Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

Залевської Вікторії Закірівни

на здобуття ступеня вищої освіти Бакалавра

Система захисту інфраструктури пристроїв Інтернету речей підприємства

Галузь знань 12 – Інформаційні технології
Спеціальність 125 – Кібербезпека
Освітня програма Кібербезпека

Шифр КРБКБ. 2102147.21.02.26 ПЗ

Виконала студентка 4 курсу група КБ-21-2 Вікторія ЗАЛЕВСЬКА
Керівник канд. техн. наук, доцент Віктор ЧЕШУН
Нормоконтролер старший викладач Сергій МОСТОВИЙ

До захисту допускаю:
Завідувач кафедри кібербезпеки Юрій КЛЬОЦ

16. 06 2025 р.

Хмельницький 2025

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Інформаційних технологій

Кафедра Кібербезпеки

Рівень вищої освіти Бакалавр

Галузь знань 12 – Інформаційні технології

Спеціальність 125 – Кібербезпека

Освітня програма Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
Юрій КЛЬОЦ
15 лютого 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
Залевській Вікторії Закірівні

1 Тема роботи Система захисту інфраструктури пристроїв Інтернету речей підприємства

Керівник роботи канд. техн. наук, доцент Чешун Віктор Миколайович

Затверджено наказом ректора університету від 07 лютого 2025 № 23

2 Строк подання студентом кваліфікаційної роботи на кафедру

3 Вихідні дані до роботи Створити систему захисту інфраструктури пристроїв Інтернету речей підприємства

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Обґрунтування вибору теми дослідження; характеристика Інтернету речей та його ролі в офісній інфраструктурі; аналіз інформаційних процесів підприємства; ідентифікація актуальних загроз для IoT-систем; дослідження нормативних документів і стандартів безпеки; оцінка потенційних порушників; проєктування мережевої інфраструктури з урахуванням вимог безпеки; моделювання офісної мережі з IoT-пристроями у Cisco Packet Tracer; впровадження заходів мережевого та фізичного

захисту; перевірка ефективності реалізованої системи; рекомендації щодо подальшої підтримки та розвитку захищеної інфраструктури.

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень) Схематичне зображення офісу, Логічна топологія офісу, Модель загроз, Матриця ризиків та модель порушника

6 Консультанти розділів кваліфікаційної роботи

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

7 Дата видачі завдання 16 лютого 2025 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапів (розділів) кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
Вибір і затвердження теми кваліфікаційної роботи	Лютий	
Ознайомлення з предметною областю	Лютий	
Дослідження існуючих рішень	Лютий	
Постановка задачі	Березень	
Визначення загальних принципів рішення задачі	Березень	
Деталізація принципів рішення задачі	Квітень	
Розробка політик експлуатації і безпеки	Квітень	
Оформлення пояснювальної записки згідно вимог	Травень	
Оформлення графічної частини	Травень	
Захист КР	Червень	

Студентка Вікторія ЗАЛЕВСЬКА

Керівник кваліфікаційної роботи Віктор ЧЕШУН

АНОТАЦІЯ

Тема кваліфікаційної роботи: Система захисту інфраструктури пристроїв Інтернету речей підприємства.

Автор роботи: Залевська Вікторія Закірівна.

Керівник роботи: Чешун Віктор Миколайович.

Пояснювальна записка: 81 с., 4 додатки, 7 рисунків, 3 таблиці, 42 джерела.

Графічна частина: 4 плакати, 9 презентаційних слайдів.

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ІНФРАСТРУКТУРА ІНТЕРНЕТУ РЕЧЕЙ, ПЛАН ЗАХИСТУ ІНФОРМАЦІЇ, МОДЕЛЬ ПОРУШНИКА.

Кваліфікаційна робота бакалавра присвячена розробці системи захисту інформації для інфраструктури Інтернету речей підприємства.

В роботі проаналізовано стан захищеності інфраструктури Інтернету речей (IoT) підприємства, визначено потенційні загрози для інформації та компонентів IoT, а також розроблено перелік заходів для забезпечення захисту даної інфраструктури. В результаті дослідження отримано супровідну документацію: план захисту інформації IoT, модель порушника та рекомендації для подальшого захисту інфраструктури. Здійснена підготовка до введення комплексної системи захисту інформаційної інфраструктури Інтернету речей підприємства в дію.

13.06.2025 _____

ABSTRACT

Subject of qualification work: Enterprise IoT device infrastructure protection system.

Author: Zalevska Viktoriia Zakirivna.

Head of work: Cheshun Viktor Mykolayovych.

Explanatory note: 81 p., 4 appendices, 7 figures, 3 tables, 42 sources

Graphic part: 4 posters, 9 presentation slides.

INFORMATION PROTECTION SYSTEM, INTERNET OF THINGS INFRASTRUCTURE, INFORMATION PROTECTION PLAN, VIOLATOR MODEL.

The bachelor's qualification work is devoted to the development of an information protection system for the Internet of Things infrastructure of the enterprise.

The work analyzes the state of security of the Internet of Things (IoT) infrastructure of the enterprise, identifies potential threats to information and IoT components, and also develops a list of measures to ensure the protection of this infrastructure. As a result of the study, accompanying documentation was obtained: an IoT information protection plan, an attacker model, and recommendations for further protection of the infrastructure. Preparations were made for the introduction of a comprehensive system for protecting the information infrastructure of the Internet of Things of the enterprise into operation. m.

13.06.2025 _____

ЗМІСТ

ВСТУП

Більшість із нас веде повсякденне життя, не усвідомлюючи що, нас постійно оточує багато пристроїв, котрі фіксують нашу фізичну присутність, голоси, біометричні показники й поведінкові вподобання. Окрім нашого персонального комп'ютера або смартфона, все частіше у нашому житті з'являються кількість речей у нашому використанні, що підключаються до Інтернету, безпосередньо чи опосередковано. До прикладу, майже у кожній домівці є робот-пилосос, розумні колонки чи холодильники з віддаленим керуванням, кожний другий має на руці фітнес-браслет або розумний годинник. Ці технології є лише частиною ширшого явища, яке активно впроваджується в різних сферах суспільного життя. Усі ці об'єкти об'єднує спільна концепція — Інтернет речей. Цей термін був запропонований Кевіном Ештоном, він хотів описати можливості радіочастотної ідентифікації яка використовувалась в корпоративних системах для відслідковування доставок товарів без втручання людини у процес, у 1999 році під час його роботи над Procter & Gamble [1].

Однак, цей стрибок у впровадженні та збільшені використання пристроїв Інтернету речей викликає значні труднощі у відповідному захисті цілісності даних, конфіденційності користувачів і забезпечення надійності системи. Занепокоєння викликало нове явище, яке розглядається як наступний етап розвитку інтернету речей. Йдеться про концепцію, що охоплює не лише з'єднання технічних пристроїв через мережу, а й включає взаємодію між людьми, цифровими даними та процесами. Такий підхід дозволяє створити єдине інформаційне середовище, здатне забезпечити більш складну та цілісну взаємодію в межах цифрової інфраструктури. Тобто, перший включає зв'язок «машина-машина», тоді як другий включає зв'язок «машина-людина» та взаємодію між людьми за допомогою технологій.

Ось тому, питання безпеки цих пристроїв стає надзвичайно актуальним. Вони проникли в усі аспекти нашого життя — від приладів у нашому повсякденному житті, до складних промислових систем. Кожен новий пристрій,

підключений до Інтернету, може стати потенційною мішенню для зловмисників, які можуть використовувати вразливості систем для атак або маніпуляцій. Наслідками може бути що-завгодно: від крадіжки особистих даних до фізичних небезпек. З розвитком технологій, зростає і потреба в удосконаленні способів забезпечення безпеки. Технічні вразливості мають усуватись на всіх етапах починаючи від проектування та закінчуючи впровадженням та протягом подальшої експлуатації пристроїв. Але нажаль, часто у таких пристроях застосовуються спрощенні або застарілі компоненти. Більшість виробників продуктів випускають обладнання та програмне забезпечення без будь-яких гарантій або тестування [2]. Надійне шифрування даних могло би пом’якшити цю проблему, але поширеним залишається ненадійне та слабке шифрування даних та обмежена потужність обробки пристроїв, яка заважає створити надійну безпеку системи.

Отже, актуальність цієї роботи зумовлена тим, що зростаюча інтеграція пристроїв Інтернету речей у бізнес-процеси підприємств супроводжена підвищенням ризиків інформаційної безпеки. Багато IoT-пристроїв не мають належного захисту або не відповідають сучасним стандартам, що створює загрози для конфіденційності, цілісності та доступності даних. Відсутність комплексного підходу до захисту, ускладнює їх ефективну експлуатацію. Тому розробка цілісної системи захисту IoT-середовища є актуальним і практично важливим завданням у сфері кібербезпеки підприємств.

Практична цінність цієї роботи полягає в можливості застосування результатів аналізу предметної області та інформаційних процесів підприємства для створення ефективної системи захисту IoT-інфраструктури. Побудовані моделі загроз і порушника стали основою для проектування комплексних захисних заходів, адаптованих до особливостей підприємства. Окрім цього, в роботі розроблено рекомендації щодо організаційної структуризації, запропоновано підхід до впровадження і тестування захисної системи, а також створено настанови з її подальшої експлуатації. Все це робить результати роботи придатними до практичного використання на приватному IT-підприємстві.

Мета кваліфікаційної роботи – спроєктувати систему захисту інфраструктури Інтернету речей офісу, на основі функціонуючого приватного IT-підприємства з урахуванням актуальних загроз, наявної архітектури мережі та специфіки IoT-пристроїв, з подальшим впровадженням і наданням рекомендацій щодо експлуатації цієї системи.

Для досягнення даної мети, необхідно почергово виконати такий перелік завдань:

– провести аналіз предметної області за темою кваліфікаційної роботи;

– здійснити огляд інформаційних процесів приватного IT-підприємства та визначити основні IoT-зони і пристрої;

– побудувати модель загроз та модель потенційного порушника з урахуванням особливостей інфраструктури

– спроєктувати систему захисту пристроїв IoT на основі отриманої інформації та виявлених ризиків;

– сформулювати рекомендації щодо організаційної структуризації процесів захисту інформації;

– розробити настанови щодо впровадження, експлуатації та супроводу системи захисту;

– провести тестування спроєктованої системи для перевірки її ефективності та надійності.

Ця робота прагне подолати прогалини у наявній системі, шляхом критичному аналізу існуючих рішень та практичного застосування. На відміну від формальних підходів, обговорювана тут актуальність ґрунтується на практичних викликах і потенційних досягненнях, висвітлюючи невирішені аспекти кібербезпеки IoT на підприємстві. Робота спрямована на дослідження та вирішення ключових питань, закладаючи основу для майбутнього прогресу.

1 ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ ТА ПОСТАНОВКА ЗАДАЧІ ЗАХИСТУ

1.1 Характеристика Інтернету речей та дослідження актуальних методів захисту

1.1.1. Опис предметної області

Інтернет речей — це концепція, що передбачає систему фізичних об’єктів, взаємопов’язаних між собою за допомогою вбудованих датчиків [3]. Окрім датчиків, мережа може мати виконавчі пристрої, вбудовані у фізичні об'єкти, які пов'язані між собою за допомогою дротових чи бездротових мереж. Ці взаємопов'язані пристрої мають можливість зчитування та приведення в дію, функцію програмування та ідентифікації, а також дозволяють виключити необхідність участі людини, за рахунок використання інтелектуальних інтерфейсів.

Типова IoT-система — це багаторівнева архітектура, що складається з різних компонентів (рис. 1.1), які працюють у тісній взаємодії для збору, обробки, передачі й аналізу даних.

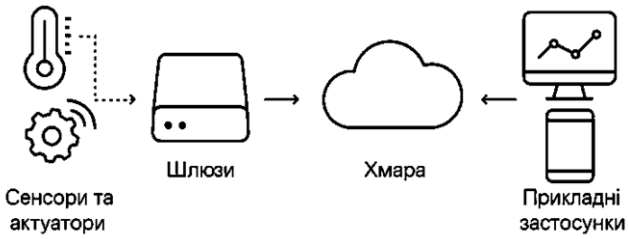


Рисунок 1.1 - Складові IoT

До основних складових можна віднести:

– сенсори (датчики);
– актуатори (виконавчі пристрої);
– гейти (шлюзи);
– мережа передачі даних;
– хмарна інфраструктура або локальні сервери.

Як приклад практичного застосування можна розглянути систему розумного поливу, сенсори вимірюють вологість грунту, гейтер приймає сигнали від сенсорів та передає їх на сервер, хмарна платформа визначає чи потрбіно вмикати полив, актуатор відкриває клапан на системі поливу і після цього інформує власника системи про виконану дію.

Сенсори – це основні пристрої збору даних, які відіграють роль «органів чуття» в IoT-системі. Вони вимірюють фізичні параметри навколишнього середовища або стан об'єктів, до яких прикріплені. Найпоширеніші типи сенсорів включають: температурні, вологості, тиску, освітленості, біометричні, рухові. Їх правильна інтеграція та налаштування безпосередньо впливають на ефективність і безпеку функціонування всієї IoT-системи.

Актуатори (виконавчі пристрої) — це компоненти, які забезпечують фізичну реакцію на дані або команди системи. Якщо сенсори спостерігають за станом середовища, то актуатори на нього впливають. Іншими словами, актуатори є «м'язами» IoT-системи, вони виконують дії у відповідь на зміну параметрів середовища або команди керування. Цю роль можуть виконувати найрізноманітніші пристрої: від мікродвигунів та динаміків до електронних замків з освітлювальними приладами.

Гейти (шлюзи) — це проміжні пристрої, що забезпечують інтеграцію локальної мережі сенсорів і актуаторів із глобальною мережею або хмарною платформою. У певних ситуаціях аналіз отриманих даних може вимагати малої кількості обчислювальних ресурсів, так що вони цілком здатні приймати деякі рішення самостійно. Приймаючи такі рішення, вони відправляють певні команди управління на актуатори, які, своєю чергою, виконують свої функції. Якщо ж обробка інформації вимагає великих витрат, або ця інформація підлягає збору, гейти відправляють її на сервери, де з нею проводиться подальша робота. Гейти також відіграють критичну роль у забезпеченні безпеки IoT-системи, виконуючи автентифікацію, контроль доступу та моніторинг мережевої активності.

Отже до основних функцій можна віднести:

– збір даних від сенсорів через локальні протоколи (Zigbee, BLE, Modbus, I2C тощо);

– протокольна конверсія в універсальні формати (MQTT, CoAP, HTTP, TCP/IP);

– локальна обробка даних (Edge processing), фільтрація, агрегація, шифрування;

– керування актуаторами згідно з логікою або правилами автоматизації;

– підключення до хмари або локального серверу через Wi-Fi, Ethernet, LTE, LoRa.

Наприклад, щоб побудувати локальну моніторингову систему для обліку людей, достатньо встановити сенсор руху і невеликий пристрій на зразок Raspberry Pi (рис. 1.2).

Рисунок 1.2 - Одноплатовий комп’ютер Raspberry Pi

Така конфігурація дозволяє виявляти кожен вхід у приміщення, рахувати кількість проходів, а також, за потреби, реагувати на певні події. Додавши простий актуатор, наприклад динамік, можна реалізувати звукову реакцію для кожного десятого входу. Така система вже набуває елементів автоматизації й зворотного зв’язку. Проте коли зростає кількість пристроїв або зростають вимоги до обробки даних (наприклад, потрібно зберігати інформацію про кількість людей за годинами, будувати графіки, прогнозувати навантаження), постає потреба у зовнішньому обчислювальному середовищі.

Центральна частина IoT-системи — це програмна платформа, яка приймає, зберігає, обробляє та аналізує дані, а також забезпечує керування пристроями. У більшості випадків використовується хмарна інфраструктура:

– обробка даних в реальному часі (наприклад, виявлення нестандартних подій);

– зберігання даних у базах (SQL, NoSQL);

– використання алгоритмів аналітики, AI/ML для прогнозування;

– взаємодія з користувачем через веб або мобільні інтерфейси;

– інтеграція з іншими сервісами (наприклад, через REST API або Webhooks).

До переваг такого рішення, можна віднести легка маштабованість, тобто можна легко підключати нові пристрої без реконфігурації системи, швидке оновлення сервісів та політик завдяки централізованого керування, доступність і відмовостійкість. Незважаючи на переваги, хмарна інфраструктура також породжує низку проблем, пов'язаних із безпекою даних (наприклад, їх передача у відкритих мережах), конфіденційністю, залежністю від постачальника послуг, а також з затримками при обробці критично важливої інформації. Ці проблеми частково вирішуються через здійснення обробки на рівні гейтів або навіть пристроїв.

Ефективна передача даних між пристроями є основою функціонування будь-якої IoT-системи. Через специфіку таких систем, велику кількість пристроїв, обмежені ресурси, різну енергоспоживаність та нестабільні мережеві умови, стандартні протоколи Інтернету не завжди підходять. У відповідь на ці виклики було розроблено низку спеціалізованих протоколів, які оптимізовані для роботи в умовах IoT [4]. Цей огляд, дозволить точніше визначити вимоги до майбутньої системи захисту та обґрунтувати вибір відповідних засобів безпеки.

MQTT — це легкий мережевий протокол, створений для обміну повідомленнями між пристроями з низькою пропускною здатністю та обмеженими ресурсами попри нестабільне з’єднання [5]. Він базується на моделі «публікатор-підписник», що дозволяє скоротити обсяг даних для передачі. Тобто,

пристрої-публікатори регулярно надсилають повідомлення, а пристрої-підписники, автоматично отримують їх. MQTT створений спеціально для IoT, тому його широко використовують в розумних будинках, промислових системах та логістиці. До вагомих переваг можна віднести:

– низьке енергоспоживання завдяки невеликому розмірі пакетів;

– ефективна робота при нестабільному з’єднанні завдяки асихроності;

– простота реалізації та маштабуванні.

CoAP — це протокол, створений спеціально для обмежених пристроїв, які працюють у мережах з обмеженою пропускною здатністю. Він побудований на основі UDP і використовує модель клієнт-сервер. Він забезпечує ефективну двосторонню комунікацію між пристроями та хмарними сервісами. До його переваг відносяться:

– легкість, завдяки невеликим пакетам та простий формат повідомлень;

– підтримка мультикастингу, тобто може працювати з мільярдом вузлів одночасно [6];

– простота у розгортанні в обмежених мережах;

– підтримка блокової передачі великих даних за допомогою маленьких пакетів.

HTTP/HTTPS — хоча він не є оптимальним для IoT, але його популярність зумовлює сумісність і наявність широкої інфраструктури. Завдяки цим параметрам, він ідеально підходить пристроям, які мають доступ до постійного живлення і стабільного інтернет-з’єднання. Але такий варіант дуже вузько спеціалізований через надлишковість для простих IoT-задач [7]. Зазвичай це протокол використовують в системах відеоспостереження, розумних термостатах або шлюзах, що передають дані на вебсервери чи в хмару. Його застосування виправдане тоді, коли важлива інтеграція з веб-інтерфейсами або необхідна підтримка сучасних стандартів безпеки, таких як TLS. Проте у випадках, де потрібна мінімальна затримка, економія енергії або ефективність при передачі невеликих обсягів даних, перевагу надають легшим протоколам, таким як MQTT або CoAP.

AMQP — це надійний протокол передачі повідомлень, який підтримує черги, маршрутизацію повідомлень і безпечну доставку [8]. Використовується переважно в критично важливих сферах, таких як банки чи держустанови. Містить аналогічні переваги як і попередні протоколи, але до цього всього спроможний підтримувати більш складніші сценарії роботи. Тому він складніший у реалізації та потребує більше ресурсів.

LoRaWAN — це протокол мережі з великою дальністю дії, який дозволяє пристроям з низьким енергоспоживанням передавати невеликі обсяги даних на великі відстані. Його популярність в промисловості, «розумних містах», сільському господарстві зумовлена доступності протоколу бездротового двостороннього зв'язку, який покриває великий радіус при низькому енергоспоживанні (деякі пристрої працюють від батареї до 10 років) [9]. Такий протокол має низку переваг, до таких можна також віднести:

- підтримка шифрування, включає 128-бітне AES шифрування;
- легка маштабованість;
- невисока вартість розгортання;
- ідеально підходить для батарейних пристроїв;
- велика дальність дії, до 20 км за містом та 2-5 км у міських умовах.

Як і в будь-якій іншій системі, у LoRaWAN є значні недоліки, такі як невисока пропускна спроможність та велика затримка передачі даних від кінцевих пристроїв, що не підходить до критичних у часі додатків, односторонній або обмежений двосторонній зв'язок.

NB-IoT — це стандарт, орієнтований на масштабовані мережі пристроїв, які передають малі обсяги даних з низькою частотою (наприклад, раз на кілька хвилин або годин), потребують надійного зв'язку, низького енергоспоживання та великого радіуса дії. Він є частиною стандарту LTE (4G) [10], розробленого міжнародною організацією 3GPP, і також підтримується в рамках мереж 5G. Такий вибір ідеально підходить для таких сценаріїв, як розумні лічильники, моніторинг екології та погоди, смарт паркінги та розумне освітлення. Він забезпечує глибоке покриття, високу надійність та тривалий час роботи батареї.

До недоліків можна віднести обмежену швидкість, потребу у SIM-карті або eSIM, дуже залежний від покриття та умов роботи оператора зв'язку та не підходить для складних задач.

У підсумку, аналіз поширених мережевих протоколів дозволив виявити їхні ключові характеристики, переваги та недоліки в контексті застосування в IoT-інфраструктурі. Ця інформація є важливою для правильного проєктування системи захисту, оскільки саме вибір і налаштування протоколів суттєво впливають на безпеку, надійність і продуктивність IoT-рішень. Надалі ці висновки будуть враховані при моделюванні безпечної мережевої взаємодії між пристроями та при впровадженні відповідних механізмів захисту.

1.1.2 Актуальна безпекова проблематика застосування пристроїв Інтернету речей

Перш ніж перейти до розгляду конкретних загроз, важливо зрозуміти, чим Інтернет речей відрізняється від класичних IT-систем у питаннях безпеки. IoT не просто ще один тип підключених пристроїв, а розподілене й дуже різнорідне середовище, де в одній мережі можуть взаємодіяти сенсори з мінімальними ресурсами, повноцінні камери відеоспостереження, мікроконтролери, смартфони та хмарні сервіси. Ці пристрої можуть суттєво відрізнятися між собою за рівнем продуктивності, підтримкою оновлень, протоколами зв’язку та операційними системами.

Через таку неоднорідність створюється велика кількість точок, через які зловмисник може проникнути в систему, тобто значно збільшується площина потенційної атаки [11]. При цьому виробники IoT-пристроїв нерідко зосереджуються на швидкому виведенні продукту на ринок, зручності користування чи енергоефективності, залишаючи питання безпеки «на потім». У результаті, без належного підходу до побудови захисту, такі пристрої можуть стати вразливим місцем у загальній інформаційній системі підприємства

Однією з ключових проблем є обмежена взаємодія між пристроями різних виробників через відсутність єдиних стандартів. У сучасних офісних інфраструктурах часто використовується обладнання від різних виробників, кожен з яких реалізує власні протоколи зв'язку, системи автентифікації, моделі керування даними та сервіси зберігання. Це ускладнює інтеграцію пристроїв у єдину безпечну систему, а також створює труднощі для централізованого моніторингу та адміністрування. Крім того, замкнуті екосистеми, характерні для багатьох комерційних рішень, можуть обмежувати доступ до конфігураційних параметрів або журналів подій, що необхідні для аудиту безпеки. Відсутність єдиного підходу до оновлень прошивки та управління ускладнює оперативне реагування на виявлені вразливості. У результаті навіть правильно налаштована мережа може залишатися під загрозою через несумісність або слабку взаємодію між її компонентами.

Ще одним викликом для безпеки є вразливість мережевих інтерфейсів. Багато пристроїв за замовчуванням мають відкриті порти або активовані сервіси, що працюють через застарілі та незахищені протоколи, зокрема Telnet, FTP чи HTTP [12]. Такі протоколи не шифрують передані дані, а отже, будь-яка третя сторона, яка має доступ до мережевого трафіку, може перехопити облікові дані, особисту інформацію або навіть керувати пристроєм дистанційно. Нерідко ці сервіси залишаються увімкненими після налаштування пристрою, що створює постійну «точку входу» для потенційного зловмисника. Крім питань конфіденційності та автентичності даних, варто також враховувати навантаження на мережу. У випадку з офісною інфраструктурою, яка активно використовує велику кількість сенсорних IoT-пристроїв, обсяг переданих даних може зростати експоненційно. Якщо канали зв'язку не оптимізовані, це призводить до затримок, втрати пакетів або збоїв у системах моніторингу та автоматизації.

Наступна серйозна проблема — недостатня ізоляція між компонентами IoT-системи. Коли всі пристрої, незалежно від їх функцій чи рівня критичності, під'єднані до однієї локальної мережі, навіть один скомпрометований вузол може становити загрозу для всієї інфраструктури. У контексті офісного середовища, де

одночасно працюють камери відеоспостереження, системи контролю доступу, кліматичне обладнання та персональні пристрої співробітників, ризики стрімко зростають. На відміну від комп’ютерів або смартфонів, які мають більш потужне ПЗ та можливості для оновлення й моніторингу, побутові чи офісні IoT-прилади зазвичай обмежені у своїх захисних механізмах. Вони рідко отримують своєчасні оновлення безпеки, а їхня ОС часто закрита або надто спрощена для ефективної реакції на загрози. У результаті, навіть банальний фітнес-трекер або «розумна» розетка можуть стати «троянським конем», через який уся мережа буде скомпрометована.

Конфіденційність у контексті IoT перетворюється на критично важливий аспект, що потребує окремої уваги. Багато IoT-пристроїв використовують технології автоматичної ідентифікації, зокрема RFID, NFC, QR- або 2D-штрих-коди, що дає змогу точно відстежувати переміщення об'єктів, їх стан і взаємодії з іншими системами [13]. Проте така прозорість в інформаційних потоках створює додаткові ризики. Ідентифікаційні мітки, якими оснащуються як речі, так і люди (наприклад, пропуски з RFID-чіпами або фітнес-трекери співробітників), часто містять унікальні коди або інформацію про поведінкові характеристики, що в сукупності може бути використано для побудови цифрового профілю. Якщо такі дані потрапляють до третіх осіб без згоди користувача, це може призвести до серйозного порушення права на приватність, а в деяких випадках і до юридичної відповідальності за порушення норм національного законодавства [13]. У зв'язку з цим особливу увагу необхідно приділяти політикам доступу, методам шифрування при зберіганні та передачі даних, а також мінімізації обсягу ідентифікаційної інформації, що циркулює мережею. Без належного контролю за цими аспектами навіть найпростіший IoT-пристрій може стати джерелом витоку критичної інформації, яка, на перший погляд, не виглядає чутливою, але в контексті повної картини може виявитися дуже цінною для зловмисника. Щоб схема автентифікації користувача для бездротових сенсорних мереж була задовільною, вона повинна відповідати певним характеристикам [15]:

– взаємна автентифікація між користувачем і шлюзовим вузлом;

– взаємна автентифікація між шлюзовим вузлом і сенсорним вузлом;

– взаємна автентифікація між користувачем і сенсорним вузлом;

– безпечна та зручна для користувача можливість зміни пароля;

– анонімність користувача;

– встановлення ключа сеансу;

– безпечна та зручна для користувача смарт-картка;

– секретний ключ/параметр шлюзового вузла є безпечним;

– зручна для користувача фаза реєстрації.

Із масштабним зростанням кількості підключених пристроїв, розширенням мережевої інфраструктури та ускладненням цифрових сервісів питання енергоспоживання виходить на новий рівень актуальності. Розвиток IoT супроводжується збільшенням обсягів переданих даних, підвищенням вимог до пропускної здатності мереж і, відповідно, значним зростанням енергетичних витрат. У довгостроковій перспективі це може мати не лише фінансові, а й екологічні наслідки. Тому одним із важливих напрямів є впровадження «зелених» технологій, що дозволяють мінімізувати споживання енергії пристроями без шкоди для їхньої функціональності. До заходів, які сприяють енергоефективності, можна віднести:

– перехід на протокол IPv6, що забезпечує оптимальніший маршрут передачі даних;

– впровадження малопотужних рішень для живлення сенсорів;

– використання енергоефективних мікроконтролерів та технологій бездротової передачі.

Однак варто зауважити, що енергоощадність нерозривно пов’язана і з безпекою. Багато пристроїв, орієнтованих на низьке енергоспоживання, часто мають обмежені ресурси для реалізації сучасних механізмів захисту [16]. Наприклад, залишення стандартних облікових записів виробника, слабка або відсутня автентифікація, а також відсутність оновлень прошивки створюють додаткові ризики. Таким чином, прагнення до енергоефективності повинне

супроводжуватись комплексним підходом до кіберзахисту, що враховує як обмеження IoT-пристроїв, так і можливі сценарії атак на рівні інфраструктури.

Розглянуті вище проблеми демонструють складність і багатогранність безпекових викликів, з якими стикаються системи Інтернету речей. Різноманітність пристроїв, відсутність уніфікованих стандартів, вразливості мережевих інтерфейсів та недоліки в організації безпеки створюють сприятливі умови для зловмисників. Щоб краще усвідомити реальний масштаб важливоті правильно розробленої системи захисту Інетерету речей приватного IT-підприємства, доцільно розглянути конкретні випадки відомих кібератак на пристрої Інтернету речей.

Mirai — вірус, який після зараження IoT-пристроїв, об’єднував у ботнет за допомогою якого, проводились для DDoS-атаки у жовтні 2016 року. Розповсюджувався він шляхом масового сканування мережі Інтернет з метою виявлення IoT-пристроїв із відкритими Telnet або SSH-портами [17]. Завдяки використанню стандартних або слабких паролів, які часто не змінювалися користувачами на пристроях, ботнет охопив сотні тисяч пристроїв маючи лише базу лише з 60 найпоширеніших пар логін-пароль. Зрештою, це призвело до DDoS-атаки на компанію Dyn, що є постачальником системи доменних імен та поштовим послугам, її клієнтами є американські гіганти, такі як Amazon, Netflix, Twitter, The Wall Street Journal, Starbucks і т. д. Атака на клієнтів, доходи і репутацію тривала більше восьми годин.

VPNFilter — вірус, що заражав маршрутизатори та мережеві пристрої, зокрема від виробників Linksys, Mikrotik, TP-Link у 2018 році, завдяки цьому отримав доступ до всіх підключених до маршрутизатора пристроїв Інтернету речей. Вірус має багатофазний розвиток на зараженому пристрої, ці фази включають: перехоплення трафіку, збирання даних, знищувати прошивки після спроби перезавантаження пристрою, отримувати контроль над функціоналом пристрою, здійснювати MITM-атаки. Кіберрозвідка Cisco Talos, опублікувала статтю, де стверджується що було уражено 54 країн, але основна мета хакерів було ураження України [18].

IoTReaper — вірус, який поширюється завдяки вже відомим вразливостей пристроїв та їхньої прошивки [19]. Його поширення стало можливим через те, що після атаки Mirai багато виробників випустили оновлення прошивок, які усували наявні вразливості, однак значна частина користувачів не встановила ці оновлення. Це і стало сприятливим середовищем для масового зараження пристроїв у 2017 році. Також, цей ботнет частково запозичує вихідний код Miray, але суттєво відрізняється кількома ключовими особливостями:

– перевершив свого попередника в декілька разів у швидкості поширення по мережі;

– не здійснює підбір паролів, натомість використовує експлойти, які спрямовані на виявлення вразливостей у веб-інтерфейсах, CGI-скриптах і службах, характерних для роутерів, відеореєстраторів, IP-камер та інших IoT-пристроїв.

Incontroller — це програмний фраємворк, орієнтований на атаки на промисловий Інтернет речей та системи його управління. Завдяки своїй універсальності він отримав неофіційну назву «швейцарський армійський ніж» серед засобів злому [20], оскільки дозволяє атакуючим здійснювати широкий спектр дій починаючи від розвідки закінчуючи безпосереднього саботажу обладнання [21]. До особливостей його поширення в першу чергу відносять відсутність належного розмежування IoT-мережі від загальної корпоративною мережею, а також використання незахищених або застарілих протоколів зв’язку, таких як Modbus, OPC UA, IEC 104 тощо. Саме ці чинники відрізняють Incontroller від його попередників і роблять його особливо небезпечним у контексті сучасних IoT-систем. Хоча активне використання Incontroller було виявлено у 2022 році, ще до реалізації масштабної атаки, його потенційна загроза оцінювалася як критична. У разі успішної реалізації атака могла б призвести до:

– виходу з ладу промислового обладнання;

– тривалого простою підприємства, яке завдало б великих фінансових втрат;

– фізичних аварій або пошкодження об'єктів критичної інфраструктури (електростанцій, насосних станцій, нафтопереробних заводів тощо);

– загроз для життя та безпеки людей, які працюють з відповідним обладнанням.

Аналіз поширення шкідливих програм Incontroller**,** IoTReaper та VPNFilter показав, що атаки ставали можливими через низку типових вразливостей: використання застарілих і незахищених протоколів, відсутність оновлень прошивки, відсутнє розмежування мережі IoT-інфраструктури, а також ненадійна автентифікація. Під час проєктування системи захисту нашої IoT-інфраструктури на приватному IT-підприємстві ці помилки будуть враховані.

1.1.3 Актуальне державне та інозенмне нормативно-правове забезпечення, стандарти та регулючі документи у сфері пристроїв Інтернету речей

Щоб захистити Інтернет речей у корпоративному середовищі, недостатньо лише правильного налаштування пристроїв, важливо спиратися на вже напрацьовані підходи та рекомендації, закріплені в міжнародних стандартах і законодавчих документах. Вони дають розуміння, як будувати безпечну інфраструктуру, які ризики враховувати і які мінімальні вимоги дотримуватися.

ISO/IEC — це міжнародні організації, які займаються стандартизацією у сфері технологій та безпеки. ISO (Міжнародна організація зі стандартизації) та IEC (Міжнародна електротехнічна комісія) спільно розробляють технічні стандарти, які допомагають стандартизувати підходи до безпеки в різних IT-галузях, зокрема в Інтернеті речей. До основних стандартів можна віднести:

– ISO/IEC 30141:2019 — це стандарт, який визначає загальну архітектуру Інтернету речей. Він описує базові компоненти IoT-системи, принципи їх взаємодії, а також механізми управління і безпеки. Головна мета цього стандарту створити стандартизований каркас, який допомагає розробникам

краще розуміти, як мають бути побудовані та інтегровані IoT-пристрої та сервіси, забезпечуючи при цьому безпеку на кожному рівні системи [22].

– ISO/IEC 27030:2024 — доповнює архітектурні положення, фокусуючись безпосередньо на безпеці комунікацій у IoT. Він встановлює вимоги щодо захисту інформації, що передається між пристроями, а також стандарти для автентифікації, авторизації та цілісності даних. Це допомагає знизити ризики перехоплення або модифікації інформації під час передачі [23].

Інститут інженерів електротехніки та електроніки (Institute of Electrical and Electronics Engineers, IEEE) один з найбільших професійних організацій у сфері технологій, яка створює стандарти для телекомунікацій, комп'ютерних мереж та бездротових систем. Її рекомендації активно використовуються в розробці безпечних Wi-Fi мереж, що є критично важливим для IoT. До основних стандартів для IoT відносяться:

– IEEE 802.1X — стандарт, що регламентує механізми контролю доступу до мережі на основі автентифікації користувачів і пристроїв. Цей протокол використовується для захисту як дротових, так і бездротових мереж, забезпечуючи, що до мережі можуть підключатися лише авторизовані пристрої [24].

– IEEE 802.11i — це стандарт, спрямований на підвищення безпеки бездротових мереж Wi-Fi. Він визначає використання сучасних алгоритмів шифрування (WPA2, WPA3), захищає канали передачі від прослуховування і забезпечує надійну аутентифікацію користувачів [25].

NIST (Національний інститут стандартів і технологій США) — це урядова установа, яка займається розробкою рекомендацій і стандартів у сфері кібербезпеки. Документи NIST часто слугують практичними посібниками для організацій усього світу при побудові захищених систем, у тому числі й IoT-рішень. Вони розробили серію спеціалізованих публікацій, які детально описують питання безпеки в даній сфері:

– NIST Special Publication 800-183 «Networks of 'Things'» — цей документ надає огляд архітектури IoT, описує її основні компоненти, взаємодію

між ними та виклики безпеки, які виникають при розгортанні таких систем. Це своєрідний вступний посібник, який допомагає зрозуміти, як організувати безпечну мережу речей [26].

– NIST SP 800-53 «Security and Privacy Controls for Information Systems and Organizations» — один із ключових документів, у якому визначено набір заходів безпеки для захисту інформаційних систем, у тому числі й IoT. Стандарт включає рекомендації щодо контролю доступу, моніторингу, захисту конфіденційності та відновлення після інцидентів [27].

– NIST SP 800-82 «Guide to Operational Technology (OT) Security» — концентрується на безпеці систем керування технологічними процесами, які часто інтегрують IoT-пристрої, особливо у промислових середовищах. Цей документ описує, як захищати такі критичні інфраструктури від зовнішніх та внутрішніх загроз [28].

– NISTIR 8228 «Considerations for Managing Internet of Things Cybersecurity and Privacy Risks» — цей звіт аналізує основні кіберризики та проблеми конфіденційності, характерні для IoT, і надає практичні рекомендації щодо їхнього управління. Він допомагає організаціям сформувати стратегії захисту, враховуючи унікальні особливості IoT [29].

Правове регулювання питань кібербезпеки та захисту інформації в Україні здійснюється через низку ключових законів, які встановлюють загальні принципи, вимоги та відповідальність у сфері безпеки інформаційних систем. Серед основних законів слід виділити:

– ЗУ «Про захист інформації в інформаційно-телекомунікаційних системах» — конкретизує заходи безпеки, які потрібно впроваджувати для захисту інформації у телекомунікаційних мережах, що включає і IoT-інфраструктуру [30].

– ЗУ «Про кібербезпеку» — регламентує питання захисту інформаційних систем, передбачає обов’язкове впровадження заходів з виявлення, запобігання та реагування на кіберінциденти, а також зобов’язує підприємства дотримуватись визначених стандартів безпеки [31].

Крім законів, важливу роль у формуванні ефективної системи захисту відіграють нормативні документи з технічного захисту інформації. Їх розробляє та затверджує Адміністрація Держспецзв'язку з метою встановлення технічних і організаційних вимог до побудови та функціонування захищених інформаційних систем. У цій дипломній роботі, ці НД ТЗІ будуть використині як методологічна база для розробки моделі загроз, моделі порушника, системи захисту та нормативно-розпорядчої документації:

– НД ТЗІ 1.1-002-99 — визначає основні принципи та вимоги до технічного захисту інформації в комп'ютерних системах від несанкціонованого доступу.

– НД ТЗІ 1.1-003-99 — встановлює єдину термінологію в галузі технічного захисту інформації, що дозволяє чітко формулювати вимоги до систем безпеки та уникати двозначностей у документації.

– НД ТЗІ 1.4-001-2005 — регламентує методику виявлення та класифікації загроз інформаційній безпеці, а також оцінювання їх впливу на інформаційні системи.

– НД ТЗІ 1.4-002-2008 — встановлює порядок формування моделі порушника, з урахуванням його можливостей, цілей та засобів реалізації атак.

– НД ТЗІ 1.5-004-06 — визначає вимоги до створення комплексної системи захисту інформації, що включає технічні, програмні та організаційні заходи безпеки.

– НД ТЗІ 2.5-010-03 — визначає загальні вимоги до організації захисту інформації в інформаційно-телекомунікаційних системах, включаючи порядок розробки систем безпеки та мінімальні заходи захисту.

– НД ТЗІ 3.7-003-05 — визначає вимоги до створення внутрішньої організаційної документації з технічного захисту інформації, зокрема інструкцій, політик та регламентів.

1.2 Огляд інформаційної структури підприємства

Інформаційна інфраструктура будь-якого сучасного підприємства виконує важливу роль у забезпеченні його стабільної роботи. Саме завдяки їй реалізуються основні цифрові процеси, включаючи обмін інформацією між працівниками, зберігання важливих даних, доступ до сервісів, а також підтримка зв’язку з клієнтами та партнерами. Аналіз загальної моделі інформаційної інфраструктури приватного ІТ-підприємства показав активне впровадження пристроїв Інтернету речей. Їх застосування дозволяє автоматизувати обслуговування, моніторинг і частину внутрішніх процесів, що в результаті сприяє підвищенню ефективності роботи підприємства та спрощує взаємодію між технічними компонентами системи.

Інформаційна система підприємства поєднує класичну мережеву інфраструктуру, до якої входять сервери, робочі станції, маршрутизатори, мережеві комутатори, з IoT-компонентами, що реалізують інтелектуальне керування середовищем офісу. Локальна обчислювальна інфраструктура забезпечує базову підтримку корпоративних сервісів, зокрема системи управління проєктами, внутрішній документообіг, поштові сервіси, засоби віртуалізації.

Усі компоненти об'єднані у одну корпоративну локальну мережу з виходом до Інтернету через шлюз, що виконує також функції фаєрвола. Щоб цифрове середовище працювало стабільно та безпечно, інфраструктуру потрібно поділити його на кілька частин. Наприклад, виділяють внутрішню мережу для серверів і пристроїв працівників, зовнішню частину для доступу до Інтернету, гостьову зону, а також окремі сегменти для критичних сервісів. Такий поділ допомагає зменшити ризики та краще контролювати обмін даними всередині компанії.

Багато IoT-пристроїв підключені до внутрішньої мережі через бездротові технології, зокрема Wi-Fi або спеціалізовані протоколи, як-от Zigbee. Таке підключення дозволяє зручно розміщувати обладнання в будь-яких частинах офісу без потреби у прокладенні додаткових кабелів. Зазвичай керування цими пристроями здійснюється через центральний шлюз, який виступає посередником

між локальною мережею та пристроями, а також забезпечує передачу команд і збір даних. Доступ до функцій управління зазвичай реалізується через мобільний застосунок або веб-інтерфейс, що дозволяє швидко змінювати налаштування, переглядати інформацію в реальному часі або отримувати сповіщення. У деяких випадках шлюз також може бути інтегрований з хмарними сервісами, що дає змогу віддаленого моніторингу та керування системою з будь-якої точки, де є Інтернет. Такий підхід зручний, але водночас вимагає додаткового захисту, оскільки бездротові протоколи мають власні специфічні вразливості, а віддалений доступ може стати потенційною точкою входу для зловмисників.

З урахуванням цього, доцільно розглянути, які саме види пристроїв Інтернету речей використовуються та які функції вони виконують у межах загальної інфраструктури.

Перелік основних пристроїв Інтернету речей та їх функції:

– розумне освітлення (сенсори присутності) – використовуються для автоматичного регулювання освітлення залежно від присутності людей або часу доби, що сприяє енергозбереженню;

– розумні термостати та кондиціонер з Wi-Fi-модулем – дозволяють підтримувати оптимальний температурний режим у приміщеннях залежно від часу доби та завантаженості офісу, віддалене керування температурою;

– смарт-розетки – надають можливість дистанційного керування, вмикання/вимикання кожного офісного пристрою окремо;

– електронні замки з біометричною автентифікацією – забезпечують контроль доступу до окремих зон офісу (наприклад, серверної кімнати чи для переговорів);

– IP-камери з функцією детекції руху – моніторинг об’єктів, виявлення підозрілої активності з надсиланням оповіщення у веб-застосунок, зберігання відеодоказів у хмарі;

– мережеві принтери/сканери з IoT функціоналом – друк і сканування документів з можливістю зберігати їх копії в хмарі чи надсилати на пошту;

– персональні фітнес-трекери працівників – моніторинг фіз активності, пульсу, геолокації;

– інтерактивні інформаційні панелі (дисплеї на базі Raspberry Pi) – виведення важливої інформації: графіків, анонсів, планів зустрічей, стану систем.

Застосування таких IoT-пристроїв дозволяє сформувати дійсно «розумне» офісне середовище. Автоматичне освітлення, контроль температури, системи безпеки, інтерактивні дисплеї та навіть персональні фітнес-трекери, усе це допомагає підвищити зручність, продуктивність і загальний рівень організації роботи. Разом із впровадженням зручних та автоматизованих рішень з'являються нові загрози, зокрема збільшення кількості вразливостей, що можуть бути використані для несанкціонованого доступу. До основних загроз, характерних для описаної інфраструктури, можна віднести:

– можливість несанкціонованого доступу до системи контролю доступу (злам розумного замка або підміна автентифікаційного ключа);

– перехоплення трафіку між сенсорами, шлюзом і хмарною інфраструктурою, особливо при відсутності шифрування;

– відсутність регулярного оновлення прошивок IoT-пристроїв, що може сприяти експлуатації відомих вразливостей;

– використання спільної мережі для офісних пристроїв і IoT-систем, що у разі компрометації одного з компонентів може створити ризик поширення атаки на критичні сервіси;

– створення дискомфортного мікроклімату для співробітників або екстремального, який взмозі виведення з ладу обладнання;

– витік персональних біометричних даних, що підпадають під дію законодавства;

– шпигування за персоналом як на роботі так і поза її межами.

Усе це показує, що безпеку в офісах із великою кількістю IoT-пристроїв не можна залишати на другому плані. Вразливості, пов'язані із застарілим ПЗ або недоліками в налаштуваннях мережі, можуть легко призвести до витоку даних або навіть до зупинки роботи окремих систем. Тому, разом із впровадженням нових

технологій, варто одразу продумувати й комплексні заходи захисту інакше користь від автоматизації може обернутись серйозними проблемами.

1.3 Постановка задачі

У підсумку, в межах цього розділу було сформовано цілісне уявлення про Інтернет речей як технологічну основу сучасної цифрової інфраструктури підприємства. Було розглянуто типові складові IoT-систем, а саме: сенсори, актуатори, шлюзи та мережеві протоколи, що забезпечують їхню взаємодію. Окрему увагу приділено актуальним викликам у сфері безпеки Інтернету речей: проаналізовано типові вразливості, відомі випадки атак, а також стандарти та нормативні акти, що регулюють безпечне впровадження таких систем. Завершуючи, ми розглянули загальний вигляд інформаційної інфраструктури конкретного приватного ІТ-підприємства, в якій IoT-технології вже інтегровані в операційні процеси.

Таким чином, на основі результатів проведеного дослідження предметної області, інформаційних джерел за темою роботи, короткого ознайомлення із об’єктом захисту, його станом та загальною безпековою проблематикою, для досягнення мети кваліфікаційної роботи, необхідно виконати такі задачі:

– дослідження інформаційних об’єктів системи, які беруть участь в обміні або зберіганні даних у межах офісної IoT-інфраструктури;

– побудова моделі загроз, що дозволить систематизувати потенційні ризики та визначити їхні джерела;

– моделювання порушника з урахуванням його можливостей, рівня доступу та цілей;

– проєктування системи захисту, що охоплюватиме як технічні, так і організаційні заходи;

– розроблення настанов щодо впровадження запропонованої системи в умовах офісу ІТ-компанії;

– формування рекомендацій зі структуризації захисних компонентів для забезпечення гнучкості та масштабованості рішення;

– тестування та аналіз результатів впровадження системи захисту для оцінки її ефективності та подальшої оптимізації.

2 ПРОЕКТУВАННЯ СИСТЕМИ ЗАХИСТУ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ ПІДПРИЄМСТВА

2.1 Дослідження інформаційних процесів підприємства та роль IoT пристроїв у них

Підприємство, для якого моделюється система захисту IoT-інфраструктури, є невеликою приватною IT-компанією, що спеціалізується на розробці програмного забезпечення та обслуговуванні корпоративних клієнтів. Компанія орендує офіс у бізнес-центрі, в якому вже передбачені початкові заходи фізичної безпеки: контрольований вхід та охорона на території будівлі.

Штат підприємства складається орієнтовно з 10–12 співробітників. Це системний адміністратор, менеджери проєктів, розробники програмного забезпечення, технічний директор, секретар. Основу команди становлять розробники програмного забезпечення — це спеціалісти, які займаються створенням веб- і мобільних застосунків, розробкою внутрішніх сервісів, а також супроводом технічної частини клієнтських рішень. Вони працюють з локальними серверами, Git-репозиторіями, а також взаємодіють із деякими IoT-пристроями через API. Оскільки вони взаємодіють із внутрішніми API та базами даних, існує ризик доступу до незахищених портів сервісів, тому що VLAN-політика не обмежує їхні запити. Ще один варіант подій, що розробник може ненавмисно мати доступ до системи, з якою він не повинен працювати. У подальшому, при створенні системи захисту, слід ретельно опрацювати політику сегментації мережі та контролю доступу, щоб запобігти випадковому або несанкціонованому доступу до критичних сервісів з боку розробників чи інших працівників

Системний адміністратор відповідає за повну підтримку цифрової інфраструктури офісу. До його обов’язків належить налаштування маршрутизаторів, керування VLAN-сегментацією мережі, конфігурація серверів, контроль безпеки даних і резервного копіювання. Проте така мінімальна сегментація є потенційно вразливою. Наприклад, у випадку компрометації пристрою в робочій VLAN-зоні, порушник може отримати доступ до пристроїв

або серверів, які фізично повинні бути ізольовані. Адміністратор має повний доступ до мережевих пристроїв, у тому числі до всіх IoT-пристроїв, які інтегровані в офісне середовище.

Менеджер проєктів координує поточні завдання, відповідає за планування роботи команди, встановлює пріоритети та контролює дедлайни. Його робота значною мірою пов'язана з хмарними сервісами для управління завданнями, а також із засобами комунікації між членами команди та клієнтами. Якщо його облікові дані буде скомпрометовано, це може призвести до витоку внутрішньої інформації. Крім того, відсутня багатофакторна автентифікації у внутрішній мережі для доступу до деяких сервісів може стати слабким місцем, зокрема якщо пристрій менеджера під'єднаний до тієї ж VLAN, що й інші критично важливі пристрої.

Секретар виконує організаційно-адміністративну функцію, тобто веде документацію, приймає відвідувачів, координує зустрічі та забезпечує загальний порядок в офісі. У роботі він використовує персональний комп'ютер, принтер, має доступ до системи відеоспостереження (в межах перегляду трансляції) та працює через службовий обліковий запис. Через такий рівень взаємодії з цифровою інфраструктурою існують ризики: наприклад, відкриття шкідливого файлу або використання вразливого браузера може стати точкою входу загрози у внутрішній сегмент мережі. У подальшому, під час проєктування системи захисту, ці особливості необхідно обов'язково врахувати, щоб мінімізувати ризики, пов'язані з людським фактором та роботою з потенційно вразливими пристроями.

Технічний керівник відділу виконує управлінську та експертну роль, контролює роботу технічної команди, затверджує архітектурні рішення щодо інфраструктури, аналізує ризики та відповідає за впровадження нових технологічних засобів. У його компетенції доступ до критичних вузлів інфраструктури, зокрема до серверів, шлюзів і IoT-сегменту, але вже на рівні стратегічного контролю, а не щоденного адміністрування. Крім того, оскільки він працює в межах тієї самої VLAN, що й аналітичні сервіси, у разі компрометації

його пристрою можливий неконтрольований доступ до систем спостереження та управління.

Загалом, усі працівники користуються персональними робочими місцями з доступом до внутрішньої мережі, який обмежується відповідно до їхніх посадових обов’язків. Такий розподіл допомагає знизити ризики випадкових дій, що можуть зашкодити системі, і водночас забезпечує більш впорядкований рух даних. Однак навіть за таких умов залишаються слабкі місця, які потребують додаткової уваги з боку безпеки.

Інфраструктура організації централізована та поділена на кілька логічних зон, що дозволяє краще відстежувати, де саме і як використовуються пристрої Інтернету речей. Центральна частина — це офісна кімната, де розташовані робочі місця співробітників. Біля входу знаходиться рецепція, яка одночасно виконує функцію контролю доступу. Окремо виділено переговорну кімнату для проведення зустрічей, а також серверну, де зосереджене обладнання, що забезпечує внутрішню IT-інфраструктуру. Для побутових потреб персоналу передбачено кімнату відпочинку, кухню та санвузол. Фізичний план приміщення з розміщенням зон представлено на (рис. 2.1):

Рисунок 2.1 − Схематичне зображення офісу

Розглянемо докладніше, які саме пристрої використовуються та як вони інтегруються в загальну інфраструктуру. Для практичного дослідження особливостей цифрової інфраструктури підприємства було прийнято рішення створити її модель у середовищі Cisco Packet Tracer. Цей інструмент дозволяє візуалізувати структуру мережі, моделювати взаємодію між пристроями та тестувати різні сценарії роботи системи без реального впливу на обладнання. Реалізація схеми в Packet Tracer дає змогу детально відтворити фізичний та логічний поділ офісу, відобразити підключення класичних мережевих елементів і IoT-пристроїв, а також провести первинний аналіз безпеки на основі отриманої моделі. Також, це дуже спростить планування розвитку інфраструктури та дозволить оцінити потенційні ризики ще до впровадження рішень у реальному середовищі. Отже, логічне розміщення і з'єднання з іншими компонентами мережі можна побачити на моделі офісу (рис.2.2).

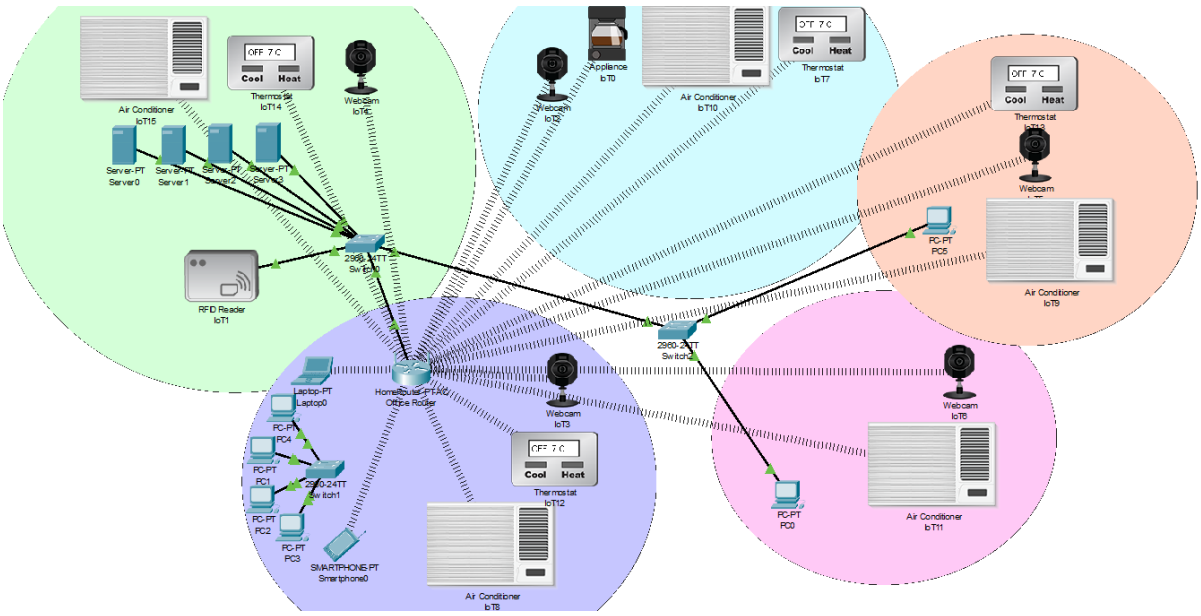


Рисунок 2.2 – Схема офісу у Cisco Packet Tracer

Philips Hue Motion Sensor (рис. 2.3) — це бездротовий сенсор руху, який здебільшого використовується для автоматичного керування освітленням у приміщенні. Його основне призначення це виявляти присутність людини та залежно від налаштувань вмикати або вимикати світло. Завдяки йому, можна не

лише зробити робочий простір зручнішим, а й суттєво знизити енергоспоживання, особливо в офісах, де співробітники часто переміщуються між різними зонами.

Однією з переваг цього сенсора є простота встановлення та налаштування. Пристрій може працювати автономно або в складі розумної системи освітлення Philips Hue, де його функціонал розширюється [32]. Наприклад, через спеціальний шлюз (Hue Bridge) сенсор можна підключити до інших елементів системи: розумних ламп, мобільного застосунку, голосових асистентів або навіть зовнішніх сервісів на приклад IFTTT.

Рисунок 2.3 – Philips Hue Motion Sensor

Сенсор працює на базі протоколу Zigbee, через який він з’єднується зі шлюзом Philips Hue Bridge, а далі з локальною мережею офісу та хмарною інфраструктурою Philips. У межах моделі офісу, що досліджується в цій роботі, встановлено у робочій зоні, переговорній кімнаті та на ресепшні. Крім того, є можливість інтегрування у більш складну IoT-інфраструктуру, наприклад, синхронізувати із системами безпеки, клімат-контролю або контролю доступу. У разі виявлення руху в неробочий час, він може надсилати сигнал на IP-камеру або активувати тривогу. Таке поєднання автоматизації та базового захисту дозволяє

зробити офіс не тільки енергоефективним, а й більш безпечним. У подальшій роботі буде розглянута можливість такого удосконалення.

У системі клімат-контролю офісу використовується розумний термостат Google Nest Thermostat (рис.2.4), який координує роботу з кондиціонерами Daikin Emura II (рис.2.5), оснащеними вбудованими Wi-Fi-модулями.

Рисунок 2.4 − Google Nest Thermostat

Така зв’язка дозволяє ефективно підтримувати комфортну температуру в різних частинах приміщення, реагуючи на зміни навколишніх умов, розклад роботи та рівень завантаженості офісу. Nest Thermostat встановлено в центральній зоні офісу, де він виконує роль основного регулятора клімату [33]. Пристрій з’єднується з локальною мережею за допомогою Wi-Fi та передає дані в Google Cloud, де відбувається обробка інформації та формування рекомендацій щодо температурного режиму. У свою чергу, Daikin Emura II [34], розміщені в окремих зонах, приймають сигнали та коригують роботу відповідно до заданих параметрів. Це дозволяє не просто вручну змінювати температуру, а автоматизувати кліматичні сценарії. Наприклад, знижувати інтенсивність охолодження у вечірній час або в неробочі дні.

Рисунок 2.5 – Daikin Emura II

На жаль, Wi-Fi-зв’язок є типовим вектором атаки для зловмисників. У цьому випадку використовуються слабкі або застарілі протоколи шифрування, зловмисник може перехопити трафік, отримати доступ до хмарного акаунта користувача або маніпулювати роботою пристроїв дистанційно. Особливої уваги потребує взаємодія з хмарною інфраструктурою, оскільки в разі компрометації облікового запису Google зловмисник отримає повний контроль над системою керування кліматом. Ця проблема є вкрай серйозною, оскільки порушення конфіденційності або цілісності каналу керування може мати критичні наслідки для безпеки всього офісного середовища. Тому виявлену вразливість необхідно обов’язково усунути на етапі проєктування системи захисту.

У системі контролю доступу офісу та для обмеження фізичного доступу до серверної кімнати, застосовується електронний замок ZKTeco AL40B (рис. 2.6), який підтримує авторизацію за відбитком пальця та через Bluetooth-підключення. Такий підхід дозволяє поєднати зручність безключового доступу з базовими механізмами біометричної автентифікації [35]. Пристрій зчитує відбитки пальців і зв’язується із системою контролю доступу через Bluetooth або локальну мережу.

Рисунок 2.6 − Електронний замок ZKTeco AL40B

У разі з'єднання через Bluetooth, авторизація здійснюється за допомогою смартфона користувача із відповідним застосунком, але у офісі інтегрується в централізовану систему обліку доступів, що дозволяє адміністратору в реальному часі переглядати журнали входів, додавати або видаляти користувачів та оперативно змінювати правила доступу Однак через використання Bluetooth-з’єднання та відсутність налаштування сучасних протоколів шифрування, зокрема BLE Secure Connections, такий замок стає потенційною ціллю для атак replay або spoofing. Цю вразливість буде враховано та усунено в наступних етапах роботи над системою захисту. Також інша важлива вразливість, це зберігання біометричних даних , що здійснюється на самому пристрої та в локальній системі без шифрування, це створює прямий ризик витоку чутливої персональної інформації. Хоча ZKTeco AL40B і не є висококласним рішенням для об'єктів із найвищим рівнем безпеки, його використання в офісному середовищі як частини багаторівневої системи захисту рекомендується за умови дотримання базових принципів безпечної конфігурації та експлуатації.

Для моніторингу ключових ділянок офісу використовується відеокамера Hikvision DS-2CD2143G0-I (рис. 2.7), яка підтримує функцію інтелектуального виявлення руху [36]. Камери встановлено на вході, у серверній кімнаті, а також у

зоні відпочинку, що дозволяє фіксувати переміщення персоналу, виявляти потенційні загрози фізичній безпеці та зменшувати ризики несанкціонованого доступу. Всі камери, що розміщені по кожній кімнаті офісу, підключені до одного роутера через Wi-Fi-з'єднання, таке рішення викликає серйозні вразливості які потрібно буде усунути.

Рисунок 2.7 − Hikvision DS-2CD2143G0-I

Відеодані такої камери, спершу надходять на мережевий відеореєстратор, де зберігаються та обробляються, а також можуть автоматично завантажуватись у хмарне сховище Hikvision Cloud для віддаленого перегляду або архівування. При поганому налаштованому міжмережевому екрані, зловмисник може отримати доступ через IP-адресу, що може дозволити перегляд відео в реальному часі. Також не менш вразливе є віддалене з'єднання з хмарою Hikvision, якщо облікові дані користувачів слабко захищені або не використовується двофакторна автентифікація.

Окрім IoT-пристроїв, інфраструктура включає основний сервер, на якому розміщено внутрішні сервіси, такі як система обліку, база даних користувачів, централізоване зберігання документів та інші необхідні сервіси для повсякденної роботи. Мережеву інфраструктуру доповнюють кілька керованих комутаторів, які забезпечують розподіл трафіку в межах офісу. Вони дозволяють здійснювати

базову сегментацію трафіку за VLAN, проте кількість таких сегментів наразі обмежена лише трьома, для робочої зони, переговорної та серверної кімнати. Це призводить до потенційної уразливості через можливе змішування різних типів трафіку, наприклад, від IoT-пристроїв, користувачів та систем управління, що може спричинити конфлікти або знизити рівень безпеки. Весь трафік маршрутизується через один основний маршрутизатор, який підтримує базову фільтрацію та управління трафіком між VLAN, але не здатен повноцінно захистити мережу від складних атак чи несанкціонованих спроб доступу. Wi-Fi точка доступу забезпечують бездротове з'єднання для співробітників і гостей офісу. Гостьова мережа ізольована від основної, але в загальному вона працює через той самий маршрутизатор, що й внутрішня мережа. Це спрощує адміністрування, але водночас створює загрозу перехресного доступу при неправильно налаштованих політиках безпеки. До того ж, у разі перевантаження точки доступу або її зламу, можна втратити контроль над певними вузлами внутрішньої інфраструктури.

Робочі місця співробітників представлені стандартними ПК, які підключені до мережі за допомогою дротового Ethernet-з'єднання. Такий спосіб підключення дозволяє зменшити ризики перехоплення трафіку, однак у випадку компрометації одного з комп'ютерів зловмисник може отримати прямий доступ до основних ресурсів мережі через відсутність детальної сегментації та обмеженого моніторингу на рівні користувачів. Крім того, не всі ПК мають однаковий рівень оновлень або систем захисту, що створює додаткову нерівномірність у загальному рівні безпеки.

Інформаційна структура підприємства побудована на поділі мережевих ресурсів за функціональним призначенням. У моделі реалізовано кілька VLAN: основна внутрішня мережа, окремий сегмент для гостьового Wi-Fi, мережа для IoT-пристроїв, а також ізольований канал для серверного обміну. Такий підхід дозволяє мінімізувати перетин між критичними системами та пристроями, що мають потенційно вразливі протоколи чи обмежену безпеку. У подальших етапах дослідження, зокрема під час побудови моделі загроз та моделі порушника, ці

вразливості буде враховано як базові передумови для формування системи захисту всієї інфраструктури підприємства.

З огляду на перелік задіяних IoT-пристроїв, їх розміщення в офісі та характер взаємодії між ними, можна зробити висновок, що офісна мережа охоплює доволі складну інформаційну структуру. У межах цієї інфраструктури постійно відбувається обмін даними, як між самими пристроями так і між ними та зовнішніми хмарними сервісами. Для подальшого аналізу важливо зрозуміти, як саме циркулює інформація в цій системі. На основі структури підприємства та моделі мережевої взаємодії можна виокремити такі основні типи інформаційних потоків (рис.2.8).

Рисунок 2.8 − Основні інформаційні потоки

В офісному середовищі обчислювальні процеси забезпечують повсякденну діяльність компанії: обробку даних, документообіг, планування та зв’язок між відділами. У цих процесах пристрої Інтернету речей можуть виступати як елементи автоматизації та підвищення ефективності, зокрема, інтерактивні інформаційні панелі слугують для поширення внутрішньої інформації, а смарт-розетки дозволяють централізовано керувати живленням офісного обладнання. В разі виходу таких пристроїв з ладу або компрометації їхнього програмного забезпечення може статися порушення офісного ритму, збої в роботі обладнання, ризик несанкціонованого відключення критичних пристроїв.

Хмарна синхронізація та взаємодія з віддаленими сервісами реалізується через постійне з'єднання з зовнішніми платформами – такими як сервіси керування пристроями, платформи збору та аналізу даних, хмарні інтерфейси безпеки. Більшість сучасних IoT-рішень, зокрема IP-камери, біометричні замки та розумні термостати, мають потребу в такій синхронізації для зберігання історії даних, віддаленого керування або обробки аналітики. Компрометація каналу зв'язку або облікових записів, через які здійснюється доступ до хмари, може призвести до втрати даних, порушення цілісності інформації або перехоплення відео- чи телеметричних потоків сторонніми особами.

Гостьовий трафік формується відвідувачами офісу, які отримують доступ до бездротової мережі для проведення презентацій, роботи або перегляду інформації. У контексті IoT-систем, ці підключення можуть створювати потенційні вектори атаки, особливо якщо гостьова мережа не ізольована від корпоративної. IoT-пристрої, як-от Raspberry Pi-дисплеї чи кондиціонери з Wi-Fi-модулями, можуть бути випадково чи навмисно атаковані з гостьової мережі, що створює ризики саботажу, шкідливого перепрошивання або запуску шкідливого коду. Системне адміністрування та моніторинг включає використання серверів, шлюзів та мережевого обладнання для забезпечення стабільної та безпечної роботи інфраструктури. IoT-пристрої, підключені до централізованої системи керування, як-от камери відеонагляду або системи автоматичного освітлення, мають канали зворотного зв'язку з адміністративними консолями. Порушення моніторингового контролю може призвести до втрати видимості над подіями в офісі, затримки реагування на інциденти та неможливості дистанційного усунення проблем.

Критичні сповіщення та тригери є важливою частиною роботи з безпекою. Наприклад, система детекції руху, інтегрована з IP-камерою, або сигнал про відкриття дверей у серверну кімнату, надсилає повідомлення адміністраторам. Такі події зазвичай супроводжуються передачею даних у внутрішню мережу або хмарне середовище, де вони можуть бути оброблені для подальших дій. Пристрій Інтернету речей в цій системі виконують функцію сенсорного "першого рівня захисту". Якщо зловмисник зможе нейтралізувати ці сповіщення або спричинити

DoS-атаки на систему оповіщення, це дозволить йому залишатися непоміченим у разі фізичного вторгнення чи втручання в інфраструктуру.

При проєктуванні мережевої інфраструктури офісу та впровадженні IoT-пристроїв основна увага була зосереджена на функціональності та зручності користування. Однак, на жаль, визначення чіткої відповідальності за безпеку цих пристроїв залишився поза увагою. Після початкової інсталяції та налаштування системи захисту, питання кібербезпеки IoT-функціоналу фактично не отримували подальшого супроводу та оновлення. Такий підхід створює серйозні ризики, адже без постійного моніторингу та управління вразливостями й потенційними загрозами IoT-мережа може стати «слабким місцем» в загальній безпековій архітектурі підприємства.

Отже, було визначено ключові інформаційні процеси підприємства та встановлено, яку роль у них відіграють пристрої Інтернету речей. Отримані результати формують основу для подальшого аналізу безпекових ризиків. У наступному розділі буде побудовано модель потенційного порушника та модель загроз, що дозволить краще зрозуміти вразливі місця в наявній інфраструктурі.

2.2 Побудова моделі загроз та моделі порушника

На попередньому етапі ми вже сформували загальне уявлення про інфраструктуру офісу IT-компанії: визначили ключові зони, дослідили склад пристроїв Інтернету речей, принципи їхньої взаємодії, а також розглянули основні інформаційні потоки між компонентами системи. Далі логічним кроком є побудова моделі загроз, тобто виявлення можливих векторів атак, слабких місць у системі та визначення того, хто або що може бути джерелом загрози. Це, у свою чергу, стане основою для подальшого проєктування системи захисту.

Коли ми говоримо про загрози для IoT-систем, маємо на увазі не якісь абстрактні небезпеки, а цілком реальні ситуації, що можуть порушити безпеку інформації або вивести з ладу частину інфраструктури. Під загрозою розуміється

будь-яка подія чи умова, яка може суперечити політиці безпеки підприємства або зашкодити ресурсам комп'ютерної системи. Згідно з національними стандартами у сфері технічного захисту інформації (зокрема, НД ТЗІ 1.1-002-99 та 1.4-001-2000), усі загрози для автоматизованих систем (до таких належить і наша офісна IoT-інфраструктура) умовно поділяються на чотири основні типи:

– порушення конфіденційності інформації, одержання інформації сторонніми особами всупереч встановлених правил доступу. Наприклад перехоплення повідомлень з датчиків чи злам відеокамери;

– порушення цілісності інформації, повне або часткове знищення інформації, її викривлення або модифікація. У випадку з IoT це може бути, скажімо, модифікація команд, які надсилаються на пристрої, або нав'язування фальшивих даних;

– порушення доступності інформації, повна або часткова втрата працездатності системи, блокування доступу до інформації. Наприклад атака типу DoS, яка виводить з ладу шлюз або хмарний сервіс, до якого прив'язані пристрої;

– втрата спостережності або керованості системи обробки, сюди входять проблеми з ідентифікацією користувачів, неконтрольованим доступом до системи чи втратою можливості слідкувати за тим, що відбувається в мережі. Тобто коли ми не можемо чітко сказати, хто і що робить у системі.

За типом основного засобу, який використовується для реалізації загрози, всі джерела загроз поділяються на такі групи:

– людина;

– апаратура (основні та допоміжні технічні засоби і системи);

– програма;

– фізичне середовище.

У разі реалізації техногенних загроз, навмисного чи не навмисного виду, уразливості системи IoT можуть призвести до серйозних наслідків, що впливають на основні аспекти безпеки інформації — конфіденційність (к), цілісність (ц) та доступність даних і сервісів (д). Побудуємо модель загроз у вигляді таблиці,

користуючись даними, отриманими в результаті попередніх досліджень (Табл. 2.1).

Таблиця 2.1 – Модель загроз

№	Тип та визначення загрози	Джерело загрози	Ймовірність	Рівень шкоди	Наслідки		
					К	Ц	Д
1	2	3	4	5	6	7	8
Випадкові загрози техногенного походження							
1.	Пожежа або вибух	Середовище	Низька	Неприпустимо високий	-	+	+
2.	Відмова або збої пристроїв IoT	Апаратура	Висока	Високий	-	+	+
3.	Відмови, помилки програмного забезпечення	Програми	Висока	Високий	-	+	+
4.	Випадкові помилки працівників, помилкове конфігурування та адміністрування системи	Людина	Висока	Неприпустимо високий	+	+	+
5.	Ураження пристроїв вірусами та іншим шкідливим ПЗ	Людина, Програми	Середня	Середній	+	+	+
6.	Аварійна відмова електроживлення	Середовище, Апаратура	Середня	Високий	-	-	+
7.	Вихід з ладу сенсорів або виконавчих пристроїв	Апаратура	Висока	Середній	-	+	+
8.	Радіоперешкоди	Середовище	Низька	Низький	-	-	+
Навмисні загрози техногенного походження							
1.	Несанкіонований віддалений доступ	Людина (зовнішній зловмисник)	Висока	Неприпустимо високий	+	+	+

Кінець таблиці 2.1

1	2	3	4	5	6	7	8

2.	Впровадження шкідливого програмного забезпечення	Людина (зовнішній зловмисник)	Висока	Високий	+	+	+
3.	Умисне пошкодження або перепрошивка пристроїв	Людина (зовнішній або внутрішній зловмисник)	Середня	Високий	-	+	+
4.	Атаки через підміну прошивки	Людина (зовнішній або внутрішній зловмисник)	Середня	Високий	+	+	+
5.	Атака на шлюзи або маршрутизатори	Людина (зовнішній зловмисник)	Висока	Неприпустимо високий	+	+	+
6.	Соціальна інженерія або фішинг	Людина (зовнішній або внутрішній зловмисник)	Висока	Високий	+	+	+
7.	Перехоплення та підміна даних з сенсорів	Людина (зовнішній зловмисник)	Високий	Середній	-	+	-
8.	Умисне перевантаження мережі (DDoS-атака)	Людина (зовнішній зловмисник)	Середня	Високий	-	-	+
9.	Цілеспрямоване видалення або пошкодження журналів подій	Людина (зовнішній або внутрішній зловмисник)	Середня	Високий	+	+	-

Після побудови моделі загроз, яка враховує типові сценарії атак, джерела їх виникнення, а також ймовірність та рівень їх шкоди в межах IoT-інфраструктури підприємства, постає питання оцінки того, наскільки ці загрози реальні та які з них можуть завдати найбільшої шкоди. Для цього було створено матрицю ризиків, яка ґрунтується на вже визначених загрозах і дозволяє краще зрозуміти, які з них потребують першочергової уваги. Матриця ризиків — це інструмент, що допомагає зіставити ймовірність виникнення кожної загрози з можливими

наслідками її реалізації. Вона надає візуальне уявлення про критичність кожного ризику та дозволяє впорядкувати їх за пріоритетністю (табл. 2.2). Такий підхід забезпечує більш зважене планування подальших заходів безпеки, зокрема в умовах обмежених ресурсів. У нашому випадку матриця стала логічним продовженням побудованої моделі загроз і лягла в основу подальших рішень щодо проєктування технічних та організаційних засобів захисту. Аналіз побудованої матриці ризиків дозволяє виокремити загрози, що мають високу ймовірність виникнення та високий або критичний рівень шкоди, тобто становлять найбільшу загрозу для стабільної роботи IoT-інфраструктури підприємства.

Таблиця 2.2 − Матриця ризиків

Шкода / Ймовірність	Низька	Середня	Висока	Неприпустимо висока
Низька	1	0	0	1
Середня	0	0	5	0
Висока	0	2	6	4

Саме ці загрози мають бути опрацьовані в першу чергу під час проєктування системи захисту. До найкритичніших ризиків належать:

– несанкціонований віддалений доступ до інфраструктури;
– помилки адміністрування та конфігурування системи;
– атаки на маршрутизатори або шлюзи;
– пожежа або вибух;
– відмови або збої пристроїв IoT.

Особливого значення набуває важливість посилення ізоляції між сегментами мережі, впровадження чітких правил контролю доступу, організація журналів подій, а також підвищення обізнаності персоналу щодо базових принципів кібербезпеки в роботі з інфраструктурою. Однак для повнішого розуміння потенційних ризиків недостатньо лише знати, які загрози можуть виникнути. Важливо також чітко уявляти, хто саме може бути їх джерелом, які

цілі переслідує потенційний зловмисник, якими ресурсами він володіє та які методи може використовувати. Саме тому наступним кроком у проєктуванні системи захисту стало формування моделі порушника, тобто уявного профілю атакувальної сторони, що допомагає більш точно визначити, як повинна поводитись система безпеки у відповідь на різні сценарії вторгнення. У випадку з IoT ця задача ускладнюється через велику кількість взаємопов'язаних пристроїв, що можуть стати точкою входу для зловмисника. Крім того, враховуючи людський фактор, дії порушника не завжди є цілеспрямованими, іноді вони можуть бути ненавмисними але не менш небезпечними.

Оскільки під порушником зазвичай розуміється конкретна особа або група осіб, побудова його чіткої математичної моделі є надзвичайно складним завданням. Тому в практиці захисту інформації, зокрема в контексті IoT, зазвичай застосовують описову або неформальну модель порушника, що враховує найбільш типові характеристики, мотивацію та рівень підготовки потенційних зловмисників. Розглянемо можливу модель порушника для досліджуваної IoT-інфраструктури (табл. 2.3). У результаті побудови моделі порушника вдалося оцінити потенційні ризики з боку різних категорій осіб, які мають доступ до внутрішньої інфраструктури підприємства. Кожна з них була проаналізована за ключовими критеріями, такими як мотивація, рівень доступу, кваліфікація, методи порушення захисту та інші чинники. Отримані результати дозволяють краще зрозуміти, хто саме становить найбільшу загрозу для системи безпеки та на що варто звернути увагу при розробці захисних заходів. Системний адміністратор отримав найвищий сумарний бал загрози (24), що цілком логічно, з огляду на його повний доступ до критичних компонентів інфраструктури, включно із захисними механізмами. Це підкреслює необхідність суворого контролю дій цієї ролі, журналювання кожного важливого доступу, а також впровадження багаторівневої автентифікації. Технічний керівник, з показником у 22 бали, також входить до групи підвищеного ризику. Його доступ до стратегічно важливих ресурсів і можливість впливати на робочі процеси створює потенціал для зловживань, навіть при високому професіоналізмі. Розробник (19 балів) має змогу взаємодіяти з

кодом, внутрішніми сервісами, а в деяких випадках і з IoT-прошивками. Це означає, що навіть ненавмисна помилка або вразливість у коді може стати точкою входу для загроз. Менеджер проєктів та секретар мають помірний рівень ризику (13–14 балів), але це не виключає ймовірності компрометації їхніх облікових записів через соціальну інженерію або фішинг. Їхня діяльність вимагає уваги з боку політик доступу та базового навчання кібергігієни.

Таблиця 2.3 – Модель порушника

№	Посада	Категорія порушника	Мотив порушника	Рівень обізнаності щодо IoT	Можливості щодо подолання системи	Можливості за часом дії	Можливості за місцем дії	Сума загроз
1	Системний адміністратор	В4 (адмін безпеки)	М4	К4	З4	Ч4	Д5	24
2	Розробник	В3 (користувач АС)	М2	К3	З3	Ч3	Д4	19
3	Менеджер проєктів	В5 (керівництво)	М2	К1	З1	Ч3	Д3	14
4	Секретар	В3 (користувач АС)	М1	К1	З1	Ч3	Д3	13
5	Прибиральник	В1 (технічний персонал)	М1	К1	З1	Ч2	Д2	9
6	Гість	В6 (зовнішній)	М1	К1	З1	Ч2	Д1	7
7	Технічний керівник	В5 (керівництво)	М3	К4	З3	Ч4	Д4	22

Гість та прибиральник, з найнижчими показниками (7–9 балів), становлять мінімальну загрозу. Проте і в їхньому випадку важливо обмежити фізичний доступ до мережевого обладнання та критичних зон, аби зменшити ризики,

пов’язані з потенційними випадковими або цілеспрямованими діями. Отже, можна зробити висновок, що найнебезпечнішими залишаються внутрішні особи з широкими правами доступу. Саме тому система захисту має містити механізми виявлення нетипової активності, чітке розмежування доступу за ролями та контроль дій персоналу з високим рівнем довіри.

2.3 Проектування системи захисту

Після аналізу наявної мережі на приватному ІТ-підприємстві, визначення інформаційних процесів, побудови моделі загроз і класифікації потенційних порушників стало очевидним, що в умовах зростання кіберзагроз та кількості використання підключених пристроїв, необхідна система захисту, яка забезпечуватиме захищене функціонування внутрішньої мережі та безпечну взаємодію з зовнішніми інформаційними середовищами.

Основною метою є удосконалення наявної системи захисту, яка забезпечить конфіденційність, цілісність та доступність інформації, що циркулює в межах офісної IoT-інфраструктури. Важливо чітко розуміти, яких саме результатів ми прагнемо досягти, основна задача полягає в розробці IoT-інфраструктури на підприємстві більш стійкою до загроз та забезпечити стабільну й безпечну роботу всіх її компонентів. Інакше кажучи, не просто поставити "захист заради захисту", а досягти реального підвищення рівня безпеки в умовах роботи невеликого ІТ-підприємства. Для цього система має захищати критичні частини мережі, зокрема IoT-пристрої, сервери та точки доступу, а також ускладнювати несанкціонований доступ до даних. Усе це базується на актуальних принципах інформаційної безпеки Інтернету речей, що діють на момент розробки, із закладеною можливістю подальшого удосконалення системи відповідно до нових викликів і загроз, з якими вона може зіткнутися в майбутньому.

Особлива увага приділяється здатності системи вчасно реагувати на загрози як з боку зовнішніх зловмисників, так і з боку внутрішніх користувачів — як у

разі навмисних дій, так і випадкових помилок. Тому в межах цієї роботи передбачається не лише посилення технічного захисту від атак, а й впровадження організаційних механізмів контролю, постійного моніторингу та оперативного інформування відповідальних осіб про потенційні або вже наявні інциденти.

Отже після побудови моделі загроз і матриці ризиків стало зрозуміло, що найбільшу небезпеку для офісної IoT-системи становлять загрози, які поєднують високу шкоду з високою або середньою ймовірністю. Саме ці загрози стали орієнтиром для визначення пріоритетних напрямків захисту. Відповідно до цього, сформульовано основні завдання, які має реалізовувати проєктована система безпеки:

– захист від несанкціонованого доступу до мережі та пристроїв
– захист від людських помилок та внутрішніх загроз;
– захист шлюзів та маршрутизаторів IoT-сегменту;
– розгортання сервера централізованого журналювання;
– безпечне оновлення і адміністрування IoT;
– виявлення та реагування на підозрілу активність;
– захист каналу для передачі даних.

З огляду на ці завдання, розпочнемо реалізацію системи захисту з найпріоритетнішого напряму, а саме протидії несанкціонованому доступу до інфраструктури Інтернету речей приватного IT-підприємства. Отже, для забезпечення контролю доступу та підвищення безпеки IoT-пристроїв в офісній мережі було реалізовано VLAN-сегментацію по бездротовій мережі, використовуючи додатково ще один домашній маршрутизатор. На рис. 2.9, зображено як саме додала роутер, один з них буде призначений для всього офісу а інший переношу у серверну кімнату та перепідключаю всі пристрої Інтернету речей до нього. Кожен з цих маршрутизаторів підключається до різних VLAN на центральному комутаторі, що дає змогу імітувати логічне розділення трафіку бездротових пристроїв.

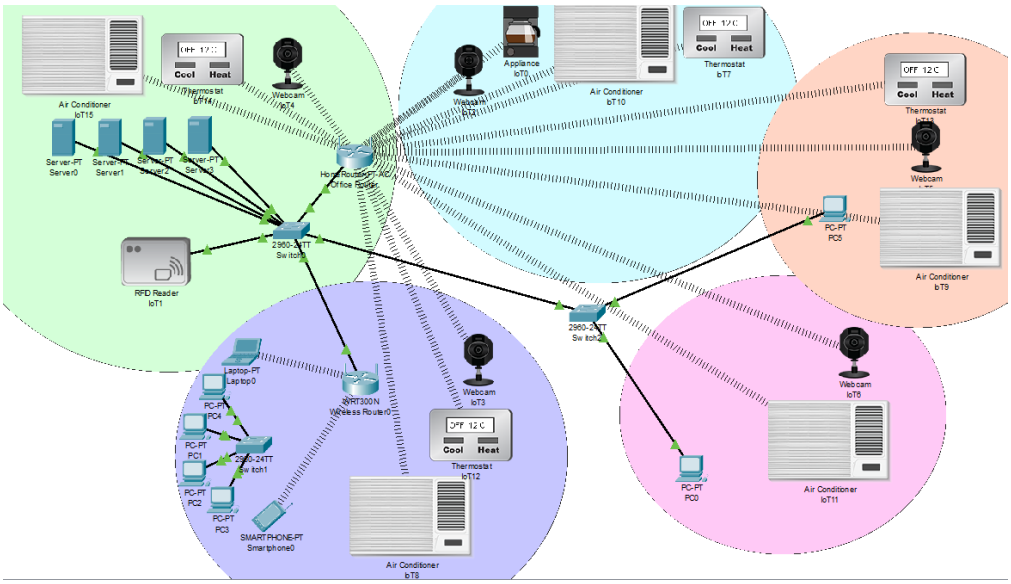


Рисунок 2.9 − Зображення додавання ще одного маршрутизатора в мережу

Першим кроком, для кожного маршрутизатора налаштовуємо унікальний SSID, який відрізнятиметься назвою, щоб користувачі могли підключатися саме до потрібної бездротової мережі. Далі на комутаторі, до якого підключаються маршрутизатори, створюємо два окремих VLAN, кожен з яких відповідає одній з Wi-Fi мереж. Потім порти комутатора, до яких підключені маршрутизатори, конфігуруємо як access-порти і призначаємо їм відповідні VLAN. Таким чином трафік від кожного бездротового маршрутизатора буде логічно відокремлений, і це дозволить відтворити розмежування VLAN на рівні Wi-Fi. Після цього бездротові клієнти, підключені до кожного SSID, отримають доступ до окремих VLAN що сегментує мережу. Для посилення контролю доступу між сегментами мережі в рамках реалізації розмежування повноважень було налаштовано списки контролю доступу. Основна ідея полягає в ізоляції мережі пристроїв Інтернету речей від інших сегментів мережі. Завдяки цьому жоден користувач з офісного сегменту не має доступу до IoT, окрім серверу, що виконує контроль, та адміністратора. Таке обмеження дозволяє запобігти втручанню сторонніх осіб, проникненню зловмисного трафіку та захищає IoT-вузли від зловживання внутрішніми або скомпрометованими хостами.

Окрім зовнішніх атак і технічних вразливостей, важливим вектором загроз для офісної IoT-інфраструктури залишаються людський фактор та внутрішні

порушники. Як показала побудована модель загроз і модель порушника, значна частина ризиків пов’язана саме з ненавмисними діями співробітників або зловживанням доступом з боку осіб, що мають довіру в системі. Тому наступним кроком у проєктуванні системи захисту є реалізація заходів, спрямованих на зниження ймовірності помилок користувачів та посилення внутрішнього контролю. Зокрема, для портів комутаторів, до яких підключаються IoT-пристрої, реалізовано фільтрацію за MAC-адресами (port security), що блокує будь-які спроби підключення невідомих пристроїв. Крім того, було обмежено HTTP-доступ до пристроїв з усіх VLAN, не обмежували тільки адміністратора. Впроваджено сегментацію через VLAN і систему облікових записів з різними рівнями привілеїв для забезпечення лише необхідного рівня доступу для персоналу. Такі заходи суттєво знижують ризики, пов’язані з людським фактором і внутрішніми загрозами.

Оскільки маршрутизатори є ключовими елементами інфраструктури Інтернету речей, важливим кроком стала їх належна захищеність від несанкціонованого доступу, змін конфігурації та потенційних атак з боку внутрішніх або зовнішніх суб’єктів. Для цього було впроваджено такі заходи:

– адміністрування маршрутизатора здійснюється виключно через захищений протокол SSH, при цьому протокол Telnet вимкнено повністю;

– доступ до інтерфейсів керування маршрутизатором дозволено лише з визначеної IP-адреси адміністративної станції за допомогою списків контролю доступу (ACL);

– усі другорядні сервіси, що не використовуються в межах IoT-сегменту (HTTP-сервер, SNMP), були вимкнені для зменшення поверхні атаки;

– здійснюється збереження резервної конфігурації пристроїв, що дозволяє швидко відновити мережу у випадку збоїв або атак.

З метою централізованого спостереження за подіями, пов’язаними з функціонуванням IoT-інфраструктури, у межах запропонованої архітектури було реалізовано окремий сервер журналювання. Його функція полягає у збереженні, обробці та аналізі подій, що надходять від маршрутизаторів, мережевого

обладнання, IoT-пристроїв та інших критичних компонентів. Для підвищення безпеки лог-сервер було фізично та логічно ізольовано в окремий сегмент мережі, який не перетинається з іншими мережевими зонами, що забезпечує базовий рівень захисту від несанкціонованого доступу. Підключення до цього вузла дозволено лише з обмеженого переліку джерел, виключно від певних IoT-пристроїв та інструментів моніторингу, що потребують передавання логів. Усі інші зони, включно з користувацькими мережами, не мають можливості звертатися до сервера, що дозволяє мінімізувати ризики витоку або модифікації інформації. Керування журналюванням здійснюється централізовано з одного адміністративного робочого місця, яке також ізольоване від загальнодоступної мережі. Важливо, що жоден IoT-пристрій не має змоги переглядати або змінювати збережену на сервері інформацію, що дозволяє зберігати цілісність логів навіть у разі компрометації окремих елементів системи. Завдяки цьому впровадженню, лог-сервер стає не лише джерелом історичних даних, а й інструментом раннього виявлення аномалій та потенційних інцидентів безпеки в реальному часі.

Узагальнюючи результати проєктування, можна стверджувати, що реалізовані заходи інформаційної безпеки дозволяють суттєво зменшити ймовірність реалізації ключових загроз, визначених у матриці ризиків. Кожен з елементів захисту, від сегментації мережі до централізованого журналювання подій, був орієнтований на послаблення впливу найбільш критичних векторів атак. Завдяки впровадженим рішенням рівень залишкових ризиків для більшості потенційних загроз знижено до прийнятного, відповідного заданим критеріям безпеки для офісної IoT-інфраструктури. Це підтверджує відповідність системи сформульованим завданням та загальній моделі загроз.

2.4 Висновок

У межах цього розділу, було проведено дослідження та всебічний аналіз структури IoT-інфраструктури підприємства. Ми окреслили основні зони

офісного простору та визначили перелік пристроїв Інтернету речей, які забезпечують функціональність, моніторинг і контроль доступу до ключових приміщень. Створена мережева схема в середовищі Cisco Packet Tracer дозволила наочно відобразити взаємозв'язки між пристроями, логіку їхнього розміщення, а також виявити потенційні вразливості у структурі.

Далі, на основі зібраної інформації, було побудовано модель загроз, яка враховує як техногенні, так і навмисні ризики, що можуть впливати на конфіденційність, цілісність та доступність інформації. У межах цієї моделі ми також визначили типові наслідки реалізації загроз та їхній вплив на функціонування IoT-системи. Відповідно, було розроблено модель порушника, яка класифікує можливих зловмисників за рівнем доступу, мотивацією та технічними можливостями.

На основі проведеного аналізу було сформовано підхід до побудови системи захисту IoT-інфраструктури підприємства. Отримані результати дозволяють зробити висновок, що захист IoT-середовища вимагає комплексного підходу, який об'єднує технічні, організаційні та процедурні заходи. Проведене дослідження створює основу для впровадження ефективних рішень у сфері безпеки сучасних підприємств, що використовують інтелектуальні пристрої в своїй повсякденній діяльності.

На наступному етапі роботи планується безпосереднє впровадження спроєктованої системи захисту в мережеву інфраструктуру підприємства. Буде розроблено настанову з експлуатації системи захисту IoT-пристроїв, яка включатиме практичні рекомендації щодо налаштування, обслуговування та оновлення системи з урахуванням змін у мережевому середовищі або складі пристроїв. Це дозволить забезпечити сталий рівень безпеки в умовах реального функціонування підприємства.

3 ІМПЛЕМЕНТАЦІЯ, ВПРОВАДЖЕННЯ, РЕАЛІЗАЦІЯ, ТЕСТУВАННЯ, СТВОРЕННЯ НАСТАНОВ ПО ЕКСПЛУАТАЦІЇ

3.1 Настанови щодо впровадження мережевої компоненти системи захисту

Побудова мережевої частини системи захисту дозволяє забезпечити захист корпоративного середовища відповідно до визначених вимог. Надійність таких аспектів, як контроль доступу, ізоляція мережевих сегментів і захист IoT-пристроїв від несанкціонованих дій, безпосередньо залежить від правильності реалізації проєктних рішень. При розробці системи були враховані як технічні особливості офісної IoT-інфраструктури, так і результати аналізу загроз і можливих порушників, що дозволило адаптувати засоби захисту до реальних умов функціонування мережі. Послідовна реалізація мережевих механізмів безпеки є необхідною для досягнення цілей, поставлених у межах розробленої системи. Для цього було обрано відповідне обладнання, яке здатне забезпечити основні функції захисту — від сегментації та контролю доступу до централізованого журналювання й обмеження внутрішніх загроз. У подальшому розглянуто перелік технічних засобів, що рекомендовані для впровадження даної системи захисту. В контексті проєктованої системи захисту маршрутизатори мають використовуватись такі, що підтримують функціональність VLAN і реалізацію списків контролю доступу (ACL). Їх використання дозволяє ефективно розмежувати сегменти мережі, ізолювати IoT-пристрої від решти інфраструктури та обмежити небажаний трафік між різними віртуальними локальними мережами. Крім того, ці пристрої забезпечують базовий захист від несанкціонованого доступу та можуть бути інтегровані в централізовану систему моніторингу й адміністрування. Серед моделей, що відповідають таким вимогам, варто відзначити Cisco ISR 4321, або бюджетніший варіант, Juniper SRX100H2. Вони поєднують гнучкість конфігурації, підтримку VPN і достатню продуктивність для офісного середовища з активною IoT-інфраструктурою.

Суттєву роль у реалізації сегментації мережі та забезпеченні контролю доступу відіграють комутатори з розширеною функціональністю. Вони

дозволяють не лише розмежувати трафік між окремими VLAN, але й забезпечити захист на рівні портів завдяки використанню механізмів Port Security. Це дає змогу контролювати, які пристрої можуть підключатися до мережі, та запобігати несанкціонованим спробам доступу, зокрема через MAC-спуфінг. Додатково підтримка протоколу 802.1X, пріоритизація трафіку (QoS) і можливість налаштування ACL безпосередньо на портах робить такі комутатори ефективним інструментом для побудови безпечного середовища. До рекомендованих моделей належать Cisco Catalyst 2960, HP Aruba 2530 та MikroTik CRS.

Для забезпечення всебічного захисту мережевої інфраструктури, окрім маршрутизаторів і комутаторів, доцільно використовувати спеціалізовані засоби, зокрема міжмережеві екрани нового покоління. Вони дають змогу не лише контролювати вхідний і вихідний трафік, а й активно виявляти спроби вторгнення завдяки інтегрованим системам IDS/IPS та функції глибокої перевірки стану з'єднань. Такі рішення як Cisco ASA 5506-X, Fortinet FortiGate 60E або програмне забезпечення pfSense [38] забезпечують гнучкість, підтримку VPN-з'єднань і можливість інтеграції з централізованими системами моніторингу безпеки.

Важливим елементом є й організація безпечного бездротового доступу до мережі. Сучасні точки доступу Wi-Fi мають підтримувати створення кількох SSID з прив'язкою до окремих VLAN, що дозволяє розмежувати трафік IoT-пристроїв, офісного обладнання, адміністративного сегменту та гостьової мережі. Окрім цього, обов'язковим є використання сучасних стандартів шифрування, таких як WPA3, а також підтримка протоколів RADIUS для контролю доступу. З-поміж придатних моделей можна відзначити Cisco Aironet 1830, Ubiquiti UniFi U6-Lite та TP-Link EAP245, які поєднують функціональність із зручною централізованою конфігурацією.

Для підтримки надійного контролю за подіями в мережі використовується сервер централізованого журналювання. Він відповідає за приймання логів із маршрутизаторів, комутаторів, точок доступу та IoT-пристроїв, а також за забезпечення їх захищеного зберігання. Такий сервер має гарантувати цілісність даних і можливість їх подальшого аналізу. У реалізації цієї функції можуть бути

використані як окремі апаратні рішення, так і програмні, до наприкладу, Linux-сервер із налаштованим rsyslog або Graylog, а також інструменти Splunk чи Elastic Stack.

Завершальним компонентом виступає спеціалізований шлюз безпеки для IoT, призначений для контролю й фільтрації трафіку між пристроями, а також для захисту протоколів, які використовуються в IoT-комунікаціях, таких як MQTT або CoAP. Важливо, щоб такі шлюзи підтримували шифрування через TLS, функціональність VPN та інтеграцію з централізованими засобами моніторингу. Для цих цілей можуть застосовуватися Cisco IoT Gateway [38] або Dell Edge Gateway, які дозволяють організувати надійний рубіж безпеки між локальною мережею та зовнішнім середовищем.

Окрім правильного підбору мережевого обладнання, важливу роль у забезпеченні стабільної та захищеної роботи всієї системи відіграє його фізичне розміщення та спосіб підключення. Раціональна організація простору, врахування вимог безпеки та технічного обслуговування дозволяють зменшити ризики, пов’язані з фізичним доступом чи збоєм живлення. З огляду на модель загроз, що була спрєктована пізніше, фізичне розміщення обладнання має бути організоване відповідно до принципів безпечного зонування. Усі ключові пристрої, зокрема маршрутизатори, центральні комутатори, а також сервер журналювання подій, доцільно розмістити в окремій серверній кімнаті. Це приміщення повинно бути обмеженим для доступу сторонніх осіб, а сам контроль доступу бажано реалізувати через карткову систему або кодовий замок. Робочі місця співробітників і пристрої, що не потребують підвищених заходів фізичної безпеки (наприклад, принтери, освітлення чи розумні сенсори), можуть розташовуватись у загальному офісному просторі. Однак навіть у такому середовищі зберігається мережеве розділення за допомогою VLAN, що дозволяє мінімізувати вплив потенційних інцидентів між логічно ізольованими сегментами. Інші IoT-пристрої, зокрема камери спостереження, датчики та контролери, встановлюються з урахуванням їхнього функціонального призначення, проте варто уникати їх доступності для фізичного втручання. Найбільш доцільним є їх розміщення під

стелею, у закритих монтажних коробках або кабель-каналах, що ускладнює спроби несанкціонованого доступу.

Що стосується організації бездротового зв'язку, то точки доступу повинні бути розміщені рівномірно в межах офісного приміщення, окремо для сегменту IoT та сегменту офісної діяльності. Це дозволяє чітко розмежовувати трафік через окремі SSID, прив'язані до відповідних VLAN. Схема підключення мережевих пристроїв також повинна бути логічно структурованою. Центральний керований комутатор, розміщений у серверній, виконує функцію вузла для підключення різних пристроїв до ізольованих VLAN-сегментів. Пристрої підключаються або напряму через фізичні порти, або опосередковано через бездротові мережі. Підключення маршрутизаторів виконується до окремих портів комутатора, кожен з яких призначений для окремого VLAN, що забезпечує точне розмежування навіть при роботі з бездротовим трафіком. Сервер журналювання, як окремий компонент системи безпеки, під'єднується до комутатора у виділеному сегменті з обмеженим доступом. Він функціонує як приймач логів з усіх інших пристроїв, не здійснюючи зворотної комунікації, що дозволяє уникнути витоку інформації чи зовнішнього втручання. Усі мережеві з'єднання рекомендовано виконувати за допомогою якісного екранованого кабелю, не нижче категорії Cat5e [39]. Кабельні лінії варто прокладати в закритих каналах або під плінтусами, уникаючи сусідства з силовими кабелями для зменшення впливу електромагнітних завад.

У критичних частинах мережі доцільно передбачити механізми резервування. Це може бути реалізовано як другий фізичний кабель між ключовими пристроями, так і додатковий бездротовий канал для аварійного доступу. У симуляційному середовищі Cisco Packet Tracer, подібне рішення моделюємо через дублювання з'єднань і налаштування резервних маршрутів.

Реалізація ефективної системи захисту потребує не лише правильного вибору обладнання, а й належного його налаштування відповідно до поставлених завдань. У контексті захисту мережевої інфраструктури Інтернету речей це стосується, зокрема, конфігурації ключових пристроїв, що відповідають за сегментацію, контроль доступу та безпечну передачу даних.

Для забезпечення ефективної сегментації мережі та контролю доступу було впроваджено низку налаштувань, що відповідають поставленим завданням захисту інфраструктури Інтернету речей. Перш за все, мережа була розділена на окремі віртуальні локальні мережі, які ізолюють IoT-пристрої від інших сегментів інфраструктури, що суттєво знижує ризики поширення потенційних атак. Так, для IoT-пристроїв виділено VLAN 10, для робочих станцій користувачів — VLAN 20, адміністративного персоналу — VLAN 30, а також окремий VLAN 99 для управління і сервера журналювання.

Додатково застосовано списки контролю доступу, які обмежують небажаний трафік між VLAN, зокрема забороняючи доступ звичайних користувачів до IoT-сегменту, залишаючи його відкритим лише для адміністраторів. Це забезпечує жорсткий контроль над тим, хто може взаємодіяти з пристроями Інтернету речей. Для бездротових мереж впроваджено стандартні методи шифрування, такі як WPA2 або WPA3, зокрема для IoT-пристроїв створено окремі захищені SSID, що також прив’язуються до відповідних VLAN. Це гарантує захищену передачу даних у бездротовому середовищі. Щоб посилити безпеку, застосовані правила контролю доступу, серед яких обмеження взаємодії пристроїв за IP-адресами, фільтрація MAC-адрес на Wi-Fi точках доступу, а також активовано механізми port security на комутаторах, що дозволяють підключення лише певних пристроїв до фізичних портів. Нарешті, загальні рекомендації включають регулярну зміну паролів, обмеження адміністрування лише з певних IP-адрес, увімкнення централізованого журналювання подій та своєчасне оновлення прошивок мережевого обладнання. Для бездротових мереж також рекомендовано активувати ізоляцію клієнтів, щоб пристрої одного SSID не мали можливості взаємодіяти між собою без необхідності.

Після впровадження базових налаштувань, що забезпечують сегментацію мережі, контроль доступу та шифрування даних, наступним важливим кроком стало гармонійне поєднання розробленої системи захисту з уже наявною інфраструктурою підприємства. Це дозволяє не лише зберегти цілісність і

стабільність мережі, а й максимально ефективно використовувати наявні ресурси, підвищуючи загальний рівень безпеки.

Першим кроком буде необхідне поєднання нового обладнання із наявними пристроями:

– підключення IoT-сегменту через VLAN, до спроєктованих VLAN для IoT-пристроїв, як реалізуються на мережевих комутаторах та маршрутизаторах та вже функціонують у мережі;

– підключення IoT-пристроїв, які отримають IP-адреси в межах виділеного підмережевого діапазону VLAN IoT;

– інтеграція із централізованим сервером журналювання та з іншими критичними сервери що розміщені у виділеному VLAN управління, з доступом, що контролюється ACL.

Другим кроком буде налаштування взаємодії з корпоративними політиками безпеки. Всі нові пристрої та обладнання повинні підтримувати централізовану автентифікацію (наприклад, через RADIUS або LDAP [40]) для відповідності корпоративним вимогам безпеки. Для Wi-Fi точок доступу налаштовується WPA2-Enterprise або WPA3-Enterprise із автентифікацією через корпоративний сервер, що забезпечує безпечний доступ до мережі. Також потрібно впровадження політик сегментації і контролю доступу. Існуючі політики контролю доступу розширюються на нові VLAN із IoT, де встановлюються чіткі правила взаємодії з IoT-пристроями. ACL на маршрутизаторах і комутаторах конфігуруються відповідно до цих правил для запобігання несанкціонованому доступу. Наступним пунктом буде журналювання та моніторинг. Система централізованого журналювання інтегрується з корпоративними SIEM-системами, що дозволяє моніторити події у реальному часі та своєчасно реагувати на потенційні інциденти. Логи IoT-пристроїв і мережевого обладнання передаються на центральний сервер із суворо обмеженим доступом. І останнє що залишається це політики оновлень і патчів. Усі мережеві пристрої, а також IoT-пристрої, підпорядковуються корпоративній політиці оновлення програмного

забезпечення для усунення вразливостей. Розгортання оновлень здійснюється централізовано з метою збереження стабільності та безпеки мережі.

Третім, не менш важливим етапом буде тестування та поступове впровадження. Нові компоненти системи захисту інтегруються поетапно із проведенням тестування сумісності, працездатності та безпеки. Для швидкого відновлення у разі непередбачених проблем виконується резервне копіювання конфігурацій та регулярні перевірки. Паралельно організовується навчання персоналу щодо нових процедур безпеки.

Отже слід підкреслити, що виконані кроки з налаштування мережевих компонентів системи захисту, починаючи від створення VLAN та впровадження правил контролю доступу до інтеграції з існуючою інфраструктурою забезпечують надійний рівень безпеки та ізоляції IoT-пристроїв у мережі приватного ІТ-підприємства. Це дозволяє мінімізувати ризики несанкціонованого доступу та розповсюдження атак, а також підтримувати стабільну і керовану роботу всієї мережевої інфраструктури. Важливість цих заходів полягає у створенні фундаменту для подальшого розвитку системи захисту, який відповідає вимогам кібербезпеки в офісному середовищі. Далі у роботі буде розглянуто рекомендації щодо організаційної структуризації, зокрема визначення відповідальних осіб і ролей, що є ключовим для ефективного функціонування системи захисту в цілому.

3.2 Рекомендації щодо організаційної структуризації

Організаційна структура системи захисту інформації — це важлива складова загального підходу до безпеки сучасних інформаційних систем, зокрема інфраструктури Інтернету речей на підприємстві. Хоча технічні заходи, такі як сегментація мережі, налаштування правил доступу чи централізоване журналювання, відіграють ключову роль, їхня ефективність значною мірою залежить від чіткого розподілу обов’язків і відповідальностей серед працівників.

Для IoT-інфраструктури, яка об’єднує різні пристрої, сервери, мережеве обладнання та користувачів, організаційна структура допомагає координувати дії з безпеки, оперативно виявляти й реагувати на інциденти, а також підтримувати постійний контроль за дотриманням внутрішніх політик. Саме завдяки правильному розподілу ролей технічні рішення працюють ефективно, а ризики несанкціонованого доступу чи внутрішніх загроз суттєво знижуються.

Наразі організаційна структура системи захисту інформації на підприємстві сформована недостатньо й не забезпечує ефективного управління безпекою IoT-інфраструктури. Відсутність чітко визначених відповідальних осіб за інформаційну безпеку значно послаблює загальний рівень захисту, створюючи суттєві ризики несанкціонованого доступу, внутрішніх загроз і технічних помилок.

Безпекові функції виконуються розпорошено і без системного підходу, часто покладаючись на ІТ-персонал, який не має спеціалізованої підготовки з кібербезпеки. Через це контроль доступу, моніторинг інцидентів та впровадження профілактичних заходів відбуваються нерегулярно та без чіткої організації. Основні проблеми полягають у наступному:

– відсутність відповідальної особи або групи, що унеможливлює централізоване управління ризиками;

– нечіткий розподіл обов’язків серед співробітників, що призводить до дублювання або ігнорування важливих завдань із захисту;

– відсутність формалізованих політик безпеки та процедур реагування на інциденти;

– недостатній рівень знань і навичок у працівників щодо безпечного користування IoT-пристроями та мережевими ресурсами.

Впровадження дієвої системи захисту інформації неможливе без чіткого розподілу посадових ролей та відповідальностей серед працівників. Важливою фігурою в цій структурі є особа, відповідальна за інформаційну безпеку, яка може виконувати роль функції керівника з питань інформаційної безпеки. Завдання цієї особи полягає в координації всіх заходів, спрямованих на забезпечення безпеки

інформації в організації. Вона відповідає за розробку й впровадження політик безпеки, що враховують особливості IoT-інфраструктури підприємства, а також контролює їх дотримання. Крім того, відповідальний за безпеку підтримує зв'язок із керівництвом підприємства, інформуючи про стан захисту та ризики, а також взаємодіє з зовнішніми організаціями, зокрема правоохоронними та спеціалізованими кібербезпековими службами. Це забезпечує оперативне реагування на інциденти та координацію дій у разі загроз. В умовах невеликого офісу, на 10–12 осіб, створення численних спеціалізованих посад з управління безпекою є недоцільним. Тому функції захисту інформації зазвичай поєднуються і розподіляються між кількома співробітниками. Серед ключових ролей варто виділити:

– адміністратор мережі та обладнання, який відповідає за налаштування і підтримку мережевих пристроїв: маршрутизаторів, комутаторів, точок доступу Wi-Fi, та здійснює базове адміністрування IoT-пристроїв, реалізує сегментацію мережі, налаштовує правила доступу і контролює фізичний доступ до обладнання;

– користувачі системи, тобто співробітники офісу, які є кінцевими користувачами IoT-пристроїв і корпоративної мережі. Їхня обізнаність і дотримання правил безпеки відіграють важливу роль у загальному захисті, тому необхідне регулярне навчання і проведення інструктажів;

– відповідальний за резервне копіювання та відновлення даних, роль якого в невеликому колективі може поєднуватися з адміністратором або відповідальним за безпеку. Ця особа відповідає за регулярне створення резервних копій важливої інформації і налаштувань, а також за відновлення систем після інцидентів.

Отже, у невеликій організації функції захисту інформації зосереджуються у кількох ключових співробітниках, що дозволяє ефективно управляти безпекою без зайвої бюрократії. Такий підхід забезпечує швидке реагування на інциденти, контроль дотримання політик безпеки та надійний захист IoT-інфраструктури підприємства.

Далі, не менш важливою складовою захищеної системи, є чітко визначений розподіл відповідальностей і повноважень серед співробітників, які беруть участь у побудові та підтримці системи інформаційної безпеки. Від того, наскільки чітко розмежовані зони відповідальності, а також права доступу й обов'язки кожного учасника, залежить ефективність реалізації заходів безпеки. Це дозволяє уникнути плутанини у виконанні завдань, знизити ризик виникнення помилок та забезпечити швидку реакцію на потенційні інциденти.

Перш за все, ключовою фігурою в системі захисту є відповідальний за інформаційну безпеку, якого часто називають CISO. Ця особа керує всіма процесами безпеки на підприємстві: вона розробляє і оновлює політики захисту інформації, стежить за дотриманням вимог нормативних документів, координує дії команди у разі виникнення загроз, а також організовує навчання співробітників з питань безпеки. CISO має розширені повноваження, включаючи адміністративний доступ до систем моніторингу, журналів подій і політик безпеки, що дозволяє йому контролювати стан захисту у будь-який момент.

Не менш важливу роль відіграє адміністратор мережі та обладнання. Його завданням є налаштування і підтримка всієї мережевої інфраструктури, що забезпечує роботу IoT-пристроїв, маршрутизаторів, комутаторів і точок доступу Wi-Fi. Ця людина відповідає за впровадження таких важливих технічних засобів захисту, як сегментація мережі за допомогою VLAN, налаштування правил контролю доступу, а також за фізичний захист обладнання. Адміністратор має обмежені адміністративні права, які дозволяють йому управляти мережею, але не втручатися в політики безпеки без погодження з керівництвом.

Крім того, окрему увагу потрібно приділити особі, відповідальній за резервне копіювання та відновлення даних. Вона контролює регулярне створення резервних копій налаштувань мережі, інформації з серверів і IoT-пристроїв, а також організовує процес відновлення даних у разі втрати або пошкодження. Важливо, щоб копії зберігались у захищеному середовищі, а процедури відновлення регулярно тестувалися. Особа, що виконує ці функції, має доступ

лише до систем резервного копіювання і певних важливих даних, не порушуючи загальну політику безпеки.

Нарешті, до системи захисту належать усі користувачі офісу, які безпосередньо працюють з IoT-пристроями та іншими IT-системами. Від них очікується дотримання встановлених правил безпеки, виконання рекомендацій, а також оперативне повідомлення про підозрілі або нестандартні ситуації. Для того, щоб забезпечити належний рівень обізнаності, користувачів регулярно навчають і контролюють дотримання внутрішніх інструкцій.

Щоб система захисту була дієвою, посадові інструкції для кожної ролі повинні бути постійно актуальними. Вони мають регулярно переглядатися та оновлюватися у відповідь на зміни у нормативній базі, технологічні нововведення або виникнення нових загроз. Внесення змін до документів рекомендується здійснювати за участю керівництва та фахівців з безпеки. Нові співробітники мають ознайомлюватися з актуальними інструкціями ще на етапі працевлаштування, що сприяє формуванню культури безпеки в колективі. Всі зміни слід документувати, щоб забезпечити прозорість і можливість аудиту. Таким чином, грамотний розподіл обов'язків і прав у системі захисту інформації формує організовану і злагоджену роботу всіх учасників процесу, мінімізує ризики людських помилок і забезпечує надійний захист IoT-інфраструктури підприємства.

Забезпечення захисту Інтернету речей підприємства приватної IT-компанії, вимагає не лише технічних засобів, а й впровадження чітко структурованих організаційних заходів і політик, що регулюють правила взаємодії персоналу з системами, реагування на загрози та підтримку належного рівня інформаційної безпеки. У середовищі малого офісу, де ресурси обмежені, особливо важливо мати зрозумілу, раціонально побудовану систему організаційного управління безпекою, яка буде не перевантаженою, але достатньо ефективною.

Одним із ключових кроків є створення внутрішніх нормативних документів, що встановлюють політику інформаційної безпеки. Така політика має містити загальні принципи захисту інформації, описати модель загроз, що актуальні для

підприємства, а також окреслити відповідальність працівників за дотримання вимог безпеки. Зокрема, має бути визначено, які пристрої дозволено підключати до корпоративної мережі, яким чином здійснюється автентифікація, хто відповідає за конфігурування мережі та які дії заборонено в контексті роботи з IoT-інфраструктурою. Окремий розділ політики повинен бути присвячений регламенту роботи з IoT-пристроями, у якому зазначаються правила підключення, періодичність оновлення прошивок, вимоги до паролів та порядок поводження з підозрілими сигналами з боку обладнання.

Надзвичайно важливим організаційним елементом є впровадження чітко визначеної процедури реагування на інциденти. У політиці необхідно описати, що саме вважається інцидентом безпеки (наприклад, несанкціоноване підключення до Wi-Fi мережі, виявлення невідомого пристрою, зміна конфігурації роутера без дозволу), а також визначити дії, які має вчинити персонал у разі його виявлення. Для малих підприємств важливо, щоб ці дії були простими, чіткими й не вимагали глибоких технічних знань. Наприклад, користувач має повідомити призначеного відповідального за безпеку, зафіксувати обставини та уникати будь-яких самостійних дій, що можуть погіршити ситуацію.

Окрему увагу слід приділити організації процедур моніторингу, звітності та аудиту. Навіть у малій мережі доцільно впровадити періодичну перевірку журналів подій, стану мережевого трафіку та статусу підключених пристроїв. Хоча ця задача може бути покладена на одну людину, вона повинна здійснювати її регулярно, наприклад, щотижня або після кожної зміни конфігурації. Необхідно також вести простий облік підключень: хто і коли підключав новий пристрій, з якою метою та на який VLAN він був спрямований. Ця звітність може вестися у формі електронної таблиці або журналу, доступ до якого має лише відповідальна особа.

Ще одним важливим компонентом є процедура оновлення системи захисту. Вона включає не лише оновлення прошивок IoT-пристроїв, маршрутизаторів і комутаторів, а й перегляд політик безпеки, налаштувань мережі, паролів і списків доступу. В умовах офісу з обмеженим персоналом доцільно проводити таке

оновлення раз на квартал або частіше, у разі виявлення нових загроз. Необхідно також зафіксувати, хто відповідальний за виконання цих дій, і як саме фіксується факт оновлення: наприклад, створюється короткий технічний звіт або запис у внутрішньому журналі.

Важливою частиною організаційної політики є також підготовка персоналу. Навіть якщо підприємство невелике, працівники повинні розуміти базові принципи безпечної роботи з IT-системами: не підключати сторонні пристрої до офісної Wi-Fi-мережі, уникати використання ненадійних додатків для керування IoT-пристроями, дотримуватись правил автентифікації. Проведення коротких інструктажів, розсилання простих пам’яток та демонстрація типових загроз, це дозволяє підвищити обізнаність персоналу та зменшити ризики, пов’язані з людським фактором.

Загалом, організаційні заходи є тією невидимою основою, яка дозволяє технічним рішенням працювати ефективно. Без встановлених правил, відповідальностей і процедур навіть найсучасніші технології не гарантують захищеності. Тому створення й підтримка внутрішньої документації, чітких регламентів і належної культури безпеки мають стати пріоритетом для будь-якого підприємства, навіть з невеликою кількістю персоналу.

Також потрібно приділити увагу для забезпечення відповідності внутрішніх організаційних і управлінських рішень чинним нормативно-правовим актам України. Це не тільки знижує ризики юридичної відповідальності, але й дозволяє впроваджувати систему захисту в уніфікованому, зрозумілому й контрольованому форматі. Варто зазначити, що, згідно із Законом України «Про основні засади забезпечення кібербезпеки України» та низкою супутніх нормативних документів, організація будь-якого підприємства, що здійснює обробку, зберігання або передавання електронної інформації, зобов’язана забезпечити належний рівень інформаційної безпеки відповідно до встановлених критеріїв ризику. Хоча більшість вимог стосуються об'єктів критичної інформаційної інфраструктури, навіть невелике приватне підприємство, яке експлуатує внутрішню комп’ютерну мережу з IoT-пристроями, повинно враховувати базові

положення цих законодавчих актів. Одним із ключових напрямів законодавчого регулювання є вимога до визначення відповідальних осіб за організацію та підтримку інформаційної безпеки. Закон України «Про інформацію» у ст. 15 вимагає встановлення процедур доступу до інформаційних ресурсів, зокрема визначення осіб, уповноважених на виконання функцій адміністрування, захисту та контролю інформації. У практичному плані це означає, що в межах навіть невеликого офісу має бути призначена особа (навіть на суміщенні посад), відповідальна за дотримання вимог безпеки, контроль за збереженням конфіденційності, цілісності та доступності даних, а також за координацію дій у разі кіберінцидентів. Особливу увагу слід звернути на рекомендації Державної служби спеціального зв'язку та захисту інформації України, які містяться в офіційних методичних матеріалах та нормативних документах [41]. Незважаючи на те, що наша організація не підпадає під визначення критичної інфраструктури, основні принципи, викладені в документі, можуть бути застосовані на адаптованому рівні. Наприклад, рекомендації щодо сегментації мережі, створення політик доступу, журналювання подій, захисту шлюзів і використання антивірусного захисту можуть бути реалізовані в обсягах, що відповідають ресурсам малого підприємства. Важливо також враховувати загальні підходи до побудови організаційної структури в галузі інформаційної безпеки [42], що б зазначити необхідність формалізації політик безпеки, впровадження безперервного циклу вдосконалення заходів захисту, а також проведення навчання персоналу. Всі ці вимоги частково або повністю враховано в нашій структурі, з урахуванням масштабів та специфіки діяльності підприємства.

Отже, підсумовуючи, успішне впровадження організаційної структури системи захисту інформації потребує поетапного, добре спланованого підходу, який поєднує призначення відповідальних осіб, проведення навчання та формування елементів внутрішнього контролю. Першим і ключовим кроком має стати офіційне закріплення відповідальності за інформаційну безпеку за конкретною особою. У нашому випадку це може бути один із співробітників технічного відділу, який вже має базові навички в роботі з мережею та розуміння

архітектури IoT-сегменту. В межах малого офісу призначення окремого CISO є малореалістичним, однак навіть часткове делегування обов'язків у цій сфері дозволяє закласти основу системної відповідальності. Одразу після призначення відповідального необхідно сформувати перелік його функціональних обов'язків: від підтримки технічних політик доступу до координації реагування на інциденти. Щоб ці обов'язки не залишалися формальністю, важливо провести початкове навчання, навіть у вигляді внутрішнього тренінгу або консультації з фахівцями, що вже мають досвід у сфері безпеки IoT. У випадку потреби можна використати доступні онлайн-курси з тематики IoT Security, розробки політик безпеки або основного управління ризиками. Навчання повинно стосуватись не лише технічного персоналу. Базові правила поводження з пристроями, принципи розмежування доступу та поведінки у разі виявлення підозрілих дій слід донести і до всіх інших співробітників офісу. Особливо це важливо в контексті захисту від людських помилок, соціальної інженерії та фішингу. Практика проведення коротких інструктажів або розсилки інформаційних бюлетенів може виявитися ефективною навіть за мінімальних ресурсів.

На завершальному етапі доцільно впровадити систему внутрішнього контролю, яка не вимагатиме значних інвестицій, але дозволить регулярно перевіряти, як дотримуються встановлені правила безпеки. Наприклад, відповідальний за ІБ може раз на місяць проводити огляд журналів доступу до IoT-пристроїв, перевірку оновлень на маршрутизаторах і точках доступу або здійснювати аудит підключених до мережі пристроїв. Також варто передбачити механізм документування цих перевірок, хоча б у вигляді простого внутрішнього протоколу, що зберігається локально або на сервері.

Таким чином, поетапне впровадження відповідальних осіб, супровідне навчання персоналу та регулярний внутрішній контроль формують організаційне підґрунтя системи безпеки. У поєднанні з технічними засобами захисту, описаними в попередніх підрозділах, ці заходи дозволяють суттєво знизити ризики несанкціонованого доступу до IoT-інфраструктури приватного IT-підприємства.

3.3 Тестування впровадженої системи захисту пристроїв IoT

З метою перевірки ефективності впровадженої системи захисту пристроїв Інтернету речей було змодельовано типову ситуацію, за якої порушник намагається отримати несанкціонований доступ до IoT-пристроїв зсередини підприємства. Уявімо, що один зі співробітників, який має фізичний доступ до приміщення офісу, вирішує навмисно або з цікавості перевірити, чи може він підключитися до мережі пристроїв автоматизації, наприклад, до IP-камери або до розумного термостата, підключеного до корпоративної IoT-мережі. Порушник має ноутбук із LAN-інтерфейсом, який він підключає до доступного Ethernet-порту, налаштованого для користувацької VLAN. У звичайних умовах це не дає йому доступу до пристроїв, які ізольовані у VLAN 20. Проте порушник свідомо змінює налаштування на своєму пристрої, імітуючи інший рівень доступу. Він запускає утиліту командного рядка на своєму ноутбуці, відкриває консоль і виконує перевірку зв'язності з потенційними IP-адресами IoT-пристроїв. Наприклад: ping 192.168.20.10. IP-адреса 192.168.20.10 належить одному з IoT-пристроїв, зокрема IP-камері, що знаходиться у VLAN 20. Оскільки комутатор і маршрутизатор налаштовані коректно, ping не проходить.

Зловмисник підозрює, що IoT-пристрої ізольовані в іншій VLAN, тому намагається вручну змінити свою VLAN або зімітувати підключення до іншого порту. Для цього змінює MAC-адресу мережевого інтерфейсу, тобто спроба обійти Port Security, використовуючи наступну команду: sudo ip link set dev eth0 address 00:11:22:33:44:55. Як тільки порт комутатора виявляє нову MAC-адресу, яка не входить до білого списку, Port Security блокує порт, на якому відбулася підозріла активність. В результаті інтерфейс мережі на ноутбуці зловмисника відключається, і далі передавати пакети через нього вже неможливо.

Далі він намагається змінити свою IP-адресу вручну на діапазон IoT-пристроїв: sudo ip addr add 192.168.20.50/24 dev eth0. Навіть попри ручне призначення IP-адреси зловмисником, маршрутизатор не пропускає трафік з VLAN 10 (робоча мережа) до VLAN 20 (IoT-сегмент). Спроба комунікації з IoT-

пристроями буде заблокована, через налаштовані списки контролю доступу, які дозволяють трафік лише від авторизованих джерел.

Повторно перевіряє зв'язність: ping 192.168.20.10. Як наслідок, ICMP-пакети не доходять до призначення, і порушник отримує повідомлення про недоступність хоста. Адже ми налаштувати списки котролю доступу на маршрутизаторі, що б блокували ICMP-трафік між VLAN-ами, за винятком дозволених службових адрес. Спроба отримати доступ до веб-інтерфейсу камери (HTTP або HTTPS), наприклад, через браузер за адресою http://192.168.20.10 за допомогою команди telnet 192.168.20.10 80. Жодна зі спроб не дає результату. Підключення через браузер або Telnet не встановлюється, на маршрутизаторі заборонений трафік на порт 80 і 23 (HTTP, Telnet) з невідомих адрес. У політиці доступу вказані лише конкретні IP-адреси, яким дозволено управляти IoT-пристроями (наприклад, адміністраторський ПК у VLAN 30).

3.4 Висновок

У цьому розділі було розглянуто практичні аспекти впровадження проєктованої системи захисту інформаційної інфраструктури Інтернету речей на приватному IT-підприємстві. Зокрема, було розроблено детальні настанови щодо впровадження мережевої компоненти захисту, починаючи від вибору обладнання до конкретних налаштувань сегментації, контролю доступу та взаємодії між виділеними сегментами. Реалізовані технічні рішення дозволили ізолювати критичні IoT-пристрої від основної мережі, забезпечити контроль над підключеннями та захистити канали взаємодії.

Окрім технічної частини, особливу увагу приділено організаційній складовій захисту. Запропоновано створення внутрішніх регламентів, розподіл ролей та обов'язків між працівниками, а також визначення відповідальних осіб за інформаційну безпеку. Ці заходи ґрунтуються на чинних нормативно-правових

актах України у сфері кіберзахисту та спрямовані на зменшення впливу людського фактора.

Проведене тестування системи захисту шляхом моделювання внутрішньої атаки дало змогу на практиці перевірити ефективність впроваджених заходів. Результати засвідчили, що всі ключові компоненти системи: Port Security, ACL, VLAN-сегментація спрацювали коректно, не дозволивши зловмиснику отримати доступ до IoT-інфраструктури. Це підтверджує доцільність обраної архітектури захисту та її здатність протистояти реальним загрозам.

Загалом, впроваджена система демонструє цілісність та ефективність як на технічному, так і на організаційному рівні, а її тестування в умовах, наближених до реальних, підтверджує відповідність поставленим завданням.

ВИСНОВКИ

В результаті виконання дипломного проєкту мною було досліджено та проаналізовано предметну область захисту інформації в середовищі Інтернету речей, охарактеризовано об’єкт захисту, офісне приміщення приватного підприємства, в якому використовується IoT-інфраструктура, включно з фізичними та інформаційними компонентами. На основі отриманих результатів було побудовано модель загроз, модель порушника, а також розроблено комплексну систему захисту IoT-інфраструктури підприємства.

Предметом даної дипломної роботи є система захисту інформації в корпоративному середовищі, що активно впровадила інфраструктуру Інтернету речей, з урахуванням особливостей офісного функціонування підприємства. Метою проєкту було здійснити комплексний аналіз інформаційної структури, побудувати моделі загроз та порушників, після чого спроєктувати та реалізувати систему безпеки, яка б забезпечила захист основних активів і відповідала технічним і організаційним можливостям підприємства.

Мета дипломної роботи була досягнута повною мірою. У процесі проєктування були враховані ключові аспекти захисту IoT: сегментація мережі, обмеження доступу, моніторинг трафіку, безпечне підключення пристроїв, захист каналів зв’язку та взаємодії з хмарними сервісами.

У ході виконання роботи, було зібрано та систематизовано теоретичні матеріали щодо побудови систем захисту IoT-інфраструктур, особливостей їх функціонування, типових вразливостей і способів їх подолання. Також було вивчено сучасні нормативні вимоги до захисту інформації як на національному, так і на міжнародному рівнях, включаючи вимоги до критичної інфраструктури.

У процесі аналізу інформаційної моделі підприємства було виявлено основні інформаційні потоки та канали взаємодії між пристроями, співробітниками, серверами та зовнішніми хмарними службами. Це дозволило створити деталізовану модель загроз, адаптовану до специфіки IoT-середовища, а

також визначити можливі сценарії дій порушників з урахуванням їхніх можливостей, мотивації та доступу.

На основі результатів аналізу було спроєктовано практичну модель офісної IoT-інфраструктури в середовищі Cisco Packet Tracer із реалізацією сегментації мережі (VLAN), базового контролю доступу (ACL), ізоляції критичних пристроїв, та впровадженням базових рекомендацій щодо налаштування безпеки Wi-Fi і Bluetooth з'єднань. Було надано рекомендації щодо призначення відповідальних за інформаційну безпеку, навчання персоналу, розробки політик доступу та реагування на інциденти.

Розроблена система захисту відповідає поставленій задачі та враховує реальні технічні обмеження підприємства, забезпечуючи при цьому базову стійкість до найбільш актуальних загроз. Вона також створює основу для подальшого вдосконалення, з можливістю розширення системи моніторингу, підключення SIEM-рішень або застосування засобів поведінкового аналізу.

Таким чином, розроблена система є готовою до впровадження, а сам проєкт може слугувати основою для подальших досліджень і розвитку безпеки IoT на підприємствах малого та середнього бізнесу.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Історія виникнення Інтернету речей. Its internet of things. URL: https://itsinternetofthings.blogspot.com/p/blog-page_50.html. (дата звернення: 20.05.2025).

2. An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks. URL: https://ioactive.com/wp-content/uploads/pdfs/IOActive_HackingCitiesPaper_cyber-security_CesarCerrudo.pdf (дата звернення: 20.05.2025).

3. Що таке IoT простими словами? Atiko. URL: https://www.atiko.com.ua/articles-ua/chto-takoe-iot-prostymi-slovami/ (дата звернення: 20.05.2025).

4. Протоколи передачі даних в IoT: які існують та чим відрізняються. Kyivstar Business Hub. URL: https://hub.kyivstar.ua/articles/protokoli-peredachi-danih-v-io-t-yaki-isnuyut-ta-chim-vidriznyayutsya (дата звернення: 20.05.2025).

5. Загальні принципи функціонування MQTT. Технології Індустрії 4.0. URL: https://pupenasan.github.io/TI40/%D0%9B%D0%B5%D0%BA%D1%86/MQTT.html (дата звернення: 21.05.2025).

6. CoAP RFC 7252 Constrained Application Protocol. Coap. URL: https://coap.space/ (дата звернення: 24.05.2025).

7. MQTT Vs. HTTP for IoT. HiveMQ. URL: https://www.hivemq.com/blog/mqtt-vs-http-protocols-in-iot-iiot/ (дата звернення: 25.05.2025).

8. Види протоколів в RabbitMQ. Друкарня. URL: https://drukarnia.com.ua/articles/rabbitmq-protokoli-FfYEy (дата звернення: 25.05.2025).

9. Огляд технології LoRaWAN. Atiko. URL: https://www.atiko.com.ua/articles-ua/obzor-tekhnologii-lorawan-ua/ (дата звернення: 25.05.2025).

10. IoT для бізнесу. Київстар Бізнес. URL: https://kyivstar.ua/business/products/iot-for-business (дата звернення: 26.05.2025).

11. Securing IoT Devices and SecurelyConnecting the Dots Using REST API and Middleware. ResearchGate. URL: https://www.researchgate.net/publication/334763600_Securing_IoT_Devices_and_SecurelyConnecting_the_Dots_Using_REST_API_and_Middleware/citations (дата звернення: 26.05.2025).

12. Частина 1. Загрози у світі речей інтернету (Безпека інтернету речей). HuckYourMom. URL: https://hackyourmom.com/osvita/chastyna-1-zagrozy-u-sviti-rechej-internetu-bezpeka-internetu-rechej/ (дата звернення: 30.05.2025).

13. Шляхи підвищення конфіденційності в мережах інтернету речей.URL: https://mapiea.kntu.kr.ua/pdf/11(42)_I/7.pdf (дата звернення: 30.05.2025).

14. Про захист персональних даних. Закон України від 01.06.2010 №2297. Дата оновлення 12.02.2025. Офіційний Портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 31.05.2025)

15. Multi-factor Authenticationforthe Internet of Things. Open Journal System. URL: https://doisrpska.nub.rs/index.php/SNG/article/view/8934/8659 (дата звернення: 31.05.2025)

16. Security and energy-efficiency in the Internet of Things: Challenges and solutions. HAL. URL:https://hal.science/hal-04011817/document (дата звернення: 31.05.2025)

17. What is the Mirai Botnet?. CloudFlare. URL: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/ (дата звернення: 31.05.2025)

18. Нова кібератака на Україну: що таке вірус VPNFilter і як з ним боротися. ExpresoTV. URL: https://espreso.tv/article/2018/05/29/nova_kiberataka_na_ukrayinu_scho_take_virus_vpnfilter_i_yak_z_nym_borotysya (дата звернення: 01.06.2025)

19. New rapidly-growing IoT Botnet - REAPER. Trendmicro. URL: https://success.trendmicro.com/en-US/solution/KA-0008042 (дата звернення: 01.06.2025)

20. Feds Uncover a ‘Swiss Army Knife’ for Hacking Industrial Control Systems. Wired. URL: https://www.wired.com/story/pipedream-ics-malware/ (дата звернення: 01.06.2025).

21. Pipedream/Incontroller : ICS-specific malware attacks. HeadMind Partners. URL:https://www.headmind.com/en/pipedream-incontroller-ics-specific-malware-attacks/ (дата звернення: 01.06.2025).

22. ДСТУ ISO/IEC 30141:2019 Інтернет речей. Еталонна архітектура. Будстандарт, сервіс документів URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=83590 (дата звернення: 01.06.2025).

23. ДСТУ ISO/IEC 27032:2024 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки. Будстандарт, сервіс документів. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=112376 (дата звернення: 01.06.2025).

24. EEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control. IEE Standard Association. URL: https://standards.ieee.org/ieee/802.1X/7345/ (дата звернення: 02.06.2025).

25. IEEE 802.11i Overview. NIST Computer Security Resource Center | CSRC. URL: https://csrc.nist.rip/archive/wireless/S10_802.11i%20Overview-jw1.pdf (дата звернення: 02.06.2025).

26. NIST's Network-of-Things Model Builds Foundation to Help Define the Internet of Things. Computer Security Resource Center. URL: https://www.nist.gov/news-events/news/2016/07/nists-network-things-model-builds-foundation-help-define-internet-things (дата звернення: 02.06.2025).

27. Security and Privacy Controls for Information Systems and Organizations. NIST Computer Security Resource Center. URL: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final. (дата звернення: 02.06.2025).

28. NIST SP 800-82 Rev. 3. NIST Computer Security Resource Center. URL: https://csrc.nist.gov/pubs/sp/800/82/r3/ipd. (дата звернення: 02.06.2025).

29. Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks. NIST Computer Security Resource Center. URL: https://csrc.nist.gov/pubs/ir/8228/final. (дата звернення: 02.06.2025).

30. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 05.07.1997 №80-94. Дата оновлення 27.03.2025. Офіційний Портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 03.06.2025).

31. Про кібербезпеку. Закон України від 05.10.2017. Дата оновлення 27.03.2025. Офіційний Портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 04.06.2025).

32. Hue Motion sensor. Philips hue. URL: https://www.philips-hue.com/en-us/p/hue-motion-sensor/046677570972#feature (дата звернення: 04.06.2025).

33. Термостат настінний Nest Learning Thermostat Gen3, Американська версія. Neosmart. URL: https://neosmart.com.ua/umnoe-upravlenie-klimatom-uk/umnye-termostaty-uk/nastennye-termostaty-uk/termostat-nastennyy-nest-learning-thermostat-gen3-amerikanskaya-versiya-uk.html (дата звернення: 04.06.2025)

34. Кондиціонер Daikin FTXJ35AW /RXJ35A Wi-Fi. Daikin Ukraine. URL: https://daikin-ukraine.com/prodazha/konditsionery-bytovye/nastennye/daikin/ftxg-emura/daikin-ftxj35aw-rxj35a-wi-fi/ (дата звернення: 04.06.2025)

35. Автономний готельний замок ZKTeco AL40B. Fortez – система безпеки. URL: https://www.forter.com.ua/avtonomniy-gotelniy-zamok-zkteco-al40b/ (дата звернення: 04.06.2025)

36. IP камера Hikvision DS-2CD2143G0-I (2.8 мм). Hikvision. URL:https://hikvision.co.ua/ua/hikvision-ds-2cd2143g0-i-28-mm/ (дата звернення: 04.06.2025).

37. PfSense Cloud VPS. Unixhost. URL: https://unixhost.pro/uk/vps_pfsense (дата звернення: 04.06.2025). (дата звернення: 05.06.2025).

38. Cisco Systems: Cisco IoT Gateways. 1nce. URL: https://www.1nce.com/en-us/resources/iot-knowledge-base/iot-hardware/iot-gateways/cisco-systems-cisco-iot-gateways (дата звернення: 05.06.2025).

39. Ethernet кабель категорії: CAT3, CAT5e, CAT6, CAT6e, CAT6a, CAT7 та CAT7a. Electrica. URL: https://electrica.net.ua/blog/kategoriyi_internet_kabelyu_cat3_cat5e_cat6_cat6e_cat6a_cat7_ta_cat7a (дата звернення: 05.06.2025)

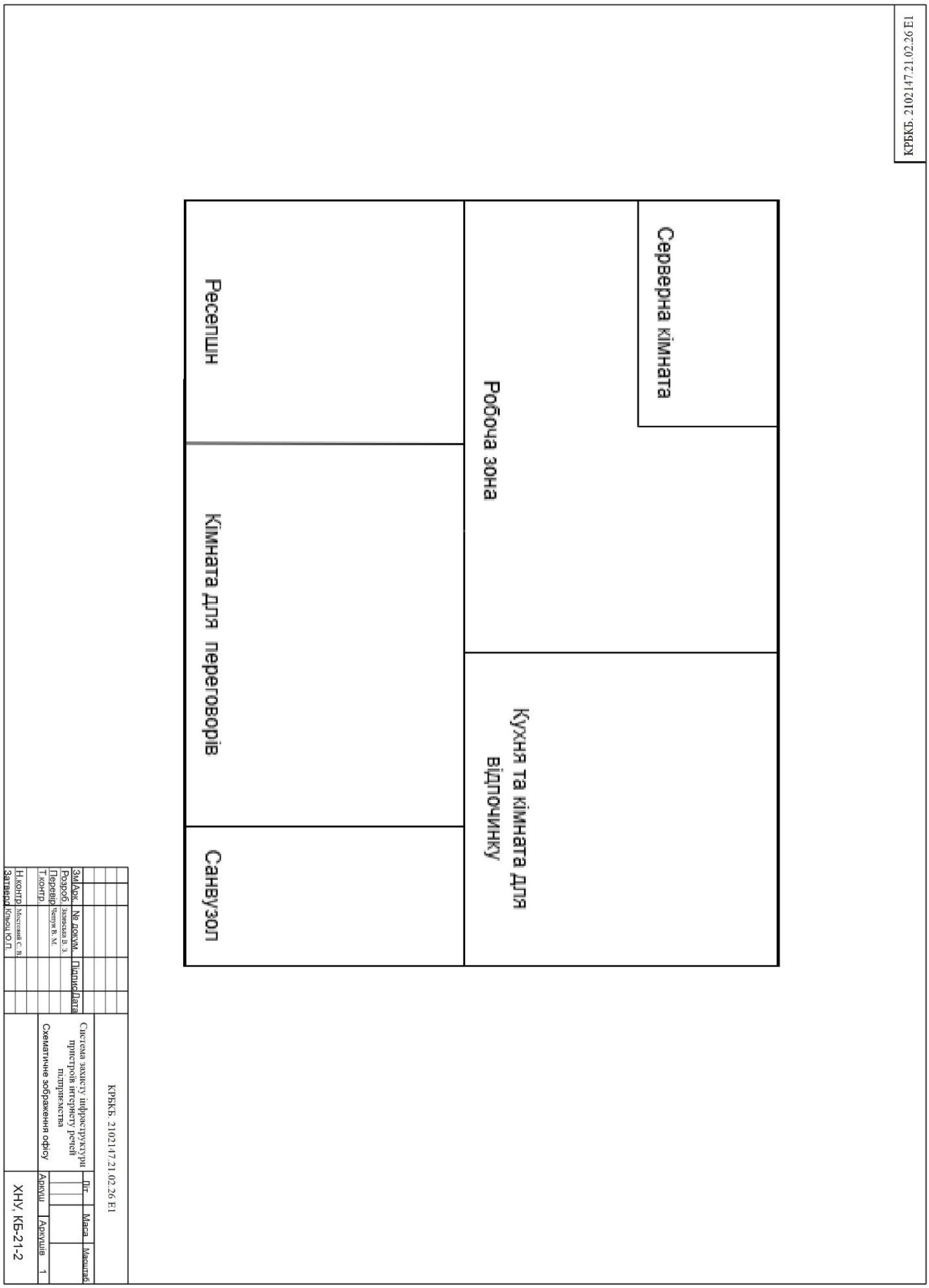
40. LDAP Vs. RADIUS. CloudRadius. URL: https://www.cloudradius.com/ldap-vs-radius-2/ (дата звернення: 05.06.2025)

41. Про затвердження Вимог до забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури. Постанова від 19.06.2019 №518. Офіційний Портал Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text (дата звернення: 05.06.2025)

42. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Будстандарт, сервіс документів. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=66910 (дата звернення: 05.06.2025)

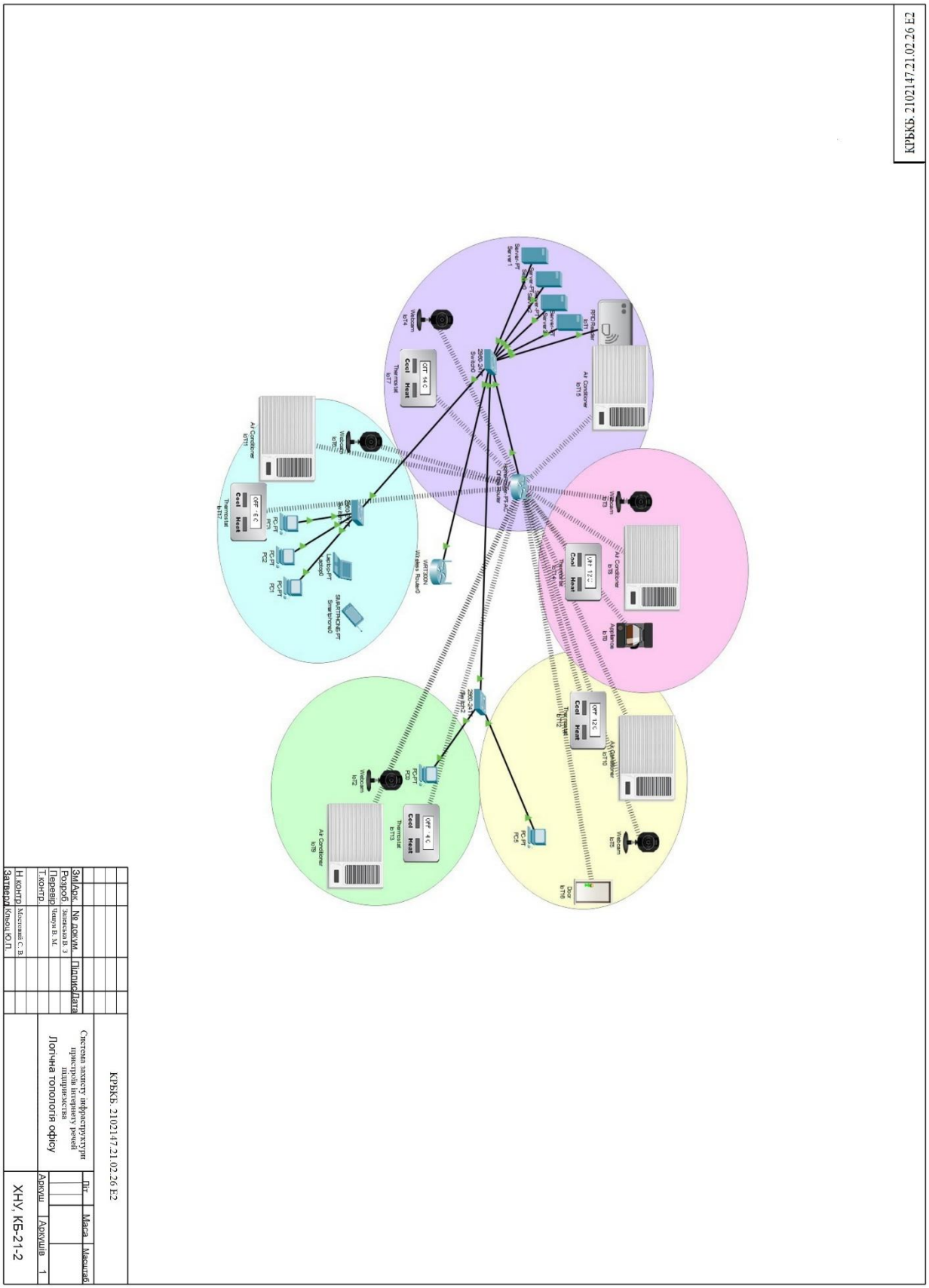
ДОДАТОК А

Схематичне зображення офісу



ДОДАТОК Б

Логічна топологія офісу



ДОДАТОК В

Модель загроз

№	Тип та визначення загрози	Джерело загрози	Ймовірність	Рівень шкоди	Наслідки		
					К	Ц	Д
1	2	3	4	5	6	7	8
Випадкові загрози техногенного походження							
1.	Пожежа або вибух	Середовище	Низька	Неприпустимо високий	-	+	+
2.	Відмова або збої пристроїв IoT	Апаратура	Висока	Високий	-	+	+
3.	Відмови, помилки програмного забезпечення	Програми	Висока	Високий	-	+	+
4.	Випадкові помилки працівників, помилкове конфігурування та адміністрування системи	Людина	Висока	Неприпустимо високий	+	+	+
5.	Ураження пристроїв вірусами та іншим шкідливим ПЗ	Людина, Програми	Середня	Середній	+	+	+
6.	Аварійна відмова електроживлення	Середовище, Апаратура	Середня	Високий	-	-	+
7.	Вихід з ладу сенсорів або виконавчих пристроїв	Апаратура	Висока	Середній	-	+	+
8.	Радіоперешкоди	Середовище	Низька	Низький	-	-	+
Навмисні загрози техногенного походження							
1.	Несанкціонований віддалений доступ	Людина (зовнішній зловмисник)	Висока	Неприпустимо високий	+	+	+
2.	Впровадження шкідливого програмного забезпечення	Людина (зовнішній зловмисник)	Висока	Високий	+	+	+
3.	Умисне пошкодження або перепрошивка пристроїв	Людина (зовнішній або внутрішній зловмисник)	Середня	Високий	-	+	+
4.	Атаки через підміну прошивки	Людина (зовнішній або внутрішній зловмисник)	Середня	Високий	+	+	+
5.	Атака на шлюзи або маршрутизатори	Людина (зовнішній зловмисник)	Висока	Неприпустимо високий	+	+	+
6.	Соціальна інженерія або фішинг	Людина (зовнішній або внутрішній зловмисник)	Висока	Високий	+	+	+
7.	Перехоплення та підміна даних з сенсорів	Людина (зовнішній зловмисник)	Високий	Середній	-	+	-
8.	Умисне перевантаження мережі (DDoS-атака)	Людина (зовнішній зловмисник)	Середня	Високий	-	-	+
9.	Цілеспрямоване видалення або пошкодження журналів подій	Людина (зовнішній або внутрішній зловмисник)	Середня	Високий	+	+	-

					КРБКБ. 2102147.21.02.26 Е3	
Зм.	Арк.	№ докум.	Підпис	Дата	Система захисту інфраструктури пристроїв інтернету речей підприємства	Літ. / Маса / Масштаб
Розроб.		Залевська В. З.			Модель загроз	
Перевір.		Чешун В. М.				Аркуш / Аркушів 1
Т.контр.						
Н.контр.		Мостовий С.В				ХНУ, КБ-21-2
Затверд.		Кльоц Ю.П.				

ДОДАТОК Г

Матриця ризиків та модель порушника

КРБКБ 2102147.21.02.26 Е4

Матриця ризиків

Імовірність \ Шкода	Низька	Середня	Висока	Неприпустимо висока
Низька	1	0	0	1
Середня	0	0	5	0
Висока	0	2	6	4

Модель порушника

№	Посада	Категорія порушника	Мотив порушника	Рівень обізнаності щодо ІОТ	Можливості щодо подолання системи	Можливості за часом дії	Можливості за місцем дії	Сума балів
1	Системний адміністратор	В4 (адміни безпеки)	М4	К4	Ч4	Ч4	Д5	24
2	Розробник	В3 (користувач АС)	М2	К3	Ч3	Ч3	Д4	19
3	Менеджер проєкту	В5 (керівництво)	М2	К1	Ч1	Ч3	Д3	14
4	Секретар	В3 (користувач АС)	М1	К1	Ч1	Ч3	Д3	13
5	Прибиральник	В1 (технічний персонал)	М1	К1	Ч1	Ч2	Д2	9
6	Гість	В6 (зовнішній)	М1	К1	Ч1	Ч2	Д1	7
7	Технічний керівник	В5 (керівництво)	М3	К4	Ч3	Ч4	Д4	22

Зм.	Арк.	№ докум.	Підпис	Дата
Розроб.		Заяковська В.З.		
Перевір.		Чапчук П.М.		
Т.контр.				
Н.контр.		Молотний С.В.		
Затверд.		Клюсь Ю.П.		

КРБКБ 2102147.21.02.26 Е4

Система захисту інфраструктури пристроїв інтернету речей підприємства

Матриця ризиків і модель порушника

Літ.	Маса	Масшт.
	Аркушів 1	

ХНУ, КБ-21-2

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Залевської Вікторії Закірівни
ПІБ здобувача вищої освіти

Студентки ФІТ, 4 курсу, групи КБ-21-2

ЗАЯВА

З правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 31.08.2023, згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлена. Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщена та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

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

05.06.25
дата

підпис

Anti-Plagiarism (UA) v-15.281 Educational

The maximum coincidence with one document 0.0%

Dictionaries check: en_US, ru_RU, ua_UA. **Errors in the documents: 9%**

ID: 244848 Title: Система захисту інфраструктури пристроїв інтернету речей підприємства Added in a DB: 2025-06-10 Authors: Залевська Вікторія Закірівна Heads: Чешун В.М. Consultants: Opponents:	Document		Sum coincidence on the DB	
	Symbols	Lexemes	Symbols	Lexemes
	118904	827	1101 (1%)	12 (1%)

Plagiarism sources

ID	Description	Plagiarism presence in the document	
		Symbols	Lexemes

Протокол аналізу звіту подібності науковим керівником

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

Автор: Залевська Вікторія Закірівна

Співавтор:

Назва: Система захисту інфраструктури пристроїв інтернету речей підприємства

Науковий керівник:

Підрозділ: Кафедра кібербезпеки

Коефіцієнт подібності 1:1.8%

Коефіцієнт подібності 2:0.1%

Мікропробіли: 0

Заміна букв: 0

Інтервали: 0

Білі знаки: 0

Дата створення звіту: 2025-06-11 05:15:26.0

Після аналізу Звіту подібності констатую наступне:

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

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

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

Обгрунтування:

11.06.2025р.

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Система захисту інфраструктури пристроїв інтернету речей підприємства

Автор: Залевська Вікторія Закірівна

Спеціальність: 125 – Кібербезпека

Освітня програма:Кібербезпека

Науковий керівник:Віктор ЧЕШУН, канд. техн. наук, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою StrikePlagiarism складає 98,2%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism складає 100%.

Згідно з правилами чинного Положення «Про систему забезпечення академічної доброчесності у Хмельницькому національному університеті» від 24.09.2024, авторська робота, обсяг оригінального тексту у відсотках до загального обсягу матеріалу в якій складає 90-100%, визначається роботою з високою унікальністю тексту і допускається до захисту.

Керівник роботи _____ Віктор ЧЕШУН

Гарант ОП _____ Віктор ЧЕШУН

Завідувач кафедри кібербезпеки _____ Юрій КЛЬОЦ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студентка Залевська Вікторія Закірівна

Тема Система захисту інфраструктури пристроїв інтернету речей підприємства

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 4; кількість сторінок записки 81.

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі, відповідно до поставленого завдання, проведене дослідження предметної області, проаналізовано законодавчу базу сфери захисту інформації та проведено обстеження об'єкта інформаційної діяльності. Також спроєктовано модель загроз та порушника та рекомендації щодо подальшого захисту. Налаштовано політики безпеки інфраструктури Інтернету речей підприємства.

2. Висновок про відповідність кваліфікаційної роботи завданню У кваліфікаційній роботі повністю виконано поставлене завдання як у теоретичній, так і в практичній частині

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У розділі 1 проаналізовано сучасні рішення у сфері захисту інформаційної інфраструктури Інтернету речей (IoT). Розглянуто актуальні стандарти кібербезпеки, включаючи IEC 62443, та нормативно-правові вимоги до захисту IoT. Особливу увагу приділено аналізу специфічних ризиків для IoT-пристроїв, каналів передачі даних і хмарних сервісів, а також розгляду інфраструктури підприємства, включаючи її структуру та існуючі вразливості. У розділі 2 розроблено концепцію системи захисту IoT-інфраструктури, включаючи ключові компоненти та механізми забезпечення безпеки. Створено формуляр IoT-пристроїв, модель загроз і порушника. Розроблено технічне завдання, план захисту інформації, а також налаштовано політики безпеки для пристроїв і мережевих елементів IoT. Проведено тестування криптографічних алгоритмів, налаштування захищених каналів зв'язку та інтеграцію систем моніторингу для виявлення загроз у реальному часі. У розділі 3 розглянуто основні етапи впровадження комплексної системи захисту IoT-інфраструктури. Детально описано процес налаштування систем безпеки, інтеграції IoT-пристроїв із корпоративними сервісами, а також впровадження антивірусного захисту і багаторівневого контролю доступу. Наведено рекомендації щодо експлуатації системи, включаючи регулярне оновлення політик безпеки, моніторинг мережі та навчання користувачів і адміністраторів. Запропоновані інструкції для ефективного управління IoT-системами та реагування на інциденти.

4. Позитивні сторони роботи Кваліфікаційна робота демонструє грунтовне розуміння специфіки захисту інформації в офісному середовищі, де використовується Інтернет речей. Було проведено комплексний аналіз нормативно-правової бази, сучасних загроз та методів захисту, що застосовуються до IoT-інфраструктур. Важливим аспектом є практична складова, яка включає моделювання захищеної мережевої архітектури з урахуванням особливостей корпоративної мережі. Робота відзначається системним підходом до аналізу інформаційних потоків, розробкою моделі порушника та вибором актуального обладнання для реалізації системи захисту. Використання інструменту

Cisco Packet Tracer забезпечує наочність проєктних рішень і підтверджує практичну цінність роботи.

5. Негативні сторони роботи У роботі недостатньо детально проаналізовано технічні характеристики IoT-пристроїв, що використовуються в інфраструктурі підприємства, зокрема їхні вразливості та вимоги до безпеки. Окремі розділи потребують кращої деталізації проєктних рішень щодо механізмів автентифікації, шифрування та контролю доступу. Крім того, в описі сценаріїв реагування на інциденти безпеки бракує конкретики щодо дій відповідального персоналу та процедур відновлення.

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення кваліфікаційної роботи відповідає темі роботи та виконане з дотриманням стандартів. В цілому, графічне оформлення є якісним, а пояснювальна записка відповідає нормам оформлення.

7. Відгук про роботу в цілому Кваліфікаційна робота заслуговує позитивної оцінки, оскільки демонструє системний та практично орієнтований підхід до вирішення завдань захисту інформації в середовищі з використанням Інтернету речей. Робота є структурованою, логічною та добре продуманою, що дозволяє читачу послідовно зануритись у всі етапи — від аналізу нормативної бази та моделі загроз до проєктування захищеної мережевої архітектури. Особливої уваги заслуговує практична частина, яка підтверджує реалістичність і доцільність прийнятих технічних рішень. Візуальні матеріали, зокрема модель мережі в Cisco Packet Tracer та план приміщення, наочно ілюструють результати розробки. Попри окремі недоліки, пов'язані з недостатньою деталізацією характеристик окремих IoT-пристроїв та технічних механізмів безпеки, робота в цілому справляє позитивне враження. Обраний підхід до моделювання, систематизація матеріалу та практична реалізація доводять високий рівень підготовки авторки та актуальність теми в сучасних умовах цифровізації підприємств.

8. Інші зауваження відсутні

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні сторони кваліфікаційної роботи, а також негативні сторони, які не зменшують практичну цінність отриманих результатів і загальну якість роботи, рекомендованою оцінкою є «добре»

РЕЦЕНЗЕНТ д.т.н., професор, зав. кафедри автоматизації комп'ютерно-інтегрованих технологій та робототехніки МАРТИНЮК Валерій Володимирович

« 13 » червня 2025. _____ (підпис)