часу [6].

Детальний аналіз загроз доцільно проводити через призму архітектурних рівнів, оскільки кожен з них має специфічні вектори атак. На рівні сприйняття (Perception Layer), де відбувається безпосередній збір даних, пристрої часто знаходяться у фізично незахищеному середовищі, що робить їх вразливими до фізичного захоплення та маніпуляцій. Однією з найпоширеніших загроз на цьому рівні є втручання у вузол (Node Tampering), коли злоумисник фізично замінює або пошкоджує пристрій, а також може викрасти його для вилучення криптографічних ключів. Іншим вектором є вкладання шкідливого коду (Malicious Code Injection), коли атакуючий вводить скомпрометований код у пам'ять вузла для виконання нелегітимних операцій. Оскільки багато датчиків використовують бездротові канали зв'язку, цей рівень також піддається атакам глушіння (Jamming), які створюють радіочастотні перешкоди, блокуючи передачу сигналів між тегами та зчитувачами. Також можливі атаки повторення (Replay Attack), коли злоумисник

перехоплює легітимні повідомлення та повторно надсилає їх для введення системи в оману [6].

Переходячи до мережевого рівня, спектр загроз розширюється, охоплюючи атаки на маршрутизацію та цілісність трафіку. Однією з небезпечних загроз є атака «чорна діра» (Sinkhole Attack), під час якої скомпрометований вузол рекламує себе як найкоротший або найшвидший маршрут до базової станції, змушуючи сусідні вузли перенаправляти весь трафік через нього, після чого дані відкидаються або аналізуються. Спорідненою загрозою є атака Сибілли (Sybil Attack), де один зловмисний вузол представляє декілька ідентичностей у мережі, що дозволяє йому маніпулювати процесами голосування, розподілом ресурсів або маршрутизацією. Крім того, на цьому рівні поширені атаки «людина посередині», коли атакуючий таємно перехоплює та, можливо, змінює повідомлення між двома сторонами, які вважають, що спілкуються безпосередньо одна з одною. Це дозволяє зловмисникам отримувати доступ до конфіденційної інформації ще до того, як вона досягне захищених серверів обробки [6].

На рівні додатків та підтримки загрози стають більш інтелектуальними та спрямовані на логіку роботи сервісів. Тут виділяють атаки міжсайтового скриптингу (Cross Site Scripting, XSS), які дозволяють вбудовувати шкідливі скрипти у веб-сторінки, що переглядаються іншими користувачами, та SQL-ін'єкції, що спрямовані на бази даних, які зберігають інформацію від IoT-пристроїв. Зловмисники можуть використовувати ці вразливості для викрадення даних користувачів або отримання повного контролю над системою управління розумним будинком чи підприємством. Також серйозною проблемою є фішинг, коли користувачів обманом змушують розкрити конфіденційні дані, та розповсюдження шкідливого програмного забезпечення, що маскується під оновлення прошивок або корисні додатки [6].

Сучасна статистика підтверджує теоретичні класифікації та демонструє тривожні тенденції зростання кількості атак. Згідно з дослідженнями, проведеними у 2024 році, однією з домінуючих загроз для споживчого сегмента IoT залишаються атаки типу «відмова в обслуговуванні». Цей тип атак, що

спрямований на вичерпання ресурсів пристрою або пропускної здатності мережі, становить значну частку всіх зареєстрованих інцидентів. Другим за поширеністю вектором є виконання коду (Exec Code), що дозволяє зловмисникам запускати довільні команди на віддалених пристроях. Часто це стає можливим через вразливості переповнення буфера (Buffer Overflow), які виникають, коли програма записує більше даних у буфер, ніж він може вмістити, перезаписуючи сусідні ділянки пам'яті. Такі вразливості є критичними, оскільки вони часто дозволяють отримати повний контроль над пристроєм без необхідності проходження автентифікації [5].

Особливої уваги потребує проблема управління доступом та автентифікацією. Значна кількість інцидентів безпеки пов'язана з використанням слабких паролів або облікових даних за замовчуванням. Багато користувачів не змінюють заводські налаштування, що дозволяє зловмисникам легко сканувати мережу та отримувати доступ до пристроїв, використовуючи загальновідомі пари логін-пароль. Дослідники зазначають, що спроби підбору паролів та використання слабких механізмів автентифікації залишаються одним з найпростіших шляхів проникнення в мережі розумних будинків. Це посилюється тим, що багато споживчих пристроїв, таких як розумні телевізори або розумні розетки, мають тривалий термін експлуатації, але короткий період підтримки з боку виробника, що призводить до накопичення відомих, але не виправлених вразливостей [5]. Розподіл пристроїв за кількістю виявлених вразливостей показано на рис. 1.2.

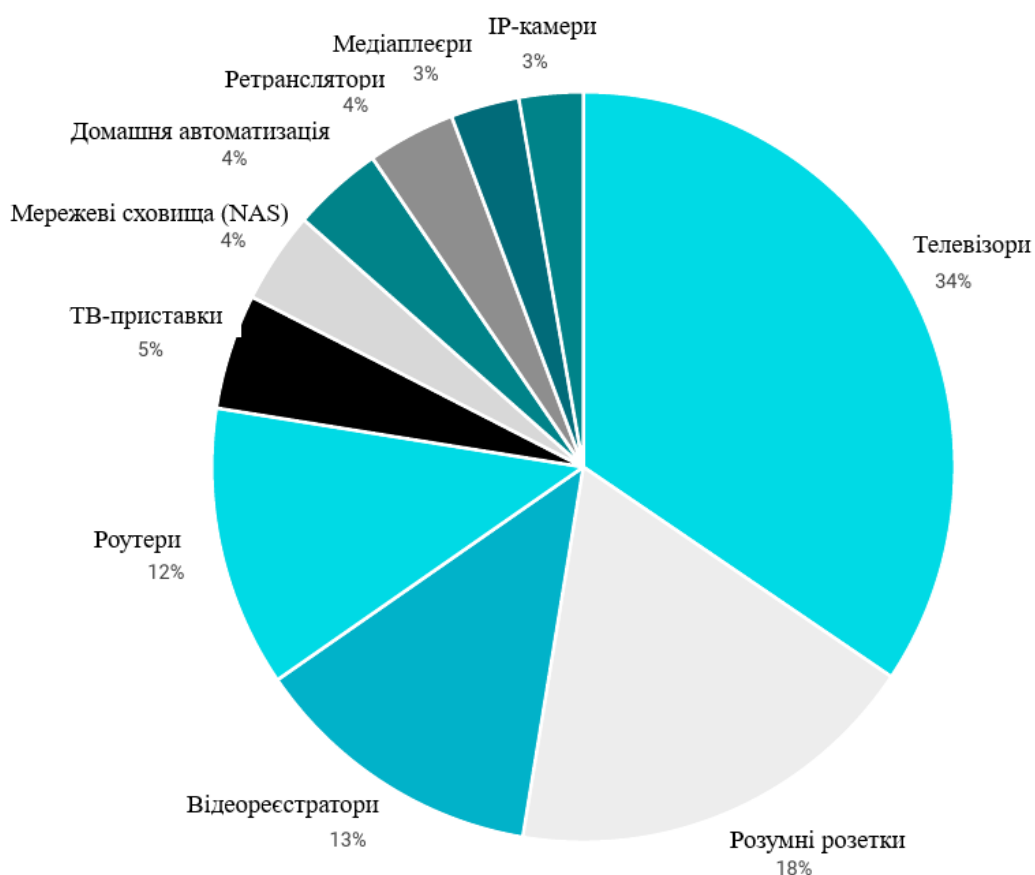


Рисунок 1.2 — Пристрої за кількістю вразливостей [5]

У промисловому секторі та критичній інфраструктурі ситуація ускладнюється злиттям традиційних ІТ-мереж та технологічних процесів. Звіти за 2025 рік вказують на те, що загрози ботнетів залишаються однією з найсерйозніших проблем для IoT-середовищ. Ботнети, такі як варіанти Mirai, продовжують еволюціонувати, використовуючи нові експлойти для зараження пристроїв та об'єднання їх у мережі для здійснення масованих DDoS-атак. Особливістю сучасних ботнетів є їхня здатність атакувати не лише споживчі пристрої, але й промислові контролери та системи автоматизації. Найбільша кількість скомпрометованих пристроїв, що є джерелом ботнет-активності, припадає на США та Китай, а найбільш атакованими секторами глобально є транспорт і виробництво [4].

Окрім зовнішніх атак, критичним фактором ризику є вразливості самого програмного та апаратного забезпечення. Аналіз вразливостей та вразливостей (Common Vulnerabilities and Exposures, CVE), опублікованих у першій половині

2025 року, показує значне зростання кількості виявлених проблем у промислових системах управління. Особливо вразливим є сектор виробництва, де фіксується найбільша кількість повідомлень про вразливості. Це пов'язано з використанням застарілого обладнання, яке важко оновлювати без зупинки виробничих процесів, а також з інтеграцією нових IoT-рішень у старі інфраструктури без належної сегментації мережі. Вразливості часто класифікуються як критичні або високого рівня, що вимагає негайної реакції, проте на практиці процес виправлення у промислових умовах може займати місяці [4].

Ще однією важливою проблемою є вразливості, пов'язані з пам'яттю та логікою обробки даних. Переповнення буфера, про яке згадувалося в контексті споживчих пристроїв, є також поширеним і в промисловому обладнанні. Окрім цього, значну загрозу становлять атаки на веб-інтерфейси управління пристроями. Багато IoT-пристроїв мають вбудовані веб-сервери для конфігурації, які часто містять вразливості типу міжсайтового скриптингу або підробки міжсайтових запитів. Це дозволяє зловмисникам перехоплювати сесії адміністраторів або змушувати пристрої виконувати небажані дії [5].

Поняття «втоми від тривог» (Alert Fatigue) також стає частиною проблематики кібербезпеки IoT. Системи моніторингу безпеки генерують величезну кількість сповіщень про потенційні загрози, значна частина з яких може бути хибнопозитивними або низькопріоритетними. Це призводить до того, що оператори безпеки можуть пропустити справді критичні інциденти серед потоку інформаційного шуму. У промислових мережах, де кількість підключених датчиків може вимірюватися тисячами, ефективна кореляція подій та автоматизація реагування стають необхідними умовами для забезпечення захисту. Без застосування інструментів на базі штучного інтелекту для фільтрації та пріоритизації загроз, традиційні методи моніторингу стають неефективними [4].

Окремо слід розглянути загрози, пов'язані з ланцюгом постачання. Багато IoT-пристроїв збираються з компонентів та програмних бібліотек від різних виробників. Вразливість в одному сторонньому модулі може скомпрометувати тисячі пристроїв різних брендів. Це ускладнюється тим, що кінцеві виробники

пристроїв часто не мають повного контролю над кодом сторонніх компонентів і не можуть оперативно випускати оновлення безпеки. Зловмисники активно використовують це, атакуючи менш захищені елементи ланцюжка постачання для проникнення в цільові мережі. Ця проблема є глобальною і вимагає впровадження стандартизованих вимог до безпеки компонентів на етапі їх проектування та сертифікації [4, 5].

Підсумовуючи класифікацію загроз, можна констатувати, що системи Інтернету речей стикаються з комплексним тиском з боку зловмисників. Вразливості існують на всіх рівнях архітектури: від фізичного доступу до сенсорів і радіоканалів, через мережеві протоколи маршрутизації, до веб-інтерфейсів та хмарних платформ управління. Статистичні дані підтверджують, що найбільш поширеними методами атак залишаються DoS-атаки, експлуатація переповнення буфера та використання слабких паролів. Ефективна стратегія захисту повинна враховувати багатовекторність загроз та застосовувати ешелонований підхід до безпеки, що охоплює як технічні засоби захисту, так і організаційні заходи [4, 5, 6].

1.3 Аналіз наслідків кібератак на IoT-інфраструктуру

Аналіз загроз та вразливостей, проведений у попередніх підрозділах, дозволяє перейти до оцінки реального та потенційного впливу кібератак на функціонування сучасного суспільства. Якщо в традиційних комп'ютерних мережах наслідки інцидентів здебільшого обмежуються втратою інформації або фінансовими збитками, то в екосистемі Інтернету речей кібернетичні загрози трансформуються у фізичні ризики. Це зумовлено природою IoT як кібер-фізичних систем, де цифрові команди безпосередньо керують матеріальними об'єктами: від побутових приладів до турбін електростанцій. Інтеграція IoT у критичну інфраструктуру створює ситуацію, коли успішна атака може призвести до катастрофічних наслідків, включаючи екологічні катастрофи, руйнування обладнання та навіть загрозу життю людей [7].

Одним із найбільш чутливих секторів, що зазнає впливу впровадження IoT, є енергетика, зокрема концепція розумних електромереж. Традиційні електромережі еволюціонували у складні системи двостороннього обміну інформацією та енергією, де мільйони розумних лічильників та датчиків контролюють розподіл навантаження. Наслідки кібератак у цій сфері можуть варіюватися від локальних перебоїв до масштабних блекаутів, що охоплюють цілі регіони. Зловмисники, отримавши доступ до систем диспетчерського управління та збору даних, які інтегровані з IoT-шлюзами, можуть маніпулювати параметрами напруги та частоти струму. Це не лише призводить до відключення споживачів, але й може спричинити фізичне пошкодження дороговартісних трансформаторів та генераторів, відновлення яких вимагає значного часу та ресурсів. Крім того, викрадення даних про енергоспоживання дозволяє зловмисникам профілювати поведінку користувачів, визначаючи їхню присутність вдома, що створює додаткові ризики фізичної безпеки [7].

Не менш критичним є вплив атак на транспортну інфраструктуру та логістику. інтелектуальні транспортні системи, що використовують IoT для управління світлофорами, моніторингу трафіку та комунікації між транспортними засобами, стають привабливою цілью для терористичних актів. Компрометація датчиків або контролерів на транспортних вузлах може призвести до штучного створення заторів, блокування руху екстрених служб або навіть провокування масових дорожньо-транспортних пригод. У залізничному транспорті втручання в системи сигналізації та автоматичного управління поїздами загрожує сходженням потягів з рейок. Оскільки сучасні транспортні засоби все частіше оснащуються модулями зв'язку для телеметрії та оновлення програмного забезпечення, існує ризик віддаленого перехоплення керування автомобілем, що перетворює його на зброю в руках хакерів [7].

Особливу категорію ризиків становлять атаки на системи водопостачання та водовідведення. Датчики IoT у цій сфері використовуються для моніторингу якості води, рівня тиску в трубах та управління хімічним складом для очищення. Успішна кібератака, спрямована на маніпуляцію показниками датчиків, може

призвести до автоматичного додавання надмірної кількості хімікатів, таких як хлор, у питну воду, що спричинить масове отруєння населення. Також можливе відключення насосних станцій, що залишить без води житлові райони та лікарні, або, навпаки, відкриття шлюзів, що призведе до затоплення територій. На відміну від фінансових систем, де транзакції можна скасувати, наслідки таких фізичних маніпуляцій часто є незворотними і вимагають негайної реакції на місці [7].

Економічні наслідки кібератак на IoT-інфраструктуру виходять далеко за межі прямих фінансових втрат від крадіжки коштів. В умовах де виробничі процеси глибоко автоматизовані та взаємопов'язані, навіть короткочасна зупинка конвеєра через DDoS-атаку або вірус-шифрувальник може призвести до зриву контрактів та мільйонних збитків. Складність оцінки економічного впливу полягає в тому, що традиційні моделі ризиків не враховують каскадні ефекти. Порушення роботи одного постачальника в ланцюжку постачання може зупинити виробництво на багатьох суміжних підприємствах [8].

Важливим аспектом аналізу наслідків є також втрата довіри та репутаційні ризики. Оприлюднення інформації про вразливість розумних пристроїв, камер спостереження або дитячих іграшок підриває довіру споживачів до технології в цілому, що може загальмувати інноваційний розвиток галузі. Витік конфіденційних даних, зібраних IoT-пристроями, має більш руйнівні наслідки, ніж витік паролів, оскільки біометричні дані, звички та розклад життя користувача неможливо змінити так само легко, як облікові дані. Це створює довгострокові загрози для приватності та особистої безпеки громадян, які можуть стати об'єктами шантажу або фізичного переслідування на основі викраденої цифрової інформації [6, 8].

Крім того, масове використання вразливих IoT-пристроїв створює глобальну загрозу для стабільності самого Інтернету. Об'єднання мільйонів скомпрометованих пристроїв у ботнети дозволяє зловмисникам генерувати трафік небаченої потужності, здатний вивести з ладу навіть найбільш захищені сервіси та національні сегменти мережі. Наслідком таких атак стає недоступність державних послуг, банківських систем та комунікаційних платформ, що в умовах гібридних

війн може використовуватися як інструмент дестабілізації соціально-політичної ситуації в країні. Зростаюча залежність критичної інфраструктури від IoT робить держави вразливими до кібершпигунства та саботажу з боку ворожих суб'єктів, перетворюючи кібербезпеку IoT на питання національної безпеки [6, 7].

Аналіз наслідків також демонструє, що існуючі методи реагування та відновлення часто є неефективними для IoT-середовища. У традиційних IT-системах заражений комп'ютер можна ізолювати, перевстановити програмне забезпечення та відновити дані з резервної копії. У випадку з IoT, особливо в промисловості та інфраструктурі, фізичне пошкодження обладнання неможливо усунути програмними методами. Заміна скомпрометованих прошивок на тисячах територіально розподілених датчиків може бути логістично неможливою або економічно недоцільною. Це призводить до того, що вразливості залишаються в системі роками, акумулюючи ризики та збільшуючи ймовірність катастрофічних наслідків у майбутньому. Саме тому економічні моделі повинні враховувати не лише вартість захисту, але й повну вартість життєвого циклу пристроїв, включаючи витрати на ліквідацію фізичних наслідків інцидентів [8].

Підсумовуючи, можна стверджувати, що наслідки кібератак на IoT-інфраструктуру мають системний та багатовимірний характер. Вони поєднують у собі прямі матеріальні збитки, загрози життю та здоров'ю людей, порушення приватності, економічні втрати та ризики національній безпеці. Злиття цифрового та фізичного світів призвела до того, що кібербезпека перестала бути виключно технічною дисципліною і стала критичним фактором забезпечення життєдіяльності сучасного суспільства. Розуміння масштабів можливих наслідків вимагає перегляду підходів до проектування систем захисту, переходячи від реактивних методів до превентивних стратегій, що базуються на глибокому аналізі ризиків та впровадженні безпеки на всіх етапах життєвого циклу IoT-систем [7, 8].

1.4 Висновки до розділу 1

У цьому розділі проведено комплексний аналіз проблематики кібербезпеки в системах Інтернету речей. Розглянуто концептуальну будову та архітектурну ієрархію IoT-мереж, простежено еволюцію архітектурних підходів від базової трирівневої моделі до семирівневої, що інтегрує безпеку як окрему архітектурну сутність. Встановлено, що відсутність єдиного стандартизованого еталону архітектури зумовлює необхідність адаптації стратегій захисту під конкретну реалізацію системи та обрані технології.

Визначено ключові архітектурні особливості Інтернету речей, які формують підвищений рівень кіберризиків. Зокрема, з'ясовано, що розміщення кінцевих вузлів у фізично доступному середовищі, обмеженість обчислювальних ресурсів, різноманітність комунікаційних протоколів та відсутність вбудованих засобів криптографічного захисту на більшості сенсорних пристроїв створюють парадоксальну ситуацію, за якої найбільш масовий сегмент мережі Інтернет одночасно є найбільш вразливим.

Здійснено класифікацію загроз IoT-систем за рівнями архітектури з опорою на тріаду інформаційної безпеки — конфіденційність, цілісність та доступність. Встановлено, що рівень сприйняття переважно вразливий до фізичних втручань у вузли, атак глушіння радіоканалу та повторення легітимних повідомлень. Мережевий рівень характеризується ризиками атак «чорна діра», Sybil, а також перехоплення даних за схемою «людина посередині». На рівні додатків та підтримки домінують загрози, спрямовані на логіку роботи сервісів, серед яких міжсайтовий скриптинг, втручання до баз даних, фішинг та розповсюдження шкідливого програмного забезпечення під виглядом легітимних оновлень.

Виявлено, що домінуючими векторами атак на пристрої Інтернету речей залишаються відмова в обслуговуванні, віддалене виконання коду через вразливості переповнення буфера, експлуатація облікових даних за замовчуванням та зараження ботнетами. Окремо встановлено, що для промислового сегмента та критичної інфраструктури характерною є підвищена кількість критичних

вразливостей, ускладнена тривалими циклами оновлення обладнання та інтеграцією сучасних IoT-рішень у застарілу інфраструктуру без належної мережевої сегментації.

Сформульовано наукову проблему дослідження, яка полягає у необхідності побудови комплексної системи захисту мережевої інфраструктури Інтернету речей, здатної компенсувати внутрішні вразливості кінцевих пристроїв засобами активного мережевого обладнання. Результати проведеного аналізу формують теоретичну базу для подальшого обґрунтування вибору конкретних технологій захисту, що буде здійснено у наступному розділі роботи.

2 ОБҐРУНТУВАННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ

2.1 Огляд сучасних підходів до забезпечення безпеки IoT

Аналіз вразливостей та потенційних наслідків кібератак, проведений у першому розділі, переконливо доводить, що традиційні моделі захисту комп'ютерних мереж є недостатньо ефективними для екосистеми Інтернету речей. Класичні методи, що базуються на захисті периметра, виходять із припущення, що всі пристрої та користувачі всередині локальної мережі є довіреними. Однак різноманітність IoT-пристроїв, їхня мобільність та обмеженість вбудованих механізмів безпеки роблять внутрішню мережу вразливою до поширення загроз мережею та інсайдерських атак. У зв'язку з цим сучасна наукова думка зміщує фокус від захисту периметра до комплексних архітектурних рішень, адаптованої криптографії та інтелектуальних систем виявлення вторгнень [9].

Фундаментальною зміною парадигми в безпеці IoT стало впровадження архітектури нульової довіри (Zero Trust Architecture, ZTA). На відміну від традиційного підходу «довіряй, але перевіряй», концепція нульової довіри керується принципом «ніколи не довіряй, завжди перевіряй». Це означає, що жоден пристрій, користувач або сервіс не отримує автоматичної довіри, незалежно від того, знаходиться він всередині корпоративної мережі чи за її межами. У контексті Інтернету речей, де кількість підключених об'єктів зростає експоненційно, ZTA вимагає безперервної автентифікації та авторизації кожного запиту на доступ до ресурсів. Ключовими елементами такої архітектури є контекстно-залежний контроль доступу, який враховує не лише облікові дані, а й поведінку, час доступу та стан безпеки самого пристрою [9].

Реалізація архітектури нульової довіри в IoT-середовищі (ZT-IoT) стикається зі специфічними викликами, пов'язаними з обмеженими обчислювальними ресурсами кінцевих вузлів. Традиційні агенти безпеки можуть бути занадто важкими для простих сенсорів. Тому дослідники пропонують полегшені моделі ZT-IoT, які використовують адаптивну мікросегментацію. Цей метод передбачає розділення мережі на ізольовані сегменти аж до рівня окремих пристроїв, що

унеможливилося поширення атаки у випадку компрометації одного вузла. Важливу роль відіграє також використання протоколу взаємної аутентифікації TLS (Mutual TLS, mTLS), який гарантує, що не тільки сервер перевіряє пристрій, а й пристрій перевіряє легітимність сервера перед початком обміну даними [9].

Невід'ємною складовою будь-якої системи захисту є криптографічні методи, проте стандартні алгоритми шифрування часто виявляються непридатними для IoT. Багато пристроїв Інтернету речей мають критичні обмеження щодо потужності процесора, обсягу оперативної пам'яті та енергоспоживання. Використання важких алгоритмів на таких пристроях призводить до швидкого виснаження батареї та неприпустимих затримок у передачі даних. У відповідь на це виник напрямок легковагової криптографії, що фокусується на розробці алгоритмів, оптимізованих для ресурсів вбудованих систем. Дослідження показують, що ефективність таких алгоритмів оцінюється за трьома основними метриками: швидкість виконання, використання пам'яті (ROM та RAM) та енергоефективність [10].

Серед сучасних підходів до легковагового шифрування виділяють адаптацію блокових та потокових шифрів. Аналіз 22 різних шифрів, проведений у нещодавніх дослідженнях, демонструє, що розробники намагаються знайти баланс між стійкістю до криптоаналізу (зокрема лінійного та диференціального) та продуктивністю. Проте суттєвою проблемою залишається відсутність стандартизованої структури для оцінки цих алгоритмів. Методологічна фрагментація ускладнює об'єктивне порівняння різних рішень, що змушує інженерів обирати методи захисту емпіричним шляхом, часто жертвуючи безпекою заради швидкодії. Тим не менш, впровадження оптимізованих криптографічних примітивів є критично важливим етапом побудови захищеної IoT-мережі [10].

Паралельно з розвитком криптографії та архітектурних моделей, значна увага приділяється децентралізації управління даними та ідентифікацією. Технологія блокчейн, яка спочатку асоціювалася з криптовалютами, знайшла своє застосування в IoT як засіб забезпечення цілісності даних та захисту від

маніпуляцій. Традиційні централізовані системи IoT мають єдину точку відмови — центральний сервер або хмарний шлюз. Якщо зловмисник виведе його з ладу або скомпрометує, під загрозою опиняється вся мережа. Блокчейн пропонує децентралізовану, незмінну та захищену від підробки структуру, де дані зберігаються у розподіленому реєстрі. Це дозволяє реалізувати прозорі механізми аудиту та забезпечити довіру між пристроями, які належать різним адміністративним доменам, без залучення третьої довіреної сторони [11].

Інтеграція блокчейну в IoT дозволяє вирішити низку проблем безпеки, включаючи захист приватності та управління ідентифікацією пристроїв. Смарт-контракти — самовиконувані програмні коди, що зберігаються в блокчейні — можуть автоматизувати процеси контролю доступу та оновлення прошивок, виключаючи людський фактор. Однак, як і у випадку з шифруванням, основною перешкодою залишається ресурсоемність. Класичні алгоритми консенсусу, такі як Proof of Work, є неприйнятними для IoT через високі енерговитрати. Тому сучасні дослідження спрямовані на розробку легковагових механізмів консенсусу та гібридних архітектур, де блокчейн використовується вибірково для критичних транзакцій [11].

Ще одним перспективним напрямком є використання методів штучного інтелекту, зокрема машинного навчання (Machine Learning, ML), для створення адаптивних систем виявлення вторгнень (Intrusion Detection Systems, IDS). Традиційні IDS, що базуються на сигнатурах, ефективні лише проти відомих атак, описи яких вже є в базі даних. В умовах динамічного середовища IoT, де постійно з'являються нові вразливості нульового дня, сигнатурний метод є недостатнім. Системи на базі машинного навчання здатні аналізувати трафік та поведінку пристроїв у реальному часі, виявляючи аномалії, що відхиляються від нормальної поведінки функціонування [12].

Застосування алгоритмів машинного навчання, таких як нейронні мережі, дерева рішень або метод опорних векторів, дозволяє автоматизувати процес класифікації загроз. Кероване навчання (Supervised Learning) використовується для виявлення відомих типів атак на основі маркованих наборів даних, тоді як

некероване навчання (Unsupervised Learning) є ефективним для виявлення нових, раніше невідомих аномалій. Поєднання цих методів у гібридних системах дозволяє значно підвищити точність детектування та знизити рівень хибних спрацювань. Проте впровадження ML-систем вимагає значних обчислювальних потужностей для навчання моделей, що часто передбачає використання граничних обчислень або хмарних ресурсів для обробки телеметрії з IoT-пристроїв [12].

Підсумовуючи огляд сучасних підходів, можна стверджувати, що забезпечення кібербезпеки в мережах IoT вимагає багаторівневої стратегії. Новітні технології, такі як легковагова криптографія, блокчейн та штучний інтелект, пропонують потужні інструменти для протидії складним загрозам. Архітектура нульової довіри виступає концептуальною основою, яка об'єднує ці технології в єдину систему захисту. Однак практична реалізація цих складних рішень часто наштовхується на обмеження апаратного забезпечення та високу вартість впровадження. Тому, незважаючи на ефективність новітніх методів, базовим фундаментом безпеки будь-якої IoT-системи залишається надійне та грамотне налаштування мережевої інфраструктури. Використання перевірених часом методів сегментації мережі, списків контролю доступу та віртуальних локальних мереж (VLAN) дозволяє реалізувати ключові принципи Zero Trust — мінімізацію привілеїв та ізоляцію загроз — використовуючи стандартне мережеве обладнання, що буде детально розглянуто в наступних розділах роботи [9, 11, 12].

2.2 Обґрунтування вибору технологій для реалізації

Вибір технологій для побудови захищеної інфраструктури Інтернету речей не може базуватися на випадкових рішеннях або лише на доступності обладнання. Він повинен бути наслідком глибокого аналізу актуальних загроз, вимог міжнародних стандартів та оцінки готовності сучасних організацій до протидії кіберризикам. У попередньому підрозділі визначено, що концепція нульової довіри (Zero Trust) є стратегічним орієнтиром для безпеки IoT. Проте практична імплементація цієї стратегії вимагає переходу від теоретичних моделей до

конкретних інженерних рішень, здатних забезпечити мережеву стійкість в умовах агресивного кіберсередовища. Обґрунтування вибору технологій для практичної частини цієї роботи спирається на чотири ключові стовпи: необхідність компенсації вразливостей кінцевих пристроїв засобами мережі, протидія специфічним атакам «людина посередині», забезпечення сегментації для локалізації загроз та використання промислових стандартів конфігурації обладнання.

Першим і фундаментальним аргументом на користь вибору мережецентричного підходу до захисту є специфіка самих пристроїв IoT. Однією з головних проблем є неможливість покладатися виключно на вбудовані засоби захисту самих пристроїв. Практика показує, що значна частина IoT-пристроїв, особливо у споживчому та промисловому сегментах, позбавлена критично важливих нетехнічних можливостей, таких як регулярна підтримка виробника, своєчасний випуск оновлень або наявність механізмів оновлення прошивки. Це створює ситуацію, коли організація не може усунути вразливість на самому пристрої, навіть якщо про неї відомо [14].

У зв'язку з цим, вибір технологій захисту зміщується у бік мережевої інфраструктури, яка виступає компенсуючим контролем. Оскільки ми не можемо гарантувати, що сам датчик або контролер здатний протистояти атаці, ми зобов'язані створити навколо нього середовище, яке унеможливило успішну експлуатацію його вразливостей. Це обґрунтовує вибір комутаційного та маршрутизуючого обладнання як основної точки докладання зусиль із захисту. Саме мережеві пристрої повинні взяти на себе функції автентифікації, фільтрації трафіку та ізоляції, які недоступні кінцевим вузлам. Такий підхід дозволяє реалізувати мінімізації ризиків навіть за умови використання потенційно вразливих компонентів [14].

Другим критичним фактором, що визначає вибір технологій, є поточний стан готовності глобальної інфраструктури до кіберзагроз. Згідно зі звітом Cisco Cybersecurity Readiness Index за 2025 рік, лише 3% організацій у світі мають зрілий рівень готовності до сучасних викликів, тоді як 71% знаходяться на

початкових стадіях. Звіт виділяє п'ять основних стовпів захисту: ідентифікаційний інтелект, надійність мережі, захист хмари, укріплення за допомогою штучного інтелекту та довіра до машин. Для контексту даної роботи найбільш релевантним є стовп «Мережева стійкість». Аналітика показує, що традиційні методи захисту периметра за допомогою брандмауерів вже не є достатніми. Звіт прямо вказує на необхідність впровадження сегментації мережі як критично важливого елемента стратегії. Більшість успішних атак на IoT відбувається через те, що після компрометації одного пристрою зловмисник отримує безперешкодний доступ до всієї плоскої мережі [13].

На основі цих даних обґрунтовується вибір технології віртуальних локальних мереж (VLAN) як базового інструменту для реалізації сегментації. VLAN дозволяє логічно розділити пристрої за функціональним призначенням, рівнем довіри або типом трафіку, незалежно від їх фізичного розташування. Це відповідає рекомендаціям щодо необхідності обмеження поширення загроз мережею. Якщо термостат у мережі IoT буде скомпрометований, знаходження його в окремому ізольованому VLAN не дозволить зловмиснику атакувати сервери баз даних або робочі станції адміністраторів, які знаходяться в інших сегментах. Вибір обладнання Cisco для моделювання цієї архітектури є доцільним, оскільки саме ця компанія є лідером у розробці стандартів сегментації та надає найбільш повний інструментарій для її налаштування [13].

Третім аспектом, що диктує вибір специфічних захисних механізмів, є анатомія загроз, характерних саме для IoT-середовища. Дослідження природи атак на Інтернет речей демонструють, що вектори нападу суттєво відрізняються від тих, що застосовуються проти звичайних ПК. Зокрема, детальний аналіз загроз виділяє атаки на мережевому рівні як одні з найбільш деструктивних. Серед них особливе місце займають атаки типу «чорна діра», Wormhole («кротова нора») та Sybil. У атаці «чорна діра» зловмисний вузол намагається привернути до себе весь мережевий трафік, оголошуючи себе найкращим маршрутом до базової станції. Це призводить до перехоплення або знищення даних. Для протидії таким загрозам недостатньо простого антивірусу; необхідні засоби контролю цілісності

маршрутизації та сувора фільтрація трафіку. Це обґрунтовує використання списків контролю доступу на рівні комутаторів та маршрутизаторів. ACL дозволяють створити правила, які чітко регламентують, з якими IP-адресами та по яких портах може спілкуватися кожен конкретний IoT-пристрій, фактично реалізуючи принцип мінімальних привілеїв на мережевому рівні [15].

Крім того, анатомія загроз вказує на високу ймовірність фізичної компрометації вузлів або підключення неавторизованих пристроїв до мережі. Зловмисник може від'єднати легітимну камеру спостереження і підключити свій ноутбук для сканування мережі. Для нейтралізації цього ризику обґрунтованим є вибір технології Port Security. Ця функція комутаторів дозволяє прив'язати конкретну MAC-адресу пристрою до фізичного порту комутатора. У разі спроби підключення пристрою з іншою MAC-адресою, порт автоматично вимикається, блокуючи вторгнення на найбільш ранньому етапі. Такий підхід відповідає рекомендаціям щодо захисту від атак клонування та несанкціонованого доступу [15].

Четвертим і, можливо, найбільш технічно специфічним обґрунтуванням є необхідність захисту від атак типу «людина посередині», які є надзвичайно поширеними в локальних мережах IoT. Дослідження, присвячені саме цьому типу атак, вказують на те, що протокол ARP (Address Resolution Protocol — протокол визначення адрес), який використовується для зіставлення IP-адрес з MAC-адресами, є фундаментально незахищеним. Він не має механізмів автентифікації, що дозволяє зловмиснику надсилати фальшиві ARP-відповіді (також відомо як ARP Spoofing), змушуючи пристрої надсилати трафік через комп'ютер атакуючого замість шлюзу. Це дозволяє перехоплювати конфіденційні дані, модифікувати команди управління або здійснювати DoS-атаки. Оскільки IoT-пристрої часто обмінюються критичними даними в автоматичному режимі, наслідки MitM (Man-in-the-Middle — атака «людина посередині») можуть бути катастрофічними [16].

Для вирішення цієї проблеми у роботі обрано технологію динамічної інспекції ARP (Dynamic ARP Inspection, DAI) у поєднанні з відстеженням DHCP (DHCP Snooping). Ці технології, доступні на комутаторах корпоративного рівня,

таких як Cisco Catalyst, дозволяють створити довірену базу даних пристроїв. Комутатор відстежує процес отримання IP-адреси через DHCP і записує легітимну пару IP-MAC. Будь-який ARP-пакет, який не відповідає цьому запису, автоматично відкидається. Вибір саме цієї комбінації технологій є єдиним надійним способом захисту від ARP Spoofing на канальному рівні без необхідності встановлення додаткового програмного забезпечення на самі IoT-пристрої, що часто неможливо через їх обмежені ресурси. Дослідники прямо вказують на DAI як на ефективний метод превентивного захисту, який усуває першопричину MitM-атак у локальних сегментах [16].

Окрім ARP Spoofing, серйозною загрозою є підробка DNS (DNS Spoofing), коли зловмисник перенаправляє запити пристрою на фальшиві сервери оновлень або управління. Хоча повний захист DNS може бути складним для впровадження на ресурсоємних сенсорах, мережеві засоби захисту дозволяють обмежити доступ пристроїв лише до визначених, довірених DNS-серверів за допомогою тих же ACL, а також контролювати DHCP-відповіді, щоб запобігти підміні адреси DNS-сервера (Rogue DHCP Server). Використання DHCP Snooping з налаштуванням довірених портів гарантує, що лише авторизований DHCP-сервер може надавати мережеві налаштування клієнтам, що нівелює цілий клас атак на інфраструктуру адресації [16].

Варто також звернути увагу на економічний та стратегічний аспект вибору технологій. Звіт Cisco 2025 року підкреслює, що однією з головних проблем є дефіцит кваліфікованих кадрів. Організації стикаються з нестачею фахівців, здатних керувати складними системами безпеки. Це обґрунтовує вибір стандартизованих, широко розповсюджених технологій, вивчення яких є стандартом де-факто для мережевих інженерів. Використання пропрієтарних або екзотичних рішень для захисту IoT може створити ризики неможливості їх обслуговування у майбутньому. Натомість, побудова системи захисту на базі класичних протоколів та інструментів забезпечує довгострокову стійкість та можливість масштабування. Звіт також відзначає зростання ролі штучного інтелекту у захисті, але підкреслює, що базовий рівень гігієни безпеки

(сегментація, управління ідентифікацією, оновлення ПЗ) залишається фундаментом, без якого впровадження ІІІ є неможливим [13].

Окремо слід обґрунтувати відмову від покладання на хмарні засоби захисту як єдиного ешелону оборони. Хоча хмарні платформи надають потужні інструменти аналітики, але втрата зв'язку з хмарию не повинна призводити до повної втрати захищеності локального сегмента. IoT-системи, особливо у критичній інфраструктурі, повинні зберігати стійкість навіть у автономному режимі. Саме тому обрані технології (VLAN, ACL, Port Security, DAI) реалізуються локально на рівні комутаторів доступу та розподілу. Це забезпечує безпеку, коли рішення про блокування загрози приймається максимально близько до джерела, без затримок на передачу даних у хмару та очікування відповіді. Такий підхід мінімізує час реакції на інцидент, що є критичним для запобігання поширенню загроз, які здатні заразити тисячі пристроїв за лічені хвилини [14, 15].

Також необхідно зазначити про важливість моніторингу та видимості. Згідно з аналітикою загроз, багато атак залишаються непоміченими протягом тривалого часу. Вибір керованих комутаторів та маршрутизаторів дозволяє налаштувати дзеркалювання трафіку (SPAN/RSPAN) для подальшого аналізу системами виявлення вторгнень, хоча в рамках даної роботи основний акцент робиться на активних методах запобігання. Проте сама архітектура мережі повинна передбачати можливість підключення засобів моніторингу без порушення технологічних процесів. Створення виділеного VLAN для управління (Management VLAN) та налаштування безпечного віддаленого доступу (SSH замість Telnet) є обов'язковими вимогами, що випливають з рекомендацій щодо захисту адміністративних інтерфейсів, які часто стають цілью для брутфорс-атак [13, 15].

Узагальнюючи вищевикладене, вибір технологій для реалізації практичної частини дипломної роботи формується у вигляді інтегрованого комплексу заходів на каналному та мережевому рівнях моделі OSI. Цей комплекс включає:

1. Сегментацію мережі за допомогою VLAN — для локалізації загроз та реалізації політик нульової довіри відповідно до рекомендацій Cisco щодо мережевої стійкості [13].

2. Списки контролю доступу — для фільтрації трафіку та обмеження взаємодії між сегментами, що компенсує відсутність вбудованих брандмауерів на пристроях IoT [14].

3. Функції безпеки комутаторів (Port Security, DHCP Snooping, Dynamic ARP Inspection) — для нейтралізації специфічних для локальних мереж атак (MitM, Spoofing, несанкціоноване підключення), які ідентифіковані як критичні загрози у дослідженнях [15, 16].

Такий набір технологій є оптимальним з точки зору балансу між ефективністю захисту, вартістю впровадження та вимогами до ресурсів. Він дозволяє побудувати захищену інфраструктуру, яка не залежить від виробників кінцевих пристроїв і здатна протистояти широкому спектру актуальних кіберзагроз, від автоматизованих ботнетів до цілеспрямованих атак перехоплення даних. Обраний підхід повністю відповідає сучасним тенденціям у сфері кібербезпеки та забезпечує виконання вимог щодо надійності, цілісності та доступності сервісів Інтернету речей. Реалізація цих механізмів у середовищі моделювання дозволить наочно продемонструвати їх ефективність та відпрацювати сценарії реагування на інциденти, що є кінцевою метою практичної складової даного дослідження.

2.3 Вибір середовища моделювання

Обґрунтування та вибір технологічних засобів захисту, проведений у попередньому підрозділі, ставить перед дослідником наступне критичне завдання — вибір адекватного інструментарію для верифікації теоретичних викладок. Специфіка Інтернету речей, яка полягає у масовості підключених пристроїв та їхній тісній інтеграції з фізичним світом, робить проведення експериментів на реальному обладнанні фінансово обтяжливим та технічно складним. Побудова

фізичного стенда, що включав би десятки різномірних сенсорів, контролерів, комутаційного обладнання та серверів, вимагає значних капіталовкладень, а також створює ризики пошкодження апаратної частини під час моделювання деструктивних кібератак. Тому в сучасній науковій практиці стандартом де-факто стає використання спеціалізованих програмних середовищ моделювання, які дозволяють створювати віртуальні копії складних мережесих інфраструктур. Вибір конкретного середовища є складним завданням, оскільки воно повинно забезпечувати баланс між точністю емуляції мережесих протоколів та здатністю відтворювати логіку роботи кінцевих пристроїв IoT [17].

На ринку програмного забезпечення для моделювання мереж існує чіткий поділ на емулятори та симулятори, кожен з яких має свої переваги та недоліки в контексті завдань даної роботи. До класу професійних емуляторів належать такі платформи, як GNS3 (Graphical Network Simulator-3) та EVE-NG (Emulated Virtual Environment Next Generation). Ці інструменти дозволяють запускати реальні образи операційних систем мережесого обладнання, зокрема Cisco IOS, Juniper Junos та інших, на віртуальних машинах. Завдяки цьому досягається максимальна наближеність до реальності в частині роботи протоколів маршрутизації (OSPF, EIGRP, BGP) та комутації.

Однак, при переході до специфіки Інтернету речей, функціональні можливості класичних емуляторів виявляються суттєво обмеженими. Головним недоліком GNS3 та EVE-NG у контексті даного дослідження є відсутність нативної підтримки кінцевих пристроїв IoT, таких як сенсори, актуатори, мікроконтролери та розумна побутова техніка. Для того, щоб змоделювати роботу, наприклад, розумної системи освітлення в середовищі GNS3, досліднику довелося б розгортати повноцінну віртуальну машину (наприклад, на базі Linux) для кожної окремої лампочки або вимикача. Такий підхід є вкрай нераціональним з точки зору використання системних ресурсів хост-машини, оскільки запуск десятків віртуальних машин для імітації простих логічних операцій призведе до перевантаження процесора та оперативної пам'яті, що зробить симуляцію нестабільною [17].

Більше того, емулятори мережевого обладнання зазвичай не мають засобів візуалізації фізичних процесів. У GNS3 неможливо наочно побачити, чи ввімкнувся вентилятор при підвищенні температури, або чи спрацювала сирена при виявленні руху. Відсутність візуального зворотного зв'язку ускладнює аналіз коректності роботи сценаріїв автоматизації, які є невід'ємною частиною IoT-систем. Враховуючи, що метою даної роботи є дослідження комплексної безпеки, яка включає не лише захист каналів зв'язку, але й перевірку реакції системи на команди управління, використання "важких" емуляторів є недоцільним.

Альтернативою виступає використання симуляторів, серед яких безперечним лідером в освітньому та науковому сегменті є Cisco Packet Tracer. Це середовище візуального моделювання, розроблене Cisco Systems, яке, на відміну від емуляторів, не запускає реальні образи ОС, а імітує їхню поведінку. Проведений аналіз функціональних можливостей Cisco Packet Tracer останніх версій дозволяє стверджувати, що це середовище є найбільш оптимальним інструментом для реалізації практичної частини даної дипломної роботи. Головним аргументом на користь Packet Tracer є його спеціалізація на Інтернеті речей, що виражається в наявності широкої бібліотеки готових компонентів IoT [19].

Середовище надає користувачеві доступ до великої кількості попередньо налаштованих сенсорів (температури, вологості, руху, диму, газу) та виконавчих механізмів (світлодіоди, сирени, дисплеї). Це дозволяє зосередитися на архітектурі мережі та налаштуванні політик безпеки, не витрачаючи час на створення базових моделей пристроїв з нуля. Важливою перевагою є можливість візуалізації фізичного стану об'єктів: у симуляторі можна спостерігати, як змінюється колір індикатора, відкриваються двері гаража або вмикається система поливу. Така інтерактивність є критично важливою для демонстрації наслідків кібератак. Наприклад, успішна атака на систему опалення може бути наочно продемонстрована через підвищення показників на віртуальному термометрі та зміну стану нагрівального елемента, що робить результати дослідження зрозумілими та переконливими [18].

Ключовим фактором вибору Cisco Packet Tracer для дипломної роботи з кібербезпеки є його підтримка повного стеку мережевих протоколів та функцій захисту, які були обґрунтовані в розділі 2.2. Симулятор дозволяє налаштовувати віртуальні локальні мережі (VLAN) та транкові з'єднання (802.1Q), що необхідно для реалізації сегментації мережі. Він підтримує створення розширених списків контролю доступу (Extended ACL), які фільтрують трафік на основі IP-адрес, портів та протоколів. Також у середовищі реалізовані функції безпеки комутаторів, такі як Port Security для обмеження доступу за MAC-адресами та DHCP Snooping для захисту від підробки DHCP-сервера. Це означає, що всі теоретично обґрунтовані методи захисту можуть бути практично реалізовані та протестовані в межах однієї програми [19].

Особливої уваги заслуговує можливість моделювання серверної інфраструктури IoT. Packet Tracer містить спеціалізовані сервіси, такі як IoT Registration Server, який виконує роль центрального контролера для реєстрації та управління розумними пристроями. Цей сервер дозволяє імітувати веб-інтерфейс управління розумним будинком або промисловим об'єктом, доступний через веб-браузер на віртуальному комп'ютері або смартфоні. Можливість налаштування автентифікації на цьому сервері (ім'я користувача та пароль) дозволяє досліджувати сценарії перехоплення облікових даних та несанкціонованого доступу до панелі управління [17].

Варто також зазначити про можливості аналізу трафіку всередині середовища. Packet Tracer має режим симуляції (Simulation Mode), який дозволяє покроково відстежувати проходження кожного пакету через мережу. Користувач може зупинити час і переглянути вміст заголовків пакетів на кожному рівні моделі OSI — від фізичного до прикладного. Це надає унікальні можливості для налагодження мережі та розуміння механізмів роботи атак. Наприклад, при моделюванні атаки "людина посередині" можна побачити, як змінюються MAC-адреси в заголовках кадрів Ethernet або як ARP-запити поширюються мережею. Така деталізація є недоступною при роботі з реальним обладнанням без використання дорогих апаратних аналізаторів трафіку [18].

Підсумовуючи порівняльний аналіз, можна констатувати, що хоча емулятори типу GNS3 переважають у точності відтворення роботи ядра маршрутизації, Cisco Packet Tracer є безальтернативним вибором для комплексного моделювання систем Інтернету речей. Його унікальна архітектура поєднує в собі достатню для цілей дослідження реалізацію мережевого стеку Cisco IOS з багатьма можливостями емуляції периферійних пристроїв та їх взаємодії з фізичним світом. Візуалізація процесів та режим покрокової інспекції пакетів роблять цей інструмент ідеальним для демонстрації ефективності запропонованих у роботі методів захисту, таких як сегментація VLAN та фільтрація ACL, у зрозумілій та наочній формі. Вибір Cisco Packet Tracer забезпечує наукову достовірність результатів моделювання, дозволяючи перевірити гіпотези дослідження без необхідності створення дороговартісного апаратного полігону [17, 18, 19].

2.4 Висновки до розділу 2

У цьому розділі обґрунтовано вибір методів та засобів забезпечення кібербезпеки мережевої інфраструктури Інтернету речей, а також інструментарію для їх практичної верифікації. Значна частина IoT-пристроїв позбавлена технічних і нетехнічних можливостей самостійного захисту, зокрема механізмів регулярного оновлення прошивки та своєчасного випуску патчів виробником. Це обґрунтовує доцільність застосування мереже-центричного підходу, за якого функції автентифікації, фільтрації трафіку та ізоляції покладаються на активне мережеве обладнання, що виступає компенсуючим контролем для вразливих кінцевих вузлів.

Встановлено, що сегментація мережі є критично важливим елементом сучасної стратегії захисту, оскільки обмежує можливості поширення загроз мережею у разі компрометації окремого пристрою. Як базовий інструмент сегментації обґрунтовано вибір технології віртуальних локальних мереж (VLAN), що дозволяє логічно розділити пристрої за функціональним призначенням та рівнем довіри незалежно від їхнього фізичного розташування.

Сформовано інтегрований комплекс захисних механізмів каналного та мережевого рівнів моделі OSI, який включає сегментацію через VLAN, розширені списки контролю доступу для фільтрації міжсегментного трафіку, технологію Port Security для протидії несанкціонованому фізичному підключенню, а також зв'язки DHCP Snooping та Dynamic ARP Inspection для нейтралізації атак типу Rogue DHCP та ARP Spoofing. Обґрунтовано, що саме така комбінація технологій забезпечує оптимальний баланс між ефективністю захисту, складністю впровадження та вимогами до обчислювальних ресурсів кінцевих пристроїв.

Аргументовано вибір обладнання Cisco Systems та командного інтерфейсу Cisco IOS, що зумовлено стандартизованістю відповідних технологій, їхньою широкою поширеністю в галузі та наявністю кваліфікованих фахівців. Окремо обґрунтовано доцільність реалізації локальних механізмів захисту як доповнення до хмарних платформ, оскільки реалізація захисту на периферії мережі забезпечує стійкість IoT-системи навіть в умовах втрати зв'язку з хмарною інфраструктурою та мінімізує час реакції на інциденти, що критично важливо для протидії масовим автоматизованим загрозам.

На завершення розділу виконано порівняльний аналіз сучасних середовищ моделювання мереж класів емуляторів та симуляторів. Розглянуто можливості професійних платформ GNS3 і EVE-NG, які забезпечують високу точність відтворення роботи реальних образів операційних систем мережевого обладнання, проте мають суттєві обмеження в частині вбудованої підтримки кінцевих IoT-пристроїв. Як оптимальний інструментарій для практичної реалізації обрано симулятор Cisco Packet Tracer, що зумовлено наявністю спеціалізованої бібліотеки сенсорів та виконавчих механізмів, можливістю візуалізації фізичних процесів, а також повною реалізацією набору засобів захисту Cisco IOS, що уможливорює перевірку усіх теоретично обґрунтованих механізмів у межах єдиного середовища.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗАХИСТУ В CISCO PACKET TRACER

3.1 Проектування та базова конфігурація мережі

Для практичної перевірки ефективності запропонованих у попередніх розділах методів захисту було обрано середовище імітаційного моделювання мереж Cisco Packet Tracer. На першому етапі практичної реалізації необхідно спроектувати базову логічну та фізичну топологію мережі, яка б адекватно відображала різноманітність сучасних систем Інтернету речей та дозволяла впроваджувати комплексні механізми безпеки на каналному та мережевому рівнях моделі OSI. В якості базового сценарію було обрано модель корпоративної інфраструктури «Розумний офіс», яка поєднує в собі традиційні робочі станції персоналу, серверну частину та набір сенсорів і виконавчих механізмів IoT.

Архітектура мережі побудована за класичною ієрархічною моделлю, адаптованою під потреби сегментації. Ядром мережі виступає маршрутизатор Cisco ISR4331, який виконує функції міжвіртуальної маршрутизації (Inter-VLAN Routing) за топологією «маршрутизатор на паличці» (Router-on-a-Stick). Рівень розподілу та доступу реалізовано на базі двох комутаторів Cisco Catalyst 2960. Перший комутатор (Switch1) логічно виділено під серверну інфраструктуру та управління, а другий (Switch0) — підключення кінцевих пристроїв користувачів та IoT-компонентів. Така структура обґрунтована необхідністю фізичного та логічного розділення критичних вузлів мережі від потенційно вразливих смарт-пристроїв.

Екосистема IoT у спроектованій топології представлена як дротовими, так і бездротовими компонентами, що відповідає реаліям розгортання розумних середовищ. Для забезпечення бездротового зв'язку до комутатора доступу підключено точку доступу (Access Point), на якій налаштовано базовий захист бездротового каналу за стандартом WPA2-PSK з шифруванням AES. Використання захищеного стандарту на рівні радіоканалу є першим етапом ешелонованої оборони, що змушує потенційного злоумисника шукати шляхи фізичного проникнення в мережу. Серед кінцевих пристроїв IoT використано

мікроконтролер (MCU), RFID-зчитувач, розумні двері, датчик диму та розумний кондиціонер. Звичайні користувачі представлені робочими станціями та ноутбуками. Загальну логічну топологію спроектованої мережі розумного офісу зображено на рис. 3.1.

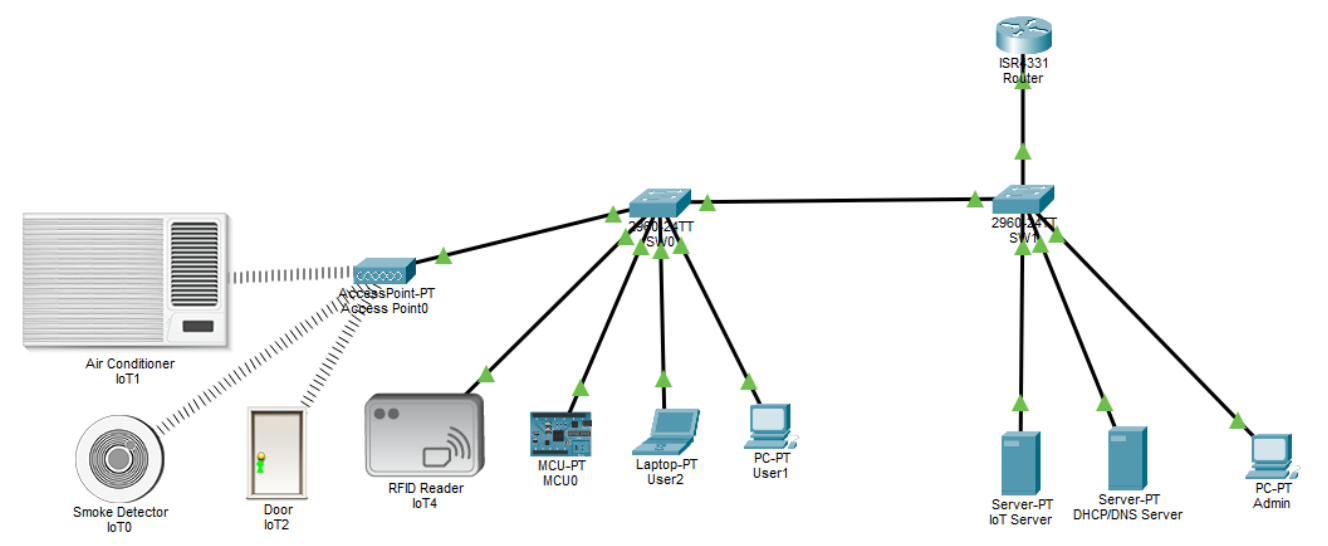


Рисунок 3.1 — Загальна логічна топологія мережі розумного офісу у середовищі Cisco Packet Tracer

Одним із базових принципів архітектури нульової довіри, визначеної як стратегічний орієнтир у розділі 2, є сегментація мережі. Для реалізації цього принципу адресний простір офісу було логічно розділено на чотири незалежні віртуальні локальні мережі (VLAN). Це дозволяє ізолювати сегменти за рівнем довіри та обмежити поширення загрози у випадку компрометації одного з вузлів. Логічну структуру сегментації наведено в Таблиці 3.1.

Таблиця 3.1 — Логічна структура віртуальних локальних мереж (VLAN)

VLAN ID	Назва	Мережева адреса	Опис сегмента
VLAN 10	Servers	192.168.10.0/24	Критична інфраструктура: сервери та робоче місце системного адміністратора.
VLAN 20	IoT_Devices	192.168.20.0/24	Ізольований сегмент для всіх розумних пристроїв (дротових та бездротових).

Продовження таблиці 3.1

VLAN ID	Назва	Мережева адреса	Опис сегмента
VLAN 30	Users	192.168.30.0/24	Користувацький сегмент: ПК співробітників та гостьові пристрої.
VLAN 99	Management	192.168.99.0/24	Мережа для віддаленого управління комутаторами (впровадження SSH).

Розподіл IP-адрес здійснюється за гібридною моделлю. Для серверного обладнання та мережевих інтерфейсів використовуються статичні IP-адреси. Кінцеві пристрої у сегментах VLAN 20 та VLAN 30 отримують мережеві реквізити динамічно від виділеного легітимного DHCP-сервера, що знаходиться у VLAN 10. Детальний план статичної адресації ключових вузлів наведено у Таблиці 3.2.

Таблиця 3.2 — План статичної адресації ключових вузлів мережі

Пристрій	Підключення	IP-адреса	Шлюз за замовчуванням
IoT Server	Switch1	192.168.10.10	192.168.10.1
DHCP/DNS Server	Switch1	192.168.10.11	192.168.10.1
PC-Admin	Switch1	192.168.10.20	192.168.10.1
Switch0 (SVI)	-	192.168.99.10	192.168.99.1
Switch1 (SVI)	-	192.168.99.11	192.168.99.1

Базова конфігурація мережевого обладнання починається з налаштування маршрутизатора ядра. Для забезпечення взаємодії між ізольованими сегментами на фізичному інтерфейсі маршрутизатора створюються логічні сабінтерфейси, кожен з яких інкапсулює трафік відповідного стандарту IEEE 802.1Q та виступає

шлюзом за замовчуванням для своєї підмережі. Фрагмент конфігурації маршрутизатора (R1) наведено нижче:

```
R1(config)# interface GigabitEthernet0/0/0
R1(config-if)# no shutdown
R1(config)# interface GigabitEthernet0/0/0.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
R1(config)# interface GigabitEthernet0/0/0.20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 192.168.20.1 255.255.255.0
```

Аналогічним чином налаштовано сабінтерфейси для VLAN 30 та VLAN 99.

Наступним кроком є конфігурація комутаторів. На рівні розподілу (Switch1) та доступу (Switch0) створюється глобальна база даних VLAN. Магістральні з'єднання (Trunk) між комутаторами та маршрутизатором налаштовуються на пропуск тегового трафіку виключно дозволених ідентифікаторів VLAN, що мінімізує ризики атак на каналному рівні. Порти доступу жорстко прив'язуються до відповідних сегментів. Для доступу до керування самими комутаторами створюються віртуальні інтерфейси (SVI) у виділеному адміністративному VLAN 99.

```
Switch0(config)# vlan 10
Switch0(config-vlan)# name Servers
Switch0(config)# vlan 20
Switch0(config-vlan)# name IoT_Devices
Switch0(config)# interface GigabitEthernet0/1
Switch0(config-if)# switchport mode trunk
Switch0(config-if)# switchport trunk allowed vlan 10,20,30,99
Switch0(config)# interface range FastEthernet0/1-10
Switch0(config-if-range)# switchport mode access
Switch0(config-if-range)# switchport access vlan 20
```

Окремої уваги потребує налаштування служб динамічної конфігурації хостів (DHCP). Оскільки легітимний DHCP-сервер фізично розташований у сегменті VLAN 10, він не може автоматично обробляти широкомовні запити від IoT-пристроїв та користувачів, які знаходяться в інших широкомовних доменах (VLAN 20 та 30). Для вирішення цієї проблеми на рівні маршрутизатора впроваджено функціонал DHCP Relay Agent. На відповідних сабінтерфейсах налаштовано команду `ip helper-address`, яка перехоплює широкомовні DHCP-запити та пересилає їх у вигляді направленого unicast-трафіку безпосередньо на IP-адресу легітимного сервера (192.168.10.11). На самому сервері створено два набори адрес: VLAN20_IoT та VLAN30_Users із відповідними параметрами шлюзів та масок.

Інтеграція IoT-компонентів передбачає їх підключення до централізованого вузла управління — IoT Registration Server. У контексті індустріальних та побутових мереж такі сервери виконують роль контролерів для збору телеметрії та відправки керуючих команд. Щоб забезпечити роботу смарт-пристроїв по бездротовому каналу, їхні стандартні мережеві модулі були замінені на Wi-Fi адаптери, після чого здійснено підключення до точки доступу з використанням налаштованого SSID (Service Set Identifier — ідентифікатор бездротової мережі) та PSK-ключа.

Реєстрація пристроїв на сервері IoT здійснюється через веб-інтерфейс. Враховуючи, що значна частина інцидентів безпеки пов'язана з використанням облікових даних за замовчуванням, при початковому налаштуванні сервера реєстрації, замість стандартних комбінацій було згенеровано складний адміністративний пароль. Це є базовим заходом протидії атакам підбору пароля на панель управління. Після створення облікового запису, кожен смарт-пристрій було автентифіковано на сервері 192.168.10.10. Результат успішної реєстрації смарт-пристроїв на сервері відображено на рис. 3.2.

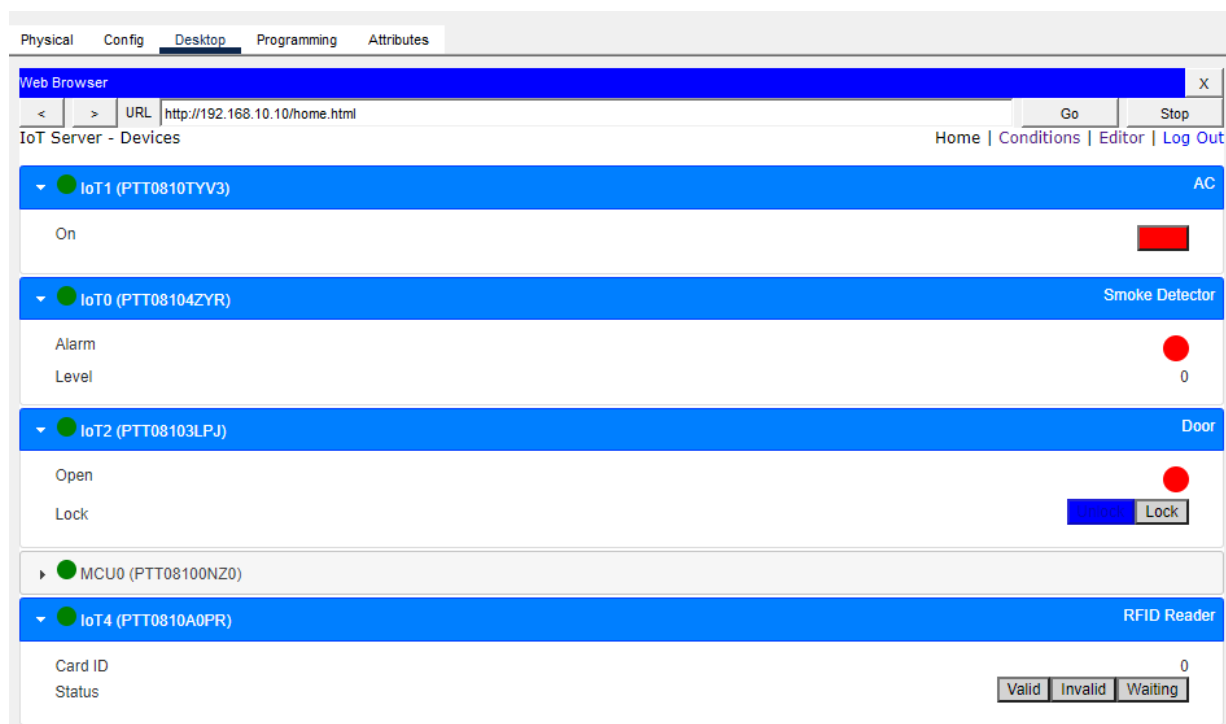


Рисунок 3.2 — Веб-інтерфейс IoT Registration Server з ПК Адміністратора, де відображається список усіх успішно підключених та активних смарт-пристроїв

Завершальним етапом базової конфігурації є перевірка працездатності інфраструктури та зв'язності між вузлами. За допомогою утиліти `ping` та візуального моніторингу статусу пристроїв у `Packet Tracer` було підтверджено, що мікроконтролер, датчики та виконавчі механізми успішно отримали IP-адреси з набору VLAN 20, робочі станції — з набору VLAN 30, а маршрутизація між сегментами функціонує коректно. Підтвердження отримання динамічної адреси та зв'язності з IoT-сервером з боку клієнта наведено на рис. 3.3.

```

User1
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.10.10: bytes=32 time<1ms TTL=127
Reply from 192.168.10.10: bytes=32 time<1ms TTL=127
Reply from 192.168.10.10: bytes=32 time<1ms TTL=127
Reply from 192.168.10.10: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::230:F2FF:FE6C:63B4
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.30.51
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                   192.168.30.1
  
```

Рисунок 3.3 — Командний рядок одного з ПК користувачів, який демонструє успішний ping до IoT сервера та отримання динамічної IP-адреси

Розроблена базова топологія забезпечує повноцінну логічну взаємодію між усіма компонентами розумного офісу. Проте на даному етапі мережа залишається відкритою, оскільки трафік між сегментами ніяк не обмежується, а порти комутаторів відкриті для підключення будь-якого стороннього обладнання. Побудована інфраструктура є ідеальним полігоном для подальшого впровадження політик нульової довіри, списків контролю доступу (ACL) та механізмів канального захисту (Port Security, DHCP Snooping, DAI) для нейтралізації специфічних для IoT кіберзагроз, що буде реалізовано у наступних підрозділах роботи.

3.2 Реалізація механізмів захисту на каналному рівні

Побудована у попередньому підрозділі базова інфраструктура мережі розумного офісу забезпечує повну зв'язність усіх вузлів, проте за своєю природою залишається вразливою до широкого спектра локальних кібератак. Більшість традиційних протоколів каналного рівня, таких як Ethernet та ARP, розроблялися з розрахунком на абсолютну довіру до всіх пристроїв у межах одного широкомовного домену. Враховуючи специфіку пристроїв Інтернету речей, які часто розміщуються у фізично доступних місцях (датчики, камери, розумні двері) та мають обмежені можливості самозахисту, забезпечення безпеки на рівні комутаторів доступу стає першим і найважливішим ешелonom оборони. Реалізація механізмів безпеки на каналному рівні передбачає комплексний підхід, що включає ізоляцію неактивних інтерфейсів, жорстку прив'язку фізичних пристроїв до портів комутатора та впровадження інтелектуальних систем аналізу локального трафіку для протидії атакам типу «людина посередині».

3.2.1 Логічна сегментація та управління неактивними портами

Фундаментальним кроком у реалізації безпеки каналного рівня є мінімізація доступних векторів атаки. Хоча логічна сегментація мережі на віртуальні локальні мережі (VLAN) була закладена на етапі базової конфігурації для розподілу трафіку серверів (VLAN 10), IoT-пристроїв (VLAN 20) та користувачів (VLAN 30), стан фізичних портів комутаторів вимагає окремого адміністративного втручання.

За замовчуванням усі порти комутаторів серії Cisco Catalyst знаходяться в активному стані та належать до стандартного VLAN 1. Якщо зловмисник отримає фізичний доступ до приміщення офісу, він може просто підключити свій портативний комп'ютер до будь-якої вільної мережевої розетки та миттєво отримати доступ до внутрішньої інфраструктури. Для нейтралізації цієї загрози було застосовано принцип заборони за замовчуванням.

Відповідно до кращих практик мережевої безпеки, на комутаторах рівня доступу (Switch0) та серверного рівня (Switch1) було створено спеціальний ізольований сегмент, відомий як «чорна діра» (Blackhole VLAN). Цьому сегменту було присвоєно ідентифікатор VLAN 999. Дана віртуальна мережа не має налаштованого інтерфейсу маршрутизації (SVI) та не маршрутизується в інші сегменти, що робить її повністю відокремленою. Усі невикористані фізичні порти були примусово переведені в режим доступу (access mode), призначені до VLAN 999 та адміністративно вимкнені командою shutdown.

Фрагмент конфігурації для ізоляції портів на комутаторі доступу Switch0:

```
Switch0(config)# vlan 999
Switch0(config-vlan)# name Blackhole
Switch0(config-vlan)# exit
Switch0(config)# interface range FastEthernet0/4-10, FastEthernet0/13-24,
GigabitEthernet0/2
Switch0(config-if-range)# switchport mode access
Switch0(config-if-range)# switchport access vlan 999
Switch0(config-if-range)# shutdown
```

Аналогічні дії були виконані на серверному комутаторі Switch1 для портів FastEthernet0/4-24. Результатом цієї конфігурації є те, що активними залишаються виключно ті порти, до яких підключені легітимні пристрої нашої топології. Статус портів та їх приналежність до VLAN для комутаторів Switch0 і Switch1 показано на рис. 3.4 і рис. 3.5 відповідно.

Device Name: SW0				
Custom Device Model: 2960 IOS15				
Hostname: Switch0				
Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	20	--	0001.425E.B001
FastEthernet0/2	Up	20	--	0001.425E.B002
FastEthernet0/3	Up	20	--	0001.425E.B003
FastEthernet0/4	Down	999	--	0001.425E.B004
FastEthernet0/5	Down	999	--	0001.425E.B005
FastEthernet0/6	Down	999	--	0001.425E.B006
FastEthernet0/7	Down	999	--	0001.425E.B007
FastEthernet0/8	Down	999	--	0001.425E.B008
FastEthernet0/9	Down	999	--	0001.425E.B009
FastEthernet0/10	Down	999	--	0001.425E.B00A
FastEthernet0/11	Up	30	--	0001.425E.B00B
FastEthernet0/12	Up	30	--	0001.425E.B00C
FastEthernet0/13	Down	999	--	0001.425E.B00D
FastEthernet0/14	Down	999	--	0001.425E.B00E
FastEthernet0/15	Down	999	--	0001.425E.B00F
FastEthernet0/16	Down	999	--	0001.425E.B010
FastEthernet0/17	Down	999	--	0001.425E.B011
FastEthernet0/18	Down	999	--	0001.425E.B012
FastEthernet0/19	Down	999	--	0001.425E.B013
FastEthernet0/20	Down	999	--	0001.425E.B014
FastEthernet0/21	Down	999	--	0001.425E.B015
FastEthernet0/22	Down	999	--	0001.425E.B016
FastEthernet0/23	Down	999	--	0001.425E.B017
FastEthernet0/24	Down	999	--	0001.425E.B018
GigabitEthernet0/1	Up	--	--	0001.425E.B019
GigabitEthernet0/2	Down	999	--	0001.425E.B01A
Vlan1	Down	1	<not set>	0030.F211.9DCB
Vlan99	Up	99	192.168.99.10/24	0030.F211.9D01

Рисунок 3.4 — Статус портів Switch0 та їх приналежність до VLAN

Device Name: SW1				
Custom Device Model: 2960 IOS15				
Hostname: Switch1				
Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	10	--	0001.97C9.7101
FastEthernet0/2	Up	10	--	0001.97C9.7102
FastEthernet0/3	Up	10	--	0001.97C9.7103
FastEthernet0/4	Down	999	--	0001.97C9.7104
FastEthernet0/5	Down	999	--	0001.97C9.7105
FastEthernet0/6	Down	999	--	0001.97C9.7106
FastEthernet0/7	Down	999	--	0001.97C9.7107
FastEthernet0/8	Down	999	--	0001.97C9.7108
FastEthernet0/9	Down	999	--	0001.97C9.7109
FastEthernet0/10	Down	999	--	0001.97C9.710A
FastEthernet0/11	Down	999	--	0001.97C9.710B
FastEthernet0/12	Down	999	--	0001.97C9.710C
FastEthernet0/13	Down	999	--	0001.97C9.710D
FastEthernet0/14	Down	999	--	0001.97C9.710E
FastEthernet0/15	Down	999	--	0001.97C9.710F
FastEthernet0/16	Down	999	--	0001.97C9.7110
FastEthernet0/17	Down	999	--	0001.97C9.7111
FastEthernet0/18	Down	999	--	0001.97C9.7112
FastEthernet0/19	Down	999	--	0001.97C9.7113
FastEthernet0/20	Down	999	--	0001.97C9.7114
FastEthernet0/21	Down	999	--	0001.97C9.7115
FastEthernet0/22	Down	999	--	0001.97C9.7116
FastEthernet0/23	Down	999	--	0001.97C9.7117
FastEthernet0/24	Down	999	--	0001.97C9.7118
GigabitEthernet0/1	Up	--	--	0001.97C9.7119
GigabitEthernet0/2	Up	--	--	0001.97C9.711A

Рисунок 3.5 — Статус портів Switch1 та їх приналежність до VLAN

3.2.2 Налаштування безпеки портів (Port Security)

Наступним вектором атак, характерним для IoT-середовища, є несанкціоноване відключення легітимного пристрою з подальшим підключенням замість нього обладнання зловмисника, або використання методів підміни MAC-адреси (MAC Spoofing). Оскільки зловмисник використовує вже існуючий і легітимно увімкнений порт, попередній метод захисту тут безсилий.

Для вирішення цієї проблеми на комутаторі доступу Switch0 було впроваджено технологію Port Security. Ця функція дозволяє регламентувати кількість та конкретні значення MAC-адрес пристроїв, яким дозволено передавати кадри через певний порт. У випадку порушення політики безпеки комутатор автоматично блокує інтерфейс, переводячи його у стан помилки (err-disable), та генерує відповідне системне повідомлення.

На портах, до яких підключені дротові IoT-компоненти (мікроконтролер, RFID-зчитувач, розумні двері) та робочі станції користувачів, було встановлено жорстке обмеження: дозволено підключення лише однієї MAC-адреси (maximum 1). Для спрощення адміністрування було використано метод динамічного закріплення MAC-адрес (Sticky MAC). При такій конфігурації комутатор автоматично вивчає першу MAC-адресу, від якої отримує кадр, та постійно зберігає її в конфігураційному файлі (running-config).

Приклад конфігурації Port Security для порту користувача на комутаторі Switch0:

```
Switch0(config)# interface range FastEthernet0/2-3, FastEthernet0/11-12
Switch0(config-if-range)# switchport port-security
Switch0(config-if-range)# switchport port-security maximum 1
Switch0(config-if-range)# switchport port-security mac-address sticky
Switch0(config-if-range)# switchport port-security violation shutdown
```

Окремої уваги та інженерного обґрунтування потребує налаштування Port Security на порту FastEthernet0/1, до якого підключена автономна точка доступу, що забезпечує зв'язок для бездротових сенсорів та виконавчих механізмів. Точка

доступу функціонує як прозорий міст канального рівня, тому комутатор отримує кадри з різними MAC-адресами від кожного бездротового клієнта, який до неї підключений. Застосування правила *maximum 1* на такому порту неминуче призведе до хибного спрацювання системи безпеки та блокування всього бездротового сегмента при спробі другого пристрою відправити дані. Для забезпечення безперебійної роботи бездротового IoT-сегмента на цьому конкретному інтерфейсі ліміт дозволених MAC-адрес був збільшений пропорційно до кількості очікуваних бездротових вузлів (у рамках даної моделі було встановлено значення *maximum 5*). Слід зазначити, що у великих корпоративних інфраструктурах використання класичного статичного Port Security на портах із точками доступу є менш ефективним. У реальних розгортаннях для захисту бездротових сегментів доцільніше застосовувати архітектуру на базі бездротових контролерів (Wireless LAN Controller, WLC) та протоколу управління CAPWAP (Control and Provisioning of Wireless Access Points — протокол управління та забезпечення бездротових точок доступу), або динамічну автентифікацію на базі порту за стандартом IEEE 802.1X із залученням RADIUS-сервера.

3.2.3 Впровадження захисту від атак типу «людина посередині»

Незважаючи на те, що Port Security надійно захищає від фізичного втручання, він не здатен запобігти логічним атакам, які можуть здійснюватися зі скомпрометованих, але легітимних пристроїв. В інфраструктурі розумного офісу IoT-пристрої здійснюють автоматизований обмін даними, покладаючись на механізми динамічного отримання IP-адрес (DHCP) та протокол визначення адрес (ARP). Обидва ці протоколи не мають вбудованих механізмів автентифікації. Це відкриває можливість для реалізації атак типу Rogue DHCP Server (підключення фальшивого сервера, який видає хибні IP-адреси та шлюзи) та ARP Spoofing (підміна ARP-відповідей для перехоплення трафіку або реалізації MitM-атак).

Для комплексного вирішення цих проблем на комутаторі доступу Switch0 було розгорнуто зв'язку технологій DHCP Snooping та Dynamic ARP Inspection. Першим етапом є налаштування функції DHCP Snooping. Дана технологія дозволяє комутатору інспектувати всі DHCP-повідомлення в мережі та відкидати нелегітимні відповіді від фальшивих серверів. Принцип роботи базується на поділі всіх портів комутатора на довірені (Trusted) та недовірені (Untrusted). Довіреним портом на Switch0 було призначено магістральний інтерфейс GigabitEthernet0/1 (Trunk), оскільки саме через нього пролягає шлях до легітимного DHCP-сервера, розташованого у VLAN 10. Усі інші порти доступу за замовчуванням залишаються недовіреними, і будь-які пакети DHCP OFFER або DHCP ACK, що надходять з них, автоматично блокуються комутатором. Одночасно з фільтрацією пакетів, процес DHCP Snooping створює критично важливий елемент безпеки — базу даних прив'язок. У цій базі комутатор динамічно реєструє легітимні відповідності між MAC-адресою пристрою, його отриманою IP-адресою, номером порту та приналежністю до VLAN.

Налаштування DHCP Snooping на Switch0:

```
Switch0(config)# ip dhcp snooping
```

```
Switch0(config)# ip dhcp snooping vlan 20,30
```

```
Switch0(config)# interface GigabitEthernet0/1
```

```
Switch0(config-if)# ip dhcp snooping trust
```

Наявність бази даних прив'язок дозволяє реалізувати другий етап захисту — динамічну інспекцію ARP (DAI). Протокол ARP використовується для зіставлення логічної IP-адреси з фізичною MAC-адресою. Уразливість полягає в тому, що пристрій може надіслати підроблену ARP-відповідь, навіть якщо його про це не запитували, і змусити інші вузли оновити свої ARP-таблиці хибними даними. Після увімкнення DAI на комутаторі Switch0, кожен ARP-пакет, що надходить з недовіреного порту, піддається перевірці. Комутатор перехоплює пакет і порівнює його вміст, IP та MAC-адресу відправника, з даними, що зберігаються у базі даних прив'язок. Якщо інформація збігається — пакет пропускається. Якщо виявляється розбіжність (наприклад, зловмисник намагається представитися шлюзом або IoT-

сервером, надсилаючи свій MAC разом із чужим IP) — комутатор негайно відкидає такий ARP-пакет і генерує запис у системному журналі. Інтерфейс Trunk до ядра мережі також було налаштовано як довірений для інспекції ARP.

Налаштування Dynamic ARP Inspection на Switch0:

```
Switch0(config)# ip arp inspection vlan 20,30
```

```
Switch0(config)# interface GigabitEthernet0/1
```

```
Switch0(config-if)# ip arp inspection trust
```

Таким чином, комплексна реалізація механізмів безпеки на каналному рівні дозволила трансформувати базову інфраструктуру у високозахищене середовище. Сегментація, відключення невикористаних портів та впровадження Port Security унеможливили фізичне підключення неавторизованого обладнання. Своєю чергою, технології DHCP Snooping та DAI гарантують цілісність інфраструктури адресації та унеможливлюють реалізацію локальних атак перехоплення трафіку, формуючи надійний фундамент для подальшого впровадження засобів контролю доступу на мережевому рівні, що буде розглянуто в наступному підрозділі.

3.3 Налаштування безпеки мережевого рівня та фільтрації трафіку

Впровадження механізмів каналного рівня, описаних у попередньому підрозділі, надійно захищає інфраструктуру розумного офісу від локальних загроз та атак підміни ідентифікаторів. Проте, оскільки ядром мережі виступає маршрутизатор (у нашій топології — R1), за замовчуванням він здійснює безперешкодну маршрутизацію (Inter-VLAN Routing) між усіма підключеними віртуальними мережами. Це означає, що у випадку успішної компрометації IoT-пристрою (наприклад, розумного кондиціонера у VLAN 20), зловмисник зможе ініціювати мережеві з'єднання з робочими станціями користувачів (VLAN 30) або критичними серверами, обходячи каналні блокування.

Для вирішення цієї проблеми та реалізації концепції нульової довіри необхідно перейти до захисту на мережевому рівні шляхом жорсткого регламентування взаємодії між сегментами. Використання списків контролю

доступу дозволяє реалізувати ключові принципи Zero Trust — мінімізацію привілеїв та ізоляцію загроз. Крім того, ACL компенсують відсутність вбудованих брандмауерів на пристроях IoT.

3.3.1 Впровадження списків контролю доступу

Для обмеження несанкціонованої мережевої активності з боку смарт-пристроїв на маршрутизаторі R1 було розроблено та застосовано розширений іменований список доступу IOT_RESTRICT. Політика безпеки для цього списку базується на принципі «заборонено все, що не дозволено явно».

Логіка створеного списку доступу передбачає наступні правила:

1. IoT-пристроєм (мережа 192.168.20.0/24) дозволено надсилати UDP-запити до легітимного DHCP-сервера (192.168.10.11) для отримання мережевих налаштувань.
2. Смарт-пристроєм дозволено обмінюватися даними виключно з центральним сервером управління IoT (192.168.10.10).
3. Явно заборонено ініціювання будь-яких з'єднань від IoT-пристроїв до робочої станції адміністратора (192.168.10.20) та до всього клієнтського сегмента користувачів (192.168.30.0/24).

Список доступу застосовується на вхідному напрямку (inbound) сабінтерфейсу маршрутизатора, який обслуговує VLAN 20. Це означає, що небажаний трафік відкидається маршрутизатором ще до етапу прийняття рішення про маршрутизацію, що заощаджує ресурси процесора.

Фрагмент конфігурації маршрутизатора R1 для впровадження ACL:

```
R1(config)# ip access-list extended IOT_RESTRICT
R1(config-ext-nacl)# permit udp 192.168.20.0 0.0.0.255 host 192.168.10.11 eq
bootps
R1(config-ext-nacl)# permit ip 192.168.20.0 0.0.0.255 host 192.168.10.10
R1(config-ext-nacl)# deny ip 192.168.20.0 0.0.0.255 host 192.168.10.20
R1(config-ext-nacl)# deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
```

```
R1(config-ext-nacl)# deny ip any any
```

```
R1(config)# interface GigabitEthernet0/0/0.20
```

```
R1(config-subif)# ip access-group IOT_RESTRICT in
```

Результат застосування розширеного списку контролю доступу на маршрутизаторі наведено на рис. 3.6.

```
R1#show access-lists
Extended IP access list IOT_RESTRICT
 10 permit udp 192.168.20.0 0.0.0.255 host 192.168.10.11 eq bootps
 20 permit ip 192.168.20.0 0.0.0.255 host 192.168.10.10 (34 match(es))
 30 deny ip 192.168.20.0 0.0.0.255 host 192.168.10.20
 40 deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
 60 deny ip any any
```

Рисунок 3.6 — Результати налаштування розширеного списку контролю доступу на маршрутизаторі

3.3.2 Налаштування захищеного віддаленого керування (SSH)

Створення виділеного VLAN для управління (Management VLAN) та налаштування безпечного віддаленого доступу є обов'язковими вимогами для захисту адміністративних інтерфейсів, які часто стають ціллю для атак підбору паролей. Протокол Telnet, який традиційно використовувався для базового налаштування, передає всю інформацію, включаючи автентифікаційні дані та адміністративні команди, у відкритому вигляді. У разі перехоплення такого трафіку зломисник може миттєво отримати повний контроль над ядром мережі.

Для захисту каналу управління на всьому мережевому обладнанні (маршрутизатор R1, комутатори Switch0 та Switch1) було впроваджено протокол Secure Shell (SSH) версії 2. Налаштування включало генерацію криптографічних ключів RSA з довжиною 2048 біт, що відповідає сучасним стандартам криптографічної стійкості. Також було створено локальну базу даних користувачів із використанням стійкого пароля та налаштовано віртуальні термінальні лінії (VTY) на прийом виключно SSH-з'єднань.

Фрагмент конфігурації для налаштування SSH (на прикладі комутатора доступу Switch0):

```
Switch0(config)# ip domain-name smartoffice.local  
Switch0(config)# crypto key generate rsa  
How many bits in the modulus [512]: 2048  
Switch0(config)# username admin secret Secur3@ccess2026!  
Switch0(config)# line vty 0 15  
Switch0(config-line)# login local  
Switch0(config-line)# transport input ssh
```

Додатковим організаційно-технічним заходом стало налаштування банера попередження (Message of the Day, MOTD), який інформує про заборону несанкціонованого доступу. Хоча банер не є криптографічним засобом захисту, його наявність виконує превентивну функцію та має важливе юридичне значення при фіксації кіберінцидентів.

Перевірка працездатності механізмів захищеного управління здійснювалася з робочої станції адміністратора (PC-Admin). Спроби підключитися до обладнання за допомогою вразливого протоколу Telnet автоматично відхилялися пристроями. Натомість підключення через клієнт SSH завершилося успішно після проходження автентифікації. Процес захищеного підключення за протоколом SSH з відображенням попереджувального банера показано на рис. 3.7.

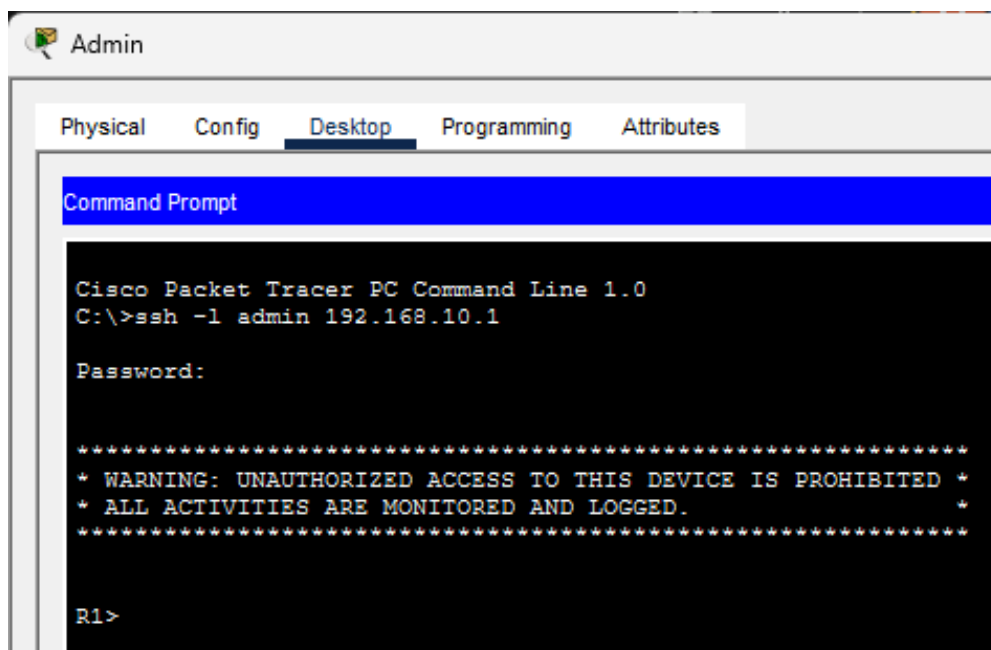


Рисунок 3.7 — Демонстрація захищеного віддаленого підключення до маршрутизатора за протоколом SSH з відображенням попереджувального банера

Таким чином, налаштування механізмів безпеки мережевого рівня завершило формування ешелонованої системи захисту. Списки контролю доступу унеможливили компрометацію суміжних сегментів через вразливі IoT-пристрої, а впровадження протоколу SSH та локальних баз автентифікації гарантує конфіденційність та цілісність каналів управління мережевою інфраструктурою.

3.4 Імітаційне моделювання атак та тестування ефективності системи захисту

Завершальним етапом практичної частини дослідження є верифікація працездатності розгорнутого комплексу засобів безпеки. Теоретичний аналіз вразливостей інфраструктури Інтернету речей доводить, що статичного налаштування захисних механізмів недостатньо; система повинна демонструвати стійкість в умовах активного кібернетичного впливу. Для перевірки надійності побудованої архітектури розумного офісу в середовищі Cisco Packet Tracer було змодельовано три класичні сценарії атак, які охоплюють різні рівні моделі OSI та

різні вектори проникнення: від фізичного доступу до логічних маніпуляцій з протоколами маршрутизації.

Методологія тестування для кожного сценарію базується на двофазному підході. На першому етапі описується вектор атаки та його потенційні наслідки для незахищеної мережі. На другому етапі імітується безпосередня дія зловмисника в середовищі моделювання, фіксується реакція налаштованих захисних механізмів (комутаторів та маршрутизатора) та аналізується результат.

3.4.1 Сценарій 1: Фізичне проникнення та спроба неавторизованого підключення

Одним із найпоширеніших векторів атак на рівні сприйняття є фізичне втручання у вузол або несанкціоноване підключення до мережевої інфраструктури. У типовому офісі зловмисник (інсайдер або відвідувач) може від'єднати кабель від легітимного пристрою (наприклад, ПК співробітника або дротового сенсора) та підключити власний портативний комп'ютер. У незахищеній мережі це дозволяє миттєво отримати IP-адресу по DHCP, розпочати сканування портів та ініціювати атаки на інші вузли.

Для імітації даної атаки в топології було використано вузол Laptop-PT Hacker. На етапі нормального функціонування мережі легітимний комп'ютер PC-User1 був підключений до порту FastEthernet0/11 комутатора Switch0. Оскільки на цьому порту було налаштовано механізм Port Security з динамічним вивченням адреси комутатор зберіг MAC-адресу легітимного ПК у своїй конфігурації. Згідно зі сценарієм, з'єднання з PC-User1 було розірвано, а до порту FastEthernet0/11 підключено ноутбук зловмисника, який має відмінну фізичну MAC-адресу мережевого адаптера. Щойно ноутбук хакера спробував ініціювати мережеву активність (відправити DHCP-запит для отримання адреси), комутатор перехопив цей кадр та здійснив перевірку вихідної MAC-адреси на відповідність базі даних дозволених адрес. Оскільки MAC-адреса хакера не збіглася із легітимною адресою, збереженою правилом maximum 1, спрацювала політика порушення

violation shutdown. Мережевий порт був миттєво заблокований та переведений у стан err-disable. У консолі комутатора було згенеровано системні повідомлення високого рівня критичності: «%PM-4-ERR_DISABLE та %PORT_SECURITY-2-PSECURE_VIOLATION». Спрацювання механізму Port Security у консолі комутатора Switch0 зафіксовано на рис. 3.8.

```
SW0

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11, changed state to down
%PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/11, putting Fa0/11 in err-disable state.
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 000D.BD52.8AD0 on port FastEthernet0/11

Switch0#show port-security interface f0/11
Port Security          : Enabled
Port Status            : Secure-shutdown
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 1
Total MAC Addresses    : 1
Configured MAC Addresses : 0
Sticky MAC Addresses   : 1
Last Source Address:Vlan : 000D.BD52.8AD0:30
Security Violation Count : 1

Switch0#
```

Рисунок 3.8 — Спрацювання захисту PSECURE_VIOLATION у консолі Switch0

Цей експеримент практично доводить ефективність застосування Port Security як першого ешелону оборони, що нівелює ризики фізичної компрометації каналного рівня.

3.4.2 Сценарій 2: Атака підміни ідентифікатора (MAC Spoofing) та спроба поширення загроз мережею

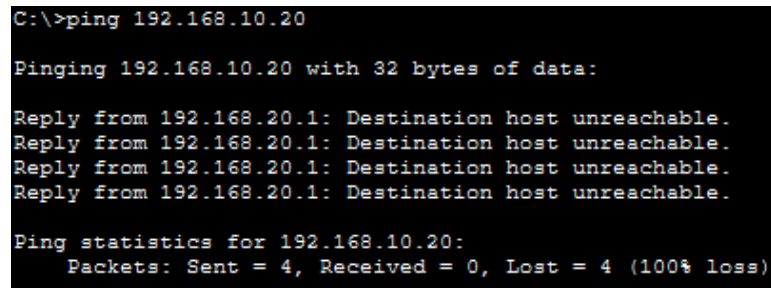
Статичні механізми захисту каналного рівня, такі як Port Security, є ефективними проти базових спроб несанкціонованого підключення, проте не гарантують абсолютної безпеки у випадку цілеспрямованої атаки кваліфікованого зловмисника. Знаючи або перехопивши фізичну MAC адресу легітимного пристрою, хакер може застосувати техніку клонування адреси (MAC Spoofing). Успішно підмінивши ідентифікатор свого мережевого адаптера, зловмисник обходить блокування порту комутатора, отримує легітимну IP-адресу в сегменті

IoT та намагається просканувати інші сегменти для атаки на критичні вузли (наприклад, сервер управління або ПК адміністратора).

Для імітації даної комплексної атаки змодельовано ситуацію, в якій зловмисник тимчасово відключив легітимний мікроконтролер від порту у сегменті VLAN 20 та зчитав його MAC-адресу. На мережевому адаптері портативного комп'ютера хакера (Laptop-PT Hacker) було змінено апаратну адресу на ідентичну легітимній. Після підключення до комутатора механізм Port Security був успішно введений в оману: порт залишився в активному стані, а пристрій зловмисника отримав динамічну IP-адресу з списку IoT-сегмента.

Отримавши логічний доступ до мережі, зловмисник ініціював спробу мережевого розвідки та доступу до високопріоритетного сегмента VLAN 10. За допомогою консолі було відправлено серію ICMP-запитів (ping) на цільову IP-адресу робочої станції системного адміністратора (192.168.10.20).

Хоча зловмиснику вдалося подолати перший рубіж оборони на каналному рівні, його мережева активність була зупинена на рівні маршрутизації. Пакети від комп'ютера хакера надійшли на шлюз за замовчуванням — сабінтерфейс маршрутизатора R1 (g0/0/0.20). Операційна система маршрутизатора проаналізувала заголовок мережевого рівня згідно з правилами розширеного списку контролю доступу IOT_RESTRICT. Виявивши, що IP-адреса джерела належить до списку 192.168.20.0/24, а адресою призначення є захищений хост 192.168.10.20, маршрутизатор застосував правило заборони. Небажаний трафік був негайно відкинутий, у консолі зловмисника відобразилося повідомлення від шлюзу «Вузол призначення недосяжний». Результат блокування ICMP-запиту з боку зловмисника та відповідні лічильники спрацювань списку доступу наведено на рис. 3.9 і рис. 3.10.



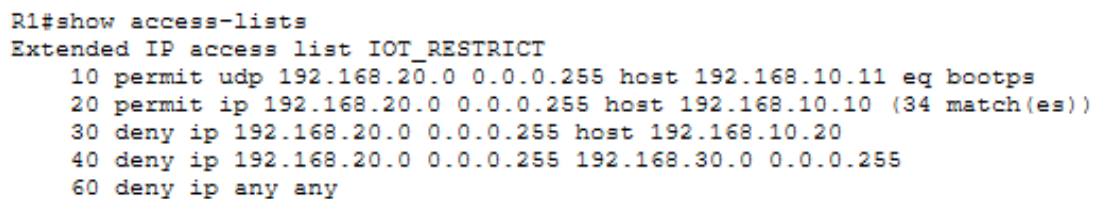
```
C:\>ping 192.168.10.20

Pinging 192.168.10.20 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 192.168.10.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

Рисунок 3.9 — Скриншот консолі Laptop-PT Hacker із заблокованим ICMP-запитом (повідомлення «Destination host unreachable»)



```
R1#show access-lists
Extended IP access list IOT_RESTRICT
 10 permit udp 192.168.20.0 0.0.0.255 host 192.168.10.11 eq bootps
 20 permit ip 192.168.20.0 0.0.0.255 host 192.168.10.10 (34 match(es))
 30 deny ip 192.168.20.0 0.0.0.255 host 192.168.10.20
 40 deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
 60 deny ip any any
```

Рисунок 3.10 — Вивід команди «show access-lists» на маршрутизаторі R1

Цей експеримент є наочною демонстрацією критичної важливості архітектури ешелонованої оборони. Компрометація пристрою та обхід каналного захисту не призвели до порушення конфіденційності чи цілісності критичної інфраструктури завдяки ізоляції сегментів на мережевому рівні.

3.4.3 Сценарій 3: Атаки типу «Людина посередині»

Атаки класу Man-in-the-Middle становлять критичну небезпеку для локальних мереж. Одним із методів реалізації MitM є розгортання нелегітимного DHCP-сервера. Зловмисник намагається швидше за справжній сервер відповісти на широкомовні запити клієнтів (DHCP OFFER), надаючи їм хибну IP-адресу шлюзу, наприклад, свого комп'ютера. Це дозволяє йому перехоплювати, аналізувати або модифікувати весь вихідний трафік користувачів та IoT-пристроїв.

До вільного порту у сегменті користувачів (VLAN 30) підключається пристрій зловмисника, на якому активується служба DHCP з налаштованим фальшивим списком адрес. Зі сторони легітимного користувача (PC-User2)

ініціюється процес динамічного отримання IP-адреси. За відсутності захисту пристрій користувача міг би отримати мережеві налаштування від сервера хакера.

Завдяки раніше впровадженій технології DHCP Snooping, комутатор Switch0 чітко розмежовує порти на довірені (Trunk-порт до легітимного сервера) та недовірені (всі клієнтські порти доступу). Коли фальшивий сервер намагається відправити пакет DHCP OFFER у мережу, комутатор інспектує цей пакет. Виявивши, що відповідь надходить з недовіреного порту, комутатор автоматично відкидає цей пакет. Користувач PC-User2 безпечно отримує налаштування від справжнього сервера 192.168.10.11, який підключений через довірений магистральний канал.

Ця ж база даних паралельно використовується технологією Dynamic ARP Inspection для блокування підроблених ARP-запитів. Будь-які спроби зломисника надіслати підроблені ARP-відповіді для прив'язки своєї MAC-адреси до IP-адреси легітимного шлюзу відкидаються комутатором, оскільки вони не збігаються із записами у довірєній базі. Момент відкидання нелегітимного DHCP-пакета в режимі симуляції Packet Tracer зафіксовано на рис. 3.11.

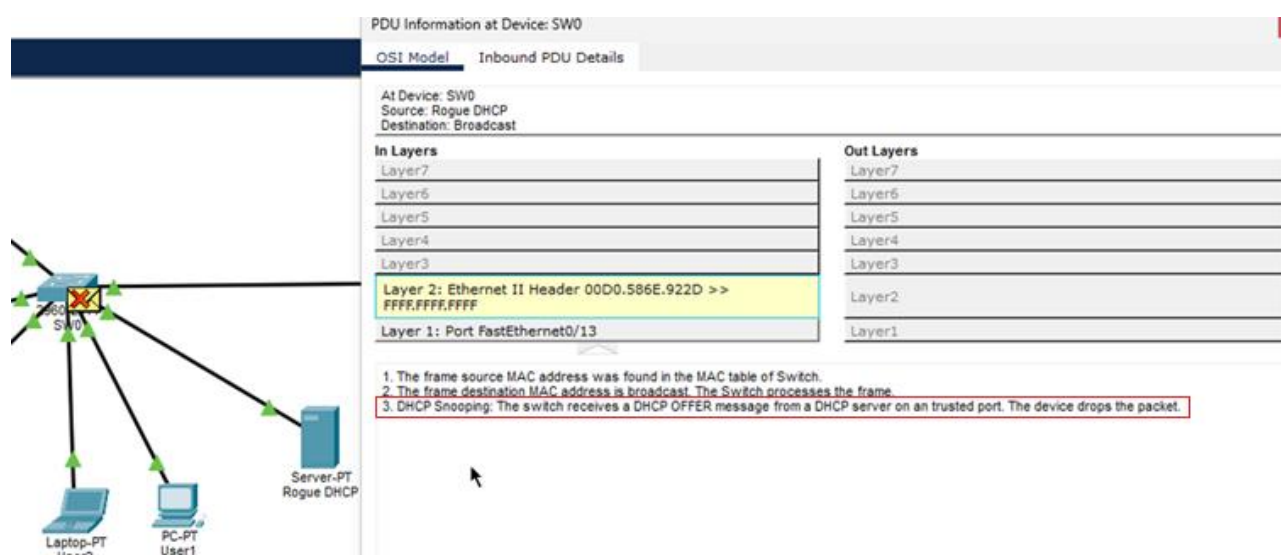


Рисунок 3.11 — Знімок з режиму симуляції у Packet Tracer, що фіксує момент відкидання нелегітимного DHCP-пакета комутатором Switch0

Тестування доводить, що застосування інспекції трафіку на каналному рівні повністю усуває фундаментальні вразливості протоколів IPv4 локальної мережі.

3.4.4 Аналіз результатів моделювання та загальна оцінка надійності

Проведене імітаційне моделювання дозволяє зробити комплексний висновок щодо надійності спроектованої архітектури кібербезпеки. Практичні експерименти довели, що використання традиційних, стандартизованих інструментів управління мережевою інфраструктурою (VLAN, ACL, Port Security, DAI) є високоефективним методом компенсації внутрішніх вразливостей пристроїв Інтернету речей.

Головним досягненням реалізованої системи є побудова ешелонованої оборони. Як продемонстрували сценарії тестування, система не покладається на єдиний бар'єр безпеки. Захист функціонує як послідовний ланцюг реакцій:

1. Якщо зломисник намагається здійснити фізичне втручання — його блокує Port Security.
2. Якщо атака відбувається логічним шляхом зсередини дозволеного порту (спроба підміни адрес або перехоплення сесій) — загрозу нейтралізують DHCP Snooping та DAI.
3. Якщо IoT-пристрій скомпрометований на рівні прикладного програмного забезпечення (наприклад, через вразливість нульового дня) — списки контролю доступу обмежують радіус ураження виключно одним ізольованим сегментом, рятуючи корпоративні дані та сервери від поширення загроз мережею.

Результати підтверджують обґрунтованість впровадження принципів нульової довіри в мережах IoT. Жодному пристрою, навіть якщо він фізично знаходиться в офісі, не надається надмірних привілеїв. Обмежені обчислювальні ресурси мікроконтролерів та сенсорів, які не здатні самотійно протистояти

кібератакам, повністю компенсуються обчислювальними потужностями мережевого обладнання Cisco.

Таким чином, практична реалізація повністю виконує поставлені завдання. Запропонований підхід до конфігурації комутаційного та маршрутизуючого обладнання забезпечує стійкість системи зв'язку до типових класів кібератак, гарантуючи конфіденційність, цілісність та безперервну доступність сервісів розумного середовища. Симуляція в середовищі Packet Tracer підтверджує коректність теоретичних висновків та може слугувати базовим еталоном для проєктування безпечних корпоративних IoT-мереж у реальних умовах експлуатації.

3.5 Висновки до розділу 3

У цьому розділі здійснено практичну реалізацію системи захисту мережевої інфраструктури Інтернету речей у середовищі імітаційного моделювання Cisco Packet Tracer. Спроектовано та розгорнуто комплексну топологію розумного офісу, яка побудована за класичною ієрархічною моделлю та об'єднує маршрутизатор Cisco ISR4331, два комутатори Catalyst 2960, бездротову точку доступу зі стандартом захисту WPA2-PSK, а також набір IoT-компонентів, серед яких мікроконтролер, RFID-зчитувач, датчик диму, розумні двері та розумний кондиціонер. Така архітектура адекватно відображає структуру сучасних корпоративних IoT-середовищ та створює репрезентативну базу для перевірки запропонованих механізмів захисту.

Виконано сегментацію мережі шляхом розгортання чотирьох ізольованих віртуальних локальних мереж — серверної, користувацької, IoT-сегмента та виділеної мережі управління. Налаштовано міжвланову маршрутизацію за топологією «маршрутизатор на паличці» з використанням сабінтерфейсів та інкапсуляції IEEE 802.1Q, а також централізований розподіл IP-адрес через механізм DHCP Relay Agent. Це дозволило реалізувати фундаментальний принцип

архітектури нульової довіри — логічне розділення пристроїв за рівнем критичності та функціональним призначенням.

Реалізовано комплекс механізмів захисту канального рівня моделі OSI. Здійснено адміністративне відключення невикористаних портів комутаторів, налаштовано технологію Port Security з динамічним вивченням MAC-адрес у режимі Sticky та політикою порушення violation shutdown. Окремо обґрунтовано особливості налаштування Port Security на порту бездротової точки доступу, де ліміт дозволених адрес було пропорційно збільшено для запобігання хибним спрацюванням. Розгорнуто механізм DHCP Snooping із чітким поділом портів комутатора на довірені та недовірені, а на основі сформованої бази даних прив'язок реалізовано Dynamic ARP Inspection, що забезпечує верифікацію кожного ARP-пакета та унеможливорює реалізацію атак підміни.

Налаштовано механізми захисту мережевого рівня. Розроблено та застосовано іменований розширений список контролю доступу IOT_RESTRICT, який жорстко регламентує міжсегментну взаємодію та обмежує комунікацію IoT-пристроїв виключно з легітимними сервісами централізованого управління. Для забезпечення конфіденційності каналу адміністративного управління налаштовано протокол Secure Shell версії 2 з криптографічними ключами RSA довжиною 2048 біт, локальною базою даних користувачів та банером попередження про заборону несанкціонованого доступу. Протокол Telnet, як такий, що передає автентифікаційні дані у відкритому вигляді, було повністю заблоковано на віртуальних термінальних лініях усіх мережевих пристроїв.

Здійснено імітаційне тестування ефективності розгорнутої системи захисту за трьома сценаріями кібератак, які охоплюють різні рівні моделі OSI та різні вектори проникнення зловмисника. Перший сценарій моделював фізичне неавторизоване підключення стороннього обладнання до порту комутатора та підтвердив спрацювання механізму Port Security з блокуванням інтерфейсу у стан err-disable. Другий сценарій передбачав підміну MAC-адреси з подальшою спробою поширення загроз мережею до критичного сегмента — обхід захисту канального рівня нейтралізовано на рівні маршрутизації шляхом фільтрації

трафіку списком контролю доступу. Третій сценарій моделював атаку «людина посередині» через розгортання нелегітимного DHCP-сервера, спроби якої були автоматично заблоковані механізмами DHCP Snooping та Dynamic ARP Inspection.

Результати імітаційного моделювання довели практичну цінність архітектури ешелонованої оборони, яка функціонує як послідовний ланцюг незалежних захисних реакцій. Експериментально підтверджено, що використання стандартизованих засобів управління мережевою інфраструктурою — VLAN, розширених списків контролю доступу, Port Security, DHCP Snooping та Dynamic ARP Inspection — є ефективним методом компенсації внутрішніх вразливостей кінцевих пристроїв Інтернету речей. Реалізована система забезпечує конфіденційність, цілісність та безперервну доступність сервісів розумного середовища, що повністю відповідає поставленим у роботі завданням та може слугувати базовим еталоном для проєктування захищених корпоративних IoT-мереж в умовах реальної експлуатації.

ВИСНОВКИ

У дипломній роботі вирішено актуальне науково-практичне завдання підвищення рівня захищеності мережевої інфраструктури Інтернету речей шляхом обґрунтування та впровадження комплексу методів захисту на каналному та мережевому рівнях моделі OSI. Поставлена мета досягнута, а сформульовані у вступі завдання виконані в повному обсязі.

У результаті проведеного дослідження здійснено системний аналіз архітектури мереж Інтернету речей та класифіковано основні вектори кіберзагроз з урахуванням специфіки IoT-обладнання. Встановлено, що відсутність єдиного стандартизованого еталону архітектури, обмеженість обчислювальних ресурсів кінцевих вузлів та їх розміщення у фізично доступному середовищі формують унікальний ландшафт загроз, який не може бути ефективно нейтралізований традиційними засобами захисту периметра. Доведено, що домінуючими векторами атак на сучасні IoT-системи залишаються відмова в обслуговуванні, експлуатація облікових даних за замовчуванням, атаки «людина посередині» та зараження ботнетами.

Обґрунтовано вибір мереже-центричного підходу до захисту IoT як єдиного способу компенсації внутрішніх вразливостей кінцевих пристроїв. Сформовано інтегрований комплекс захисних механізмів, що включає сегментацію мережі через віртуальні локальні мережі, розширені списки контролю доступу, технологію Port Security, а також зв'язки DHCP Snooping та Dynamic ARP Inspection. Як середовище реалізації обрано симулятор Cisco Packet Tracer, що забезпечує повну підтримку стеку засобів захисту Cisco IOS у поєднанні зі спеціалізованою бібліотекою IoT-компонентів.

Спроектовано та реалізовано в середовищі імітаційного моделювання комплексну топологію захищеної мережі розумного офісу з сегментацією на чотири ізольовані віртуальні локальні мережі та централізованим управлінням IoT-інфраструктурою. Налаштовано повний цикл механізмів захисту каналного та мережевого рівнів, включно з протоколом Secure Shell версії 2 для безпечного

адміністрування. Проведено імітаційне тестування ефективності розробленої системи за трьома сценаріями кібератак: фізичне неавторизоване підключення, підміна MAC-адреси з переміщенням та атака «людина посередині» через розгортання нелегітимного DHCP-сервера. У всіх сценаріях підтверджено коректне спрацювання захисних механізмів та локалізацію загроз.

Експериментально доведено практичну цінність архітектури ешелонованої оборони, за якої компрометація одного рівня захисту не призводить до порушення безпеки системи в цілому завдяки незалежному функціонуванню наступних рубежів. Отримані результати підтверджують, що використання стандартизованих засобів управління мережевою інфраструктурою забезпечує ефективну реалізацію принципів архітектури нульової довіри в середовищах Інтернету речей без необхідності модифікації кінцевих пристроїв.

Практична цінність роботи полягає в тому, що розроблена модель захищеної IoT-інфраструктури може бути використана як базовий еталон при проєктуванні корпоративних мереж розумних офісів, промислових об'єктів та об'єктів критичної інфраструктури. Подальші дослідження доцільно спрямувати на інтеграцію систем виявлення вторгнень на базі машинного навчання та впровадження централізованої автентифікації за стандартом IEEE 802.1X із залученням RADIUS-сервера для масштабування запропонованих рішень на рівень великих корпоративних мереж.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures / M. A. Obaidat та ін. *Computers*. 2020. Т. 9, № 2. С. 44. URL: <https://doi.org/10.3390/computers9020044> (дата звернення: 31.05.2026).
2. Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence / T. Mazhar et al. *Brain Sciences*. 2023. Vol. 13, no. 4. P. 683. URL: <https://doi.org/10.3390/brainsci13040683> (дата звернення: 31.05.2026).
3. Awais M., Iqbal J. Layered Architecture of Internet of Things — A Review. *2nd International Conference on Scientific and Academic Research (ICSAR) : proceedings* (Konya, Turkey, March 14—16, 2023). All Sciences Proceedings, 2023. P. 124–131. URL: <https://as-proceeding.com/index.php/icsar/article/download/281/228> (дата звернення: 31.05.2026).
4. OT/IoT Cybersecurity Trends and Insights: 2025 1H Review / Nozomi Networks Labs. Nozomi Networks, July 2025. 35 p. URL: <https://www.nozominetworks.com/ot-iot-cybersecurity-trends-insights-july-2025> (дата звернення: 31.05.2026).
5. The 2024 IoT Security Landscape Report / Bitdefender, NETGEAR. Bitdefender, 2024. 28 p. URL: https://blogapp.bitdefender.com/hotforsecurity/content/files/2024/06/2024-IoT-Security-Landscape-Report_consumer.pdf (дата звернення: 31.05.2026).
6. H.J. F. B., S. S. A Survey on IoT Security: Attacks, Challenges and Countermeasures. *Webology*. 2022. Т. 19, № 1. С. 3741–3763. URL: <https://doi.org/10.14704/web/v19i1/web19246> (дата звернення: 31.05.2026).
7. Daş R., Gündüz M. Z. Analysis of Cyber-Attacks in IoT-based Critical Infrastructures. *International Journal of Information Security Science*. 2019. Т. 8, № 4.

P. 122–133. URL: <https://dergipark.org.tr/en/pub/ijiss/article/1048750> (дата звернення: 31.05.2026).

8. Economic impact of IoT cyber risk - analysing past and present to predict the future developments in IoT risk analysis and IoT cyber insurance / P. Radanliev та ін. *Living in the Internet of Things: Cybersecurity of the IoT* - 2018, м. London, UK. 2018. URL: <https://doi.org/10.1049/cp.2018.0003> (дата звернення: 31.05.2026).

9. Al-Balasmeh H. Zero Trust Architecture for IoT Device Ecosystems. *International Journal of Basic and Applied Sciences*. 2025. Т. 14, № 4. С. 818–825. URL: <https://doi.org/10.14419/r30vpf59> (дата звернення: 31.05.2026).

10. Silva C., Tenório N., Bernardino J. Lightweight Encryption Algorithms for IoT. *Computers*. 2025. Т. 14, № 12. С. 505. URL: <https://doi.org/10.3390/computers14120505> (дата звернення: 31.05.2026).

11. Enaya A., Fernando X., Kashef R. Survey of Blockchain-Based Applications for IoT. *Applied Sciences*. 2025. Т. 15, № 8. С. 4562. URL: <https://doi.org/10.3390/app15084562> (дата звернення: 31.05.2026).

12. Panahi M., Roumanjani F., Ranjbar V. Machine Learning-Based Intrusion Detection Systems for IoT Security: A Survey. 2023. 8 p. URL: <https://doi.org/10.13140/RG.2.2.24990.92489> (дата звернення: 31.05.2026).

13. 2025 Cisco Cybersecurity Readiness Index / Cisco Systems, Inc. May 2025. 22 p. URL: <https://www.cisco.com/go/CybersecurityReadinessIndex> (дата звернення: 31.05.2026).

14. IoT Device Cybersecurity Guidance for the Federal Government / M. Fagan та ін. Gaithersburg, MD : National Institute of Standards and Technology, 2021. URL: <https://doi.org/10.6028/nist.sp.800-213> (дата звернення: 31.05.2026).

15. Anatomy of Threats to the Internet of Things / I. Makhdoom та ін. *IEEE Communications Surveys & Tutorials*. 2019. Т. 21, № 2. С. 1636–1675. URL: <https://doi.org/10.1109/comst.2018.2874978> (дата звернення: 31.05.2026).

16. Fereidouni H., Fadeitseva O., Zalai M. IoT and Man-in-the-Middle Attacks. *SECURITY AND PRIVACY*. 2025. Т. 8, № 2. URL: <https://doi.org/10.1002/spy2.70016> (дата звернення: 31.05.2026).

17. Gwangwava N., Mubvirwi T. B. Design and Simulation of IoT Systems Using the Cisco Packet Tracer. *Advances in Internet of Things*. 2021. Т. 11, № 02. С. 59–76. URL: <https://doi.org/10.4236/ait.2021.112005> (дата звернення: 31.05.2026).
18. Yousif A. M. Y. Internet of Things Simulation Performance using Cisco Packet Tracer Platform. *International Journal of Computer Applications*. 2023. Т. 185, № 30. С. 46–49. URL: <https://doi.org/10.5120/ijca2023923064> (дата звернення: 31.05.2026).
19. Smart and secure home using IOT Simulations with Cisco Packet Tracer / R. R. Chaudhari та ін. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. 2020. С. 88–93. URL: <https://doi.org/10.32628/cseit206311> (дата звернення: 31.05.2026).