Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки

МАГІСТЕРСЬКА КВАЛІФІКАЦІЙНА РОБОТА
на тему:
ЗАСОБИ ЗАХИСТУ INTERNET OF THINGS В КОРПОРАТИВНІЙ КОМП'ЮТЕРНІЙ МЕРЕЖІ

Виконав студент 2 курсу, групи 2КІ-22м
Спеціальності 123 – Комп'ютерна інженерія
Костюк О. В.
Керівник к.т.н., доц. каф. ОТ
Савицька Л. А.
"07" 12 2023 р.
Опонент к.ф-м.н., доц. каф. МБІС
Шиян А. А.
"08" 12 2023 р.

Допущено до захисту
Завідувач кафедри ОТ
д.т.н., проф. Азаров О.Д.

"11" 12 2023 р.

ВНТУ 2023

ВІННИЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки
Галузь знань — Інформаційні технології
Освітній рівень — магістр
Спеціальність — 123 Комп'ютерна інженерія
Освітньо-професійна програма — Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедри ОТ, д.т.н., проф.
_____ О.Д. Азаров
" 26 " вересня 2023 р.

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

студенту **Костюку Олегу Віталійовичу**

1. Тема роботи «Засоби захисту Internet of Things в корпоративній комп'ютерній мережі» керівник роботи Савицька Людмила Анатоліївна к.т.н., доцент, затверджено наказом вищого навчального закладу від **18.09.2023** року **№ 247**

2 Строк подання студентом роботи **10.12.2023**.

3 Вихідні дані до роботи: огляд ключових проблем та загроз безпеці пристроїв в корпоративних мережах IoT; вивчення методів та засобів захисту IoT-пристроїв у корпоративному середовищі; проведення перевірки та аналізу отриманих результатів; виконання економічних розрахунків для оцінки доцільності впровадження нової розробки.

4 Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): вступ, актуальний стан справ у сфері Internet of Things, технологічний дизайн системи IOT, організація мережі за 4-рівневим технологічним дизайном internet of things, економічна частина.

5 Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): технічне завдання, загальна схема мережі, конфігураційні файли ключових пристроїв.

6 Консультанти розділів роботи приведені в таблиці 1.

Таблиця 1— Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада Консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1-4	Савицька Людмила Анатоліївна, к.т.н., доцент		
5	Небава Микола Іванович, проф., к.е.н		

7 Дата видачі завдання **19.09.2023 р.**

8 Календарний план виконання МКР приведений в таблиці 2.

Таблиця 2 — Календарний план

№ з/п	Назва етапів МКР	Строк виконання	Підпис
1	Постановка задачі	**23.09.2023**	
2	Актуальний стан справ у сфері Internet of Things	**28.09.2023**	
3	Технологічний дизайн системи IOT	**10.10.2023**	
4	Організація мережі за 4-рівневим технологічним дизайном Internet of Things	**28.10.2023**	
5	Практична реалізація захисту за моделлю безпечного дизайну системи Internet of Things	**23.10.2023**	
6	Вибір ПЗ для моделювання	**27.10.2023**	
7	Моделювання роботи мережі	**03.11.2023**	
8	Розрахунок економічної частини	**11.11.2023**	
9	Оформлення пояснювальної записки та ілюстративного матеріалу	**20.11.2023**	
10	Виконання магістерської кваліфікаційної роботи	**01.12.2023**	
11	Перевірка якості виконання магістерської кваліфікаційної роботи та усунення недоліків	**04.12.2023**	
12	Підписи супроводжувальних документів у керівника, опонента, нормо контролера	**11.12.2023**	
13	Перевірка «антиплагіат»	**11.12.2023**	
14	Попередній захист	**22.11.2023**	

Студент Костюк Олег Віталійович

Керівник к.т.н., доц. Савицька Людмила Анатоліївна

АНОТАЦІЯ

УДК 004

Костюк Олег Віталійович, магістр кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки, oleg.kostuik14@gmail.com, Вінниця, Хмельницьке шосе, 95. Засоби захисту Internet of Things в корпоративній комп'ютерній мережі. Магістерська кваліфікаційна робота зі спеціальності 123 – Комп'ютерна інженерія, Вінниця: ВНТУ, 2023 – 89 с. На українській мові. Бібліографія: 27 назв; рис.: 30; таблиць: 7

Дана магістерська кваліфікаційна робота присвячена аналізу та вдосконаленню засобів захисту Internet Of Things в корпоративних комп'ютерних мережах. Складові технології Internet Of Things оперують різними типами даних, в тому числі і персональними відомостями, тож питання безпеки під час передавання такої інформації важливе. Основна увага приділяється розробці вдосконаленого технологічного дизайну системи Internet Of Things.

Дослідження ґрунтуються на аналітичній роботі із сучасними науковими літературними джерелами та інформаційними ресурсами різного походження від компаній, що надають послуги мережевого обладнання, налаштування подібних мереж та їх вивчення, наприклад, Cisco.

Ключові слова: Internet Of Things, інформаційна безпека, рівні стеку, безпековий технологічний дизайн системи IoT, модель безпечного дизайну системи Internet Of Things.

ANNOTATION

UDC 004

Kostiuk Oleh Vitaliyovych, magister of computing engineering department, Vinnytsya national technical university, department of the computer engineering, oleg.kostuik14@gmail.com, Vinnytsya, Khmelnytsk highway, 95. Internet of Things protection in the corporate computer network. Master's thesis on specialty 123 - Computer engineering, Vinnytsia: VNTU, 2023 - 89 p. In Ukrainian language. Bibliography: 26 titles; pic.: 30; tables: 7

This master's thesis is devoted to the analysis and improved protection of the Internet of Things in corporate computer networks. The component technologies of the Internet of Things work exclusively with data types, including personal information, so the issue of security during the transfer of such information is important. The main focus is on the development of an improved technological design of the Internet of Things system.

Research is based on analytical work with modern scientific literary sources and information resources of various origins from companies that provide network equipment services, configuration of similar networks and their study, for example, Cisco.

Key words: Internet of Things, information security, stack levels, secure technological design of the IoT system, model of secure design of the Internet Of Things system.

ЗМІСТ

ВСТУП

Актуальність теми дослідження слід розпочати з започаткування розвитку Internet of Things (IoT) та його використання у 2000-х роках. У цьому напрямку активно працюють численні відомі та інші компанії, такі як IBM, Intel, Google, Cisco, Microsoft, Amazon, і Siemens. [1-7]. Уже у період між 2018 і 2019 роками кількість пристроїв, які були підключені до мережі, вагомо перевищила населення Землі. Згідно з передбаченнями, до 2025 року кількість таких підключених пристроїв мала сягнути від 50 до 70 мільярдів одиниць. Це експоненційне зростання створює значні ризики для безпеки інформації, яка обробляється, передається та зберігається цими пристроями. Для запобігання цим ризикам необхідно дотримуватись вимог, включаючи ті, які встановлені Регламентом Європейського Парламенту і Ради ЄС 2016/679 від 27 квітня 2016 року щодо захисту особистих даних та вільного обігу таких даних, що відомий також як GDPR. [4, 8, 9]. Тому тема дослідження є актуальною.

Отже, потрібно провести аналіз та покращення захисту IoT в корпоративних комп’ютерних мережах. Основний акцент зроблено на розробці розширеного та вдосконаленого технологічного дизайну системи IoT.

Метою дослідження є підвищення безпеки та захисту пристроїв Internet Of Things всередині корпоративної комп’ютерної мережі від несанкціонованого доступу. Це досягається за допомогою вдосконаленого технологічного дизайну системи IoT.

Для досягнення поставленої в роботі мети необхідно виконати такі завдання:

— проаналізувати архітектуру і ключові компоненти екосистеми Internet Of Things та особливості роботи технології IoT з точки зору взаємодії, обробки даних та розподілу інформації в системах IoT;

— виконати аналіз загроз інформаційній безпеці IoT;

— спроектувати вдосконалений технологічний дизайн системи Internet Of Things;

— запропонувати розподіл загроз безпеці по рівням технологічного дизайну системи Internet Of Things;

— розробити модель безпечного дизайну системи Internet Of Things урахуванням 4-рівневого дизайну системи Internet Of Things;

— розробити модель корпоративної комп'ютерної мережі в програмному середовищі Packet Tracer з захистом у відповідності до запропонованого технологічного дизайну системи IoT.

Об'єктом дослідження є інформаційні процеси у відомому протокольному стеку TCP/IP та моделі відкритих систем Open Systems Interconnection, а також відомі технологічні безпекові процеси для Internet Of Things в корпоративних комп'ютерної мережах.

Предметом дослідження є методи та засоби захисту IoT в корпоративних комп'ютерних мережах.

Новизна дослідження полягає у такому:

— вдосконалена відома трирівнева модель системи Internet Of Things за рахунок приведення її до архітектури IoT від CISCO, що надає новій архітектурі подібність до принципів побудови сервіс-орієнтованої архітектури (SOA);

— розширено методологічну базу методів та засобів захисту IoT в межах корпоративної комп'ютерної мережі.

Практична цінність полягає у такому:

— розроблено прототип корпоративної комп'ютерної мережі в програмному середовищі Packet Tracer (від компанії CISCO), яка враховує безпекові аспекти запропонованого технологічного дизайну системи IoT.

Публікація та апробація полягає у розширенні методологічної бази методів та засобів захисту IoT в межах корпоративної комп'ютерної мережі, що може стати поштовхом для подальшого удосконалення процесів захисту

елементів IoT в корпоративній комп’ютерній мережі. Також, була опублікована стаття: «ЗАСОБИ ЗАХИСТУ INTERNET OF THINGS В КОРПОРАТИВНІЙ КОМП’ЮТЕРНІЙ МЕРЕЖІ / Савицька, Т.І. Коробейнікова, О.В. Костюк, І. С. Колесник // Інформаційні технології та комп`ютерна інженерія. – 2023. – № 2. – С. 61-70», у журналі ІТКИ.

1 АКТУАЛЬНИЙ СТАН СПРАВ У СФЕРІ INTERNET OF THINGS

У першому розділі магістерської кваліфікаційної роботи розглянемо сучасний стан питання в галузі Internet of Things.

Інтернет речей (або IoT, від англійської абревіатури Internet of Things) – це глобальна система, в якій різні фізичні пристрої, обладнані сенсорами, датчиками і засобами комунікації, підключені до Інтернету [10]. Ці цифрові пристрої можуть збирати інформацію з навколишнього середовища за допомогою своїх сенсорів, спілкуватися з іншими пристроями, обмінюватися даними та виконувати віддалений моніторинг стану різних об'єктів. Вони також можуть аналізувати зібрані дані та приймати рішення на основі цієї інформації. До прикладів таких інтелектуальних об'єднаних датчиків входять: розумні дверні дзвінки, гаражні ворота, термостати, пристрої для відстеження активності, медичні імпланти, світлофори, системи паркування та багато інших. Отже, фізичні об'єкти, які взаємодіють між собою або з навколишнім середовищем, передаючи дані через мережу, отримали назву Internet Of Things. [10].

1.1 Архітектура та ключові елементи системи IoT

Поняття Internet Of Things відображає глобальну систему взаємно підключених та зв'язаних пристроїв різного типу, що призначені для поліпшення процесу прийняття рішень різного характеру, заснованого на аналізі величезних обсягів даних, які накопичуються цими пристроями. Іншими словами, Internet Of Things – це мережа, в якій об'єкти і пристрої спілкуються між собою та надсилають дані для покращення різноманітних рішень.

Система Internet Of Things складається з багатьох компонентів і складових. До цього переліку входять пристрої виконання, сервіси і технології, які використовуються для оптимальної роботи цієї перспективної галузі. В цей

перелік включаються різні типи сенсорів, пристроїв для збору даних, засоби передавання інформації, хмарні обчислення, аналітичні інструменти та багато інших компонентів. Усі вони спільно працюють, щоб забезпечити надійну і ефективну роботу Internet Of Things та підтримувати вирішення різних завдань та завдань у різних галузях та сферах життя [11].

Перелічимо засоби, сервіси і технології.

Сенсори (розумні датчики/виконавчі механізми) це вбудовані системи, які мають операційні системи реального часу та використовуються для збору даних. Вони також обладнані джерелами безперебійного живлення і використовують мікро-електромеханічні системи (МЕМС).

Вбудовані системи зв'язку з датчиками, ці системи забезпечують зв'язок між датчиками. Зона охоплення бездротових персональних мереж може варіюватися від нульової відстані до 100 метрів. Для обміну даними між датчиками використовуються низькошвидкісні малопотужні інформаційні канали, які не завжди базуються на протоколі IP.

Локальні обчислювальні мережі (LAN), зазвичай це системи обміну даними на базі протоколу IP, такі як 802.11 Wi-Fi, що використовуються для швидкої бездротової радіозв'язку. Ці мережі можуть бути як піринговими (Peer-to-peer), так і зірковими.

Агрегатори, маршрутизатори, шлюзи (gateways), пограничні пристрої (Edge Device), ці пристрої служать постачальниками вбудованих систем і включають в себе різні компоненти, такі як процесори, динамічна оперативна пам'ять і системи зберігання даних. Вони також можуть бути виробниками модулів, пасивних компонентів, тонких клієнтів і радіосистем, а також надавати послуги з міжплатформного програмного забезпечення. У додаток до цього, вони відіграють роль у розробці інфраструктури туманних обчислень, надають інструментарій для граничної аналітики, забезпечують безпеку граничних пристроїв і управляють сертифікатами.

Глобальна обчислювальна мережа, в цю категорію входять оператори стільникового зв'язку, оператори супутникового зв'язку, і оператори малопотужних глобальних мереж (Low-Power Wide-Area Network, LPWAN). Для IoT зазвичай використовуються транспортні протоколи Інтернету, такі як MQTT, CoAP, і навіть HTTP.

Хмарна інфраструктура, це хмарні ресурси, які виступають в ролі постачальників різноманітних послуг і платформ для системи Internet Of Things. Вони також надають інфраструктуру для обробки потокових і пакетних даних, баз даних і аналізу даних. Крім того, хмарні постачальники надають інструменти для аналізу та розробки програмного забезпечення, а також сервіси машинного навчання.

Сервіси аналізу даних, величезні обсяги інформації передаються в хмару для проведення подальшого аналізу. Робота з великими даними і отримання конкретних результатів вимагають комплексної обробки даних та використання методів аналізу та машинного навчання.

Забезпечення безпеки, під час інтеграції всіх компонентів архітектури в єдину систему постає питання забезпечення кібербезпеки. Безпека є критичним аспектом на всіх рівнях, від фізичних датчиків до центральних обчислювальних систем, включаючи системи зв'язку та протоколи передавання даних. На кожному рівні необхідно гарантувати конфіденційність, доступність та цілісність даних. У цьому ланцюжку не може бути слабких точок, оскільки екосистема Internet Of Things стає об'єктом атак з боку хакерів у всьому світі.

Ця архітектура Internet Of Things об'єднує різноманітні компоненти та послуги, щоб забезпечити збір, обробку, зберігання та аналіз даних. Вона включає в себе різні типи пристроїв, мереж і сервісів і вимагає високого рівня безпеки для захисту інформації від потенційних загроз.

На рисунку 1.1 нижче представлено схематичне зображення архітектури Internet Of Things за версією компанії CISCO [10].

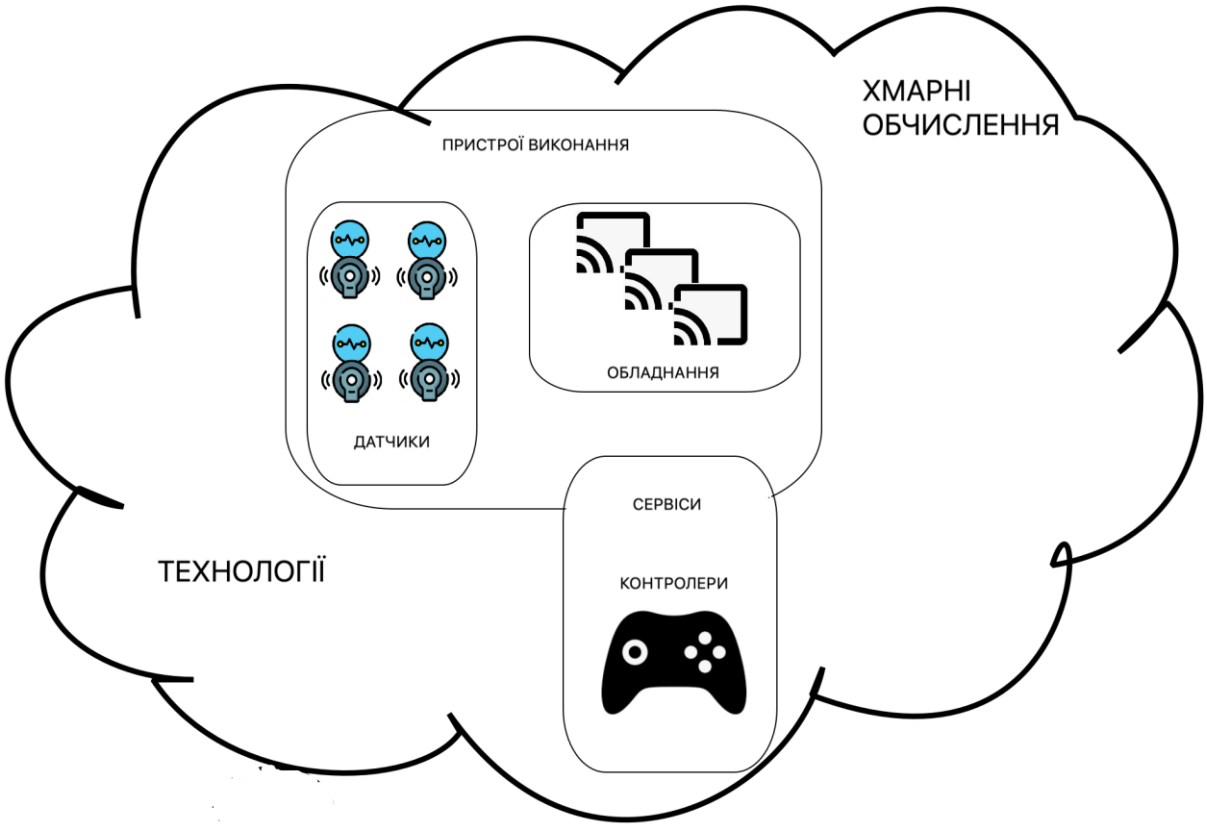


Рисунок 1.1 — Складові архітектури системи Internet Of Things

З різних поглядів компаній і спеціалізованих організацій архітектурна модель Internet Of Things може включати в себе різні рівні обслуговування та подання. Наприклад, Міжнародний союз електрозв'язку (МСЕ-Т) вивів 4-х рівневу модель архітектури IoT, тоді як Всесвітній форум IoT (IoT World Forum, IWF) розробив еталонну модель, яка складається з 7 рівнів [12,13,17]. Відмінність між цими моделями полягає в їхній конкретній реалізації. У загальних рисах вони нагадують архітектуру традиційних систем автоматизації управління технологічними процесами.

У таблиці 1.1, наведеній нижче, представлена одна з прикладних 3–рівневих моделей архітектури системи Internet Of Things, яка розглядає питання безпеки на кожному рівні та можливі варіанти їх вирішення. Наслідком цього є більш глибоке розуміння аспектів безпеки в контексті Internet Of Things [14].

Таблиця 1.1 — Складові трирівневої моделі системи Internet Of Things

РІВЕНЬ ВИКОНАВЧИХ ПРИСТРОЇВ	Безпека IoT	RFID-пристрої, бездротові сенсорні пристрої, GPS-пристрої
	Безпека мережі IoT	
ТРАНСПОРТНИЙ РІВЕНЬ	Доступ до мережі IoT	WIFI-мережі, Ad hoc-мережі
	WAN	Мобільний Інтернет, Інтернет
	LAN	Безпека локальної мережі
ПРИКЛАДНИЙ РІВЕНЬ	IoT Applications	Інформаційна логістика, інтелектуальна мережева безпека, моніторинг середовища
	IoT Application support	Безпека середовища розробки, платформи хмарних обчислень, поміжні технології безпеки

Як вже було відзначено в даній роботі, остаточний вигляд структури Internet Of Things залежить від багатьох факторів, включаючи потреби та особливості конкретного проекту і реальні можливості для їх впровадження. Розподіл функцій системи на її рівнях також є важливим аспектом, який потребує чіткості та розуміння.

Для поліпшення розподілу функцій автором пропонується розширений дизайн системи IoT (порівняно із див. Таблиця 1.1) з додатковим рівнем інтерфейсів, що надає новій архітектурі подібність до принципів побудови сервіс-орієнтованої архітектури (SOA). На рисунку 1.2 нижче наведено розширений дизайн системи IoT, що складається з 4 рівнів. Цей дизайн дозволяє краще розуміти та оптимізувати функціональний розподіл в контексті системи Internet Of Things.

<table>
<tr><th>3-LAYER MODEL</th><th>4-LAYER MODEL</th></tr>
<tr><td>Прикладний рівень</td><td>Службовий рівень</td></tr>
<tr><td>Транспортний рівень</td><td>Рівень корпоративної комп’ютерної мережі</td></tr>
<tr><td rowspan="2">Рівень виконавчих пристроїв</td><td>Рівень локальних інтерфейсів</td></tr>
<tr><td>Рівень датчиків</td></tr>
</table>

Рисунок 1.2 — Запропонований розширений технологічний дизайн системи IoT

Кожен з вказаних компонентів на цьому ілюстрації виконує свою конкретну функцію. Рівень датчиків займається збором даних. Рівень локальних інтерфейсів відповідає за забезпечення взаємодії між різними учасниками системи, рівень корпоративної комп’ютерної мережі відповідає за передачу даних, і службовий рівень дозволяє створювати та управляти різними сервісами.

Ця ілюстрація демонструє, що кожен з компонентів в мережі має свою важливу функцію. Рівень датчиків відповідає за збір великої кількості різноманітних даних, рівень локальних інтерфейсів виконує роль посередника, який дозволяє різним частинам системи спілкуватися та обмінюватися інформацією. Рівень корпоративної комп’ютерної мережі відповідає за ефективну передачу цих даних між різними пристроями та підсистемами. Нарешті, службовий рівень включає в себе можливості створення, налагодження та керування різними сервісами та функціоналом мережі.

Кожен із цих рівнів є важливою ланкою в цій складній системі, і їх спільна робота дозволяє Internet Of Things працювати ефективно та надійно.

1.2 Взаємодія, обробка даних та розподіл інформації в системах IoT

Один із ключових етапів у системі є належний процес інтеграції запланованих приладів для збору даних, таких як різноманітні датчики та сенсори з рештою мережі.

Підключення датчика до корпоративної комп’ютерної мережі є обов'язковим кроком, щоб забезпечити можливість зберігання та доступу до зібраних ним даних. Це може вимагати використання дротового Ethernet-з'єднання або бездротового з'єднання з контролером. Контролери відповідають за ефективний збір даних від датчиків та забезпечення наявності мережевого чи Інтернет-підключення. Крім того, ці пристрої можуть мати можливість для прийняття негайних рішень або надсилати дані на більш потужний комп'ютер для подальшого аналізу, незалежно від того, чи цей аналіз відбувається в межах локальної мережі чи в іншому місці.

Передавання даних та налагодження мережевого з'єднання в системах Internet Of Things базуються на системах зв'язку ближньої дії, відомих як персональні мережі (Personal Area Network, PAN) [12-13]. Зазвичай ці мережі не використовують правила IP-протоколу та можуть бути як бездротовими, так і дротовими.

До бездротових мереж та протоколів IoT відносяться Bluetooth, мережі типу "mesh", Zigbee та Z-Wave. До дротових мереж належать різноманітні промислові мережі та протоколи.

Крім PAN, активно використовуються бездротові локальні мережі та мережі на основі IP-протоколу, включаючи широкий спектр Wi-Fi-мереж на основі стандартів IEEE 802.11, 6LoWPAN і технології Thread [12-13]. Часто застосовуються також системи телекомунікацій на основі стільникових

стандартів (3G, 4G LTE) та нові стандарти, які сприяють роботі IoT, такі як Cat-1 і Cat-NB, а також протоколи LoRaWAN і Sigfox [10].

Датчики часто взаємодіють з виконавчими механізмами, які відповідають за фізичні дії на основі отриманих даних. Ці механізми перетворюють електричний струм, отриманий від датчика, на конкретні фізичні впливи. Наприклад, якщо датчик реєструє підвищену температуру в приміщенні, він надсилає цю інформацію мікроконтролеру. Мікроконтролер може використовувати ці дані для активації виконавчого механізму, який, наприклад, увімкне кондиціонер.

Багато сучасних пристроїв, таких як фітнес-трекери, кардіостимулятори, призначені для імплантації в тілі пацієнтів, лічильники повітря в шахтах та лічильники води в сільському господарстві, потребують бездротового з'єднання. Оскільки багато датчиків розташовані в віддалених місцях і живуть від акумуляторів або сонячних панелей, необхідно звертати увагу на ефективне використання енергії. Щоб оптимізувати роботу датчика і підвищити його доступність, слід використовувати рішення з низьким споживанням енергії. Таким чином, максимально ефективно використовувати ресурси.

Взаємодія з "речами" відбувається за допомогою датчиків, сенсорів та інших пристроїв для збору інформації, подібно до класичних систем управління для будь-якого об'єкта керування. Ці датчики об'єднуються разом з інфраструктурою для інтеграції з рівнем обробки подій через мережу Інтернет і формують так звану граничну область.

Події, які надходять із граничної області, зберігаються та обробляються відповідно до поставленої задачі (це відбувається на службовому рівні). На цьому рівні дані зберігаються, обробляються та перенаправляються потрібним додаткам. Дані обробляються за допомогою аналітичних сервісів і на їхній основі відбувається процес машинного навчання, що дозволяє робити певні висновки про об'єкт. Цей рівень, як правило, реалізований за допомогою

хмарних або туманних обчислень. Остаточні результати, контроль, віддалене керування та адміністрування системи проводяться за допомогою прикладних застосунків через Інтернет-з'єднання (рівень локальних інтерфейсів).

Важливо відзначити, що немає необхідності відправляти абсолютно всі дані, що генерують пристрої для збору інформації, у хмарний сервіс. Це може впливати на ефективність обробки даних і вартість. Для цього можна передбачити обробку на межі поточної мережі (граничні обчислення) або включити граничний маршрутизатор в сектор системи, що обслуговує хмару. Крім того, для хмарних обчислень існують власні стандарти, такі як архітектура OpenFog [11].

Ця взаємодія дозволяє оптимізувати обробку даних та забезпечує більш гнучкий підхід до розподілу інформації в системах Internet Of Things.

1.3 Аналіз загроз інформаційній безпеці IoT

Датчики та сенсори, використовувані в пристроях Internet Of Things (IoT), здатні збирати широкий спектр особистих даних. Наприклад, фітнес-трекери, системи моніторингу вдома, камери безпеки та транзакції з банківськими картками генерують особисті, бізнесові та екологічні дані. Ці дані часто об'єднуються з іншими джерелами і можуть бути використані для різних цілей, навіть без відома користувачів.

Сполучення даних, отриманих від фітнес-моніторів, із даними про стан дому може призвести до визначення місцезнаходження власника або його рухів. Цей гнучкий підхід до збору та агрегації даних може використовуватися для розв'язання важливих завдань, наприклад, для аналізу впливу на довкілля та прийняття рішень щодо його поліпшення. Проте такий підхід також відкриває можливості для порушення конфіденційності особистих даних та корпоративної інформації, а також може бути використаний для корпоративного шпигунства та інших негативних цілей [10,14,15].

Треба бути обережними та свідомими щодо обробки та зберігання особистих даних в системах IoT, а також вдосконалювати заходи безпеки для захисту приватності і конфіденційності інформації [10,14,15].

Велика кількість систем IoT розташована не лише в безпечних зонах, таких як домівка або офіси, але і в громадських місцях, віддалених регіонах, на рухомих транспортних засобах і навіть вбудована в людей. Ця розповсюдженість робить системи IoT важливою мішенню для різних видів кібератак. Напади на пристрої IoT, добре організовані і спрямовані, вже стали реальністю, а також пошук вразливостей у національних системах безпеки.

Для того, щоб уникнути або хоча б зменшити ризик таких ситуацій, необхідно аналізувати та враховувати всі потенційні вразливості обраних компонентів системи IoT та їх специфікації. Крім того, варто розробити стратегії для запобігання різним видам атак і методи захисту для їх подолання.

Забезпечення безпеки на всіх рівнях є критично важливим для успішної функціонування системи IoT. Це підвищує безпеку взаємодії між пристроями, надійність і сумісність всіх процесів. Правильна і ефективна система безпеки визначає успіх у реалізації та застосуванні IoT-рішень [17].

В системі IoT існують ключові аспекти безпеки, які включають забезпечення конфіденційності, цілісності та доступності даних та системи.

Конфіденційність даних:

— недостатня стійкість аутентифікації, що може призвести до несанкціонованого доступу до системи;

— небезпечні інтерфейси входу, такі як через Інтернет або мобільний зв'язок, які можуть стати вразливими для атак;

— відсутність шифрування транспортного рівня, що призводить до можливості простого доступу до передаваних даних;

— неправильне управління доступом до даних, яке може допустити несанкціонований доступ до конфіденційної інформації.

Цілісність даних:

— забезпечення конфіденційності та цілісності даних, разом із керуванням ризиками, є важливим аспектом безпеки;

— наявність стандартних заходів щодо забезпечення конфіденційності за замовчуванням;

— дотримання політики цілісності даних та відстеження, профілювання та управління даними для запобігання незаконній обробці даних.

Доступність системи:

— встановлення системи управління доступом для користувачів, що дозволяє регулювати права доступу;

— запобігання використанню небезпечного програмного забезпечення на пристроях;

— забезпечення неперервності послуг і системи;

— заходи для запобігання та протидії шкідливим атакам на системи IoT.

Загальний підхід до цих аспектів безпеки є критично важливим для забезпечення стабільної та надійної роботи системи IoT.

1.4 Постановка задач дослідження

Метою даного дослідження є підвищення безпеки та захисту пристроїв Internet Of Things всередині корпоративної комп’ютерної мережі від несанкціонованого доступу. Це досягається за допомогою вдосконаленого технологічного дизайну системи IoT. Для досягнення поставленої в роботі мети необхідно виконати такі завдання:

— проаналізувати архітектуру і ключові компоненти екосистеми Internet Of Things та особливості роботи технології IoT з точки зору взаємодії, обробки даних та розподілу інформації в системах IoT;

— виконати аналіз загроз інформаційній безпеці IoT;

— спроектувати вдосконалений технологічний дизайн системи Internet Of Things;

— запропонувати розподіл загроз безпеці по рівням технологічного дизайну системи Internet Of Things;

— розробити модель безпечного дизайну системи Internet Of Things урахуванням 4-рівневого дизайну системи Internet Of Things;

— розробити модель корпоративної комп’ютерної мережі в програмному середовищі Packet Tracer з захистом у відповідності до запропонованого технологічного дизайну системи IoT.

Загалом, планується розширити методологічну базу методів та засобів захисту Internet Of Things в межах корпоративної комп’ютерної мережі, що може стати поштовхом для подальшого удосконалення процесів захисту елементів IoT в корпоративній комп’ютерній мережі.

2 ТЕХНОЛОГІЧНИЙ ДИЗАЙН СИСТЕМИ IOT

У другому розділі магістерської кваліфікаційної роботи подамо основну ідею технологічного дизайну системи Internet Of Things.

Стек технологій – це сукупність стандартних технологічних рішень, які сприяють досягненню поставлених завдань [11]. У цьому дослідженні під терміном "стек технологій" розуміється спільне використання відповідних технічних рішень для вирішення завдань, пов'язаних із розробкою та впровадженням системи IoT [20]. Це дозволить об'єднати технології в єдину структуру з визначеними цілями. Створення та використання стеку технологій для IoT, надає можливість отримати розуміння технічних та програмних рішень для досягнення конкретних цілей, уникаючи великих обсягів наукових та технічних досліджень і створює основу для подальших перспективних досліджень технологій для поліпшення існуючого стеку чи розроблення нових технологічних рішень.

В цій роботі здійснено аналітичне припасування технологічного дизайну системи IoT до відомого протокольних та технологічних стеків. Зокрема, до протокольного стеку TCP/IP та відомої моделі відритих систем OSI [12,15]. Це дало можливість спроектувати поліпшений дизайн системи IoT на основі проведених досліджень та набутого досвіду щодо релевантності тієї чи іншої технології чи способу реалізації відповідно завданням дослідження.

2.1 Технологічний дизайн системи Internet Of Things

Відповідно до моделі сервіс-орієнтованої архітектури (Service-oriented architecture, SOA) технологічний дизайн системи Internet Of Things буде містити 4 чотири рівні, згідно досліджень, проведених у 1 розділі роботи (рис. 1.2).

Відобразимо відкриту модель OSI, відомий протокольний стек TCP/IP, прототипну 3-рівневу модель та модель технологічного дизайну системи Інтернету речей за принципами SOA (рис. 2.1).

OSI	TCP/IP	3-LAYER Sec.IOT DESIGN	**4-LAYER Sec.IOT DESIGN**
7 Application 6 Presentation 5 Session	Application	Прикладний рівень	**Службовий рівень**
4 Transport	Transport	Транспортний рівень	**Рівень корпоративної комп'ютерної мережі**
3 Network	Network		
2 Data Link	Network Access	Рівень виконавчих пристроїв	**Рівень локальних інтерфейсів**
1 Physical			**Рівень датчиків**

Рисунок 2.1 — Приведення технологічного дизайну системи Internet Of Things до відомих стандартів

Така архітектура (рис 2.1) забезпечує взаємодію між великою кількістю різних пристроїв. Кожен з цих рівнів має такі функції:

— рівень датчиків взаємодіє з апаратними засобами та датчиками для визначення стану системи Інтернету речей та безпосередньо збирання даних (рівень 1);

— рівень локальних інтерфейсів надає різні методи та засоби взаємодії системи Інтернету речей з безпечною мережею (LAN) (рівень 2);

— рівень корпоративної комп'ютерної мережі надає повноцінну мережеву інфраструктуру, яка для стабільної підтримки з'єднань у корпоративній комп'ютерній мережі (рівень 3);

— службовий рівень дає можливість керувати засобами та сервісами між користувачам та додатками (рівень 4).

За використання запропонованого технологічного дизайну, ця система розбивається на підсистеми, які взаємодіють між собою та можуть бути використані для підтримки функціонування новоствореної системи. Цей підхід гарантує безперебійну роботу, оскільки при відмові одного компонента інші продовжать функціонувати. У випадках, коли надійність та доступність є ключовими завданнями у проектуванні, ця модель виявляється найкращим вибором.

Цей підхід спрощує взаємодію з протоколами передавання даних та різними рівнями системи, оскільки сприяє покращенню взаємодії між об'єктами та спрощує процес керування. Модель технологічного дизайну системи Інтернету речей організована на основі принципів SOA, дає Інтернету речей можливість повністю реалізувати свій потенціал і показати всі свої переваги. Ця модель дозволяє створювати складні сервіси, де для виконання різних завдань можна виділити окремі об'єкти системи [10].

2.2 Безпековий технологічний дизайн системи Internet Of Things

У кожної системи є своя власна структура, або інакше кажучи, дизайн, що визначає, як взаємодіють всі її складові. Система Інтернету речей не є винятком.

Після аналізу джерел (виконано у 1 розділі дисертаційної роботи) було прийнято рішення зобразити взаємозв'язок компонентів системи IoT з аспектами безпеки. Цю залежність можна побачити на рисунку 2.2.

Рисунок 2.2 — Безпековий технологічний дизайн системи Internet Of Things

Нині цифрові технології проникають у всі сфери життя, запити до безперебійної роботи програмних чи апаратних продуктів стають все актуальнішими. Несанкціоноване втручання на різних рівнях таких систем може завдати збитків. Тому під час розробки будь-якого програмного чи апаратного продукту, включно з цільовою системою Інтернету речей, забезпечення безпеки стає надзвичайно важливим [11].

На рисунку 2.3 зображено відповідність рівнів стеку системи IoT і проблем безпеки, притаманних цим рівням.

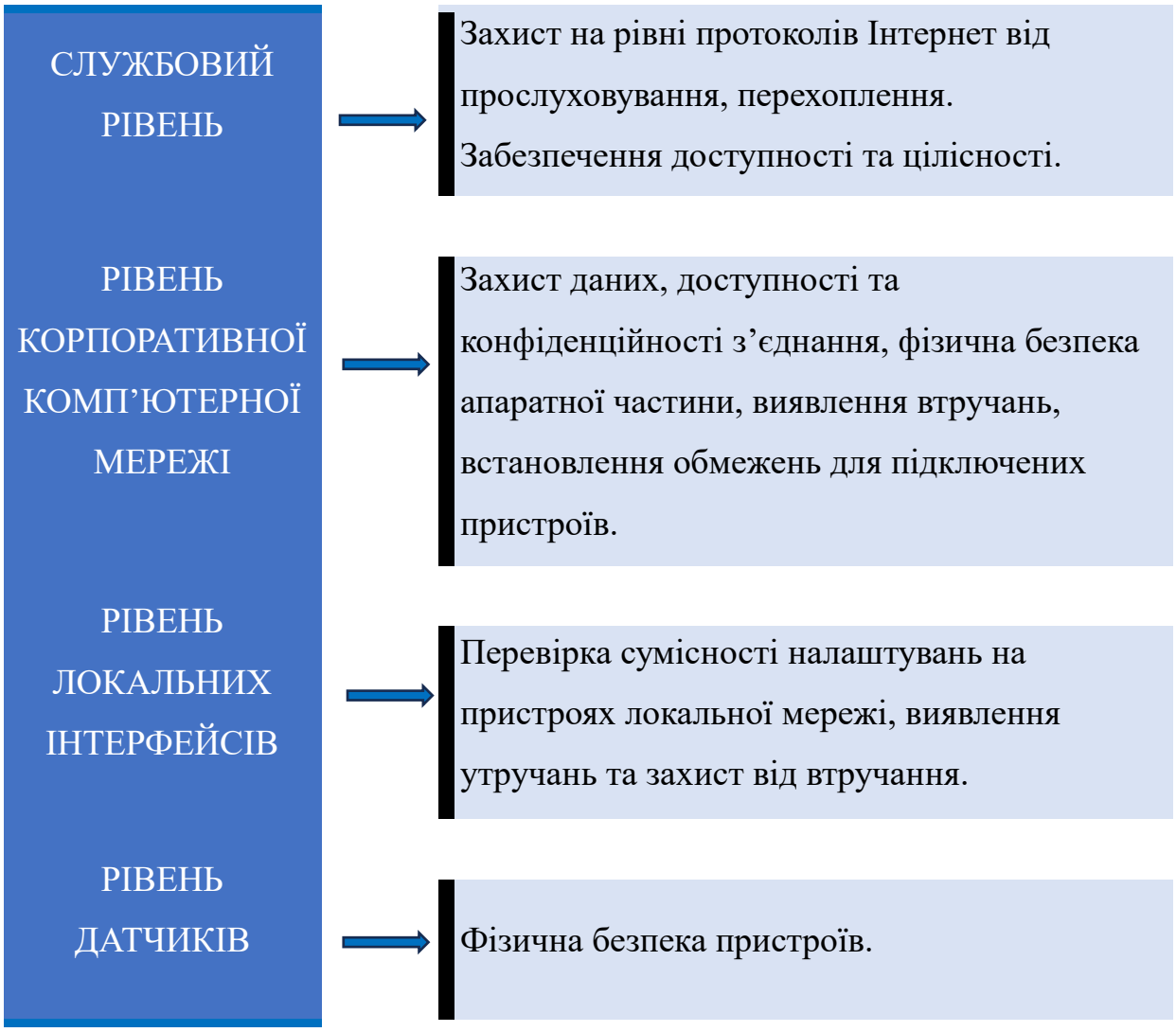


Рисунок 2.3 — Розподіл загроз безпеці по рівням технологічного дизайну системи Internet Of Things

З урахуванням зростаючої мобільності, сучасна архітектура системи повинна бути високою у рівні адаптабельності для ефективної обробки різноманітних динамічних взаємодій на всіх рівнях її структури. Надання більш високого рівня абстракції, який може приховати деякі деталі реалізації, є безперечною перевагою стандартних архітектурних рішень і моделей.

Такий безпековий технологічний дизайн системи IoT є інтегрованою системою і гарантує надійну роботу своїх компонентів та забезпечує зв'язок між фізичними та віртуальними складовими.

Для створення цілісної системи обов'язково важливим є докладний підхід до проектування, з особливою увагою до процедур відновлення системи після виникнення неполадок. Враховуючи, що створення безпечного середовища має велике значення, важливо враховувати масштабність системи.

2.3 Модель безпечного дизайну системи Internet Of Things

Якщо враховувати використання відкритих стандартів, тоді запропонуємо вирішення питань безпеки на різних рівнях технологічного дизайну системи Internet Of Things. З метою підвищення загальної захищеності системи IoT, кожен рівень стеку використовує різні протоколи, послуги та механізми безпеки. Отже, кожен рівень прагне досягти важливих цілей, включаючи забезпечення безпеки інформації, фізичної безпеки та стійкого функціонування системи управління безпекою, як окремо, так і в цілому. Розподілимо рівні технологічного дизайну системи Internet Of Things (згідно рис. 2.1) відповідно їх функціональним елементам та розпишемо кожен згідно архітектури IoT та з погляду безпеки та аналізу літературних джерел у п.1.1 та п. 1.2 у вигляді таблиці 2.1 нижче.

OSI	TCP/IP	ДИЗАЙН IOT	ОБ'ЄКТ ЗАХИСТУ (ПРОТОКОЛ, ТЕХНОЛОГІЯ, ТОЩО)	МЕТОД ЗАХИСТУ	ОПИС
7	Додатків	СЛУЖБОВИЙ РІВЕНЬ	DHCP, SSH, CoAP, AMQP, XMPP, masquerad	DHCP snooping, RSA, ACL, IPS, брандмауер, шифрування,	Хмарні послуги, сервіси аналізу даних, машинне навчання, зв'язок з пристроями (частково), безпека додатків
6					
5					
4	Транспортний	РІВЕНЬ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ	DDoS, DoS, IPv4, IPv6, MQTT та DDS, TLS / SSL, MITM, TCP, UDP	SYN protection, 6LowPAN,	Зв'язок з пристроями, провідні та безпровідні мережі, протоколи передавання даних (частково), корпоративні мережні пристрої (частково)
3	Інтернету				
2	Мережевого доступу	РІВЕНЬ ЛОКАЛЬНИХ ІНТЕРФЕЙСІВ	MAC, MIM, DNS, ARP, Адресні spoofing, STP, RFID, WSN, PKI, VLAN	PortSecurity, DAI, BPDU Guard IPSG, PortFast	Мережні пристрої (частково), протоколи передавання даних (частково), міжплатформне ПЗ
1		РІВЕНЬ ДАТЧИКІВ	selfish загроза, фізична безпека, порушення цілісності даних, зловмисне ПЗ	IPsec, IEEE 802.11 AH	Датчики, безперебійне живлення, ОС реального часу, безпека, GPS, Bluetooth

Таблиця 2.1 — Модель безпечного дизайну системи Internet Of Things

У таблиці 2.1 наведені складові та задачі для окремого рівня моделі безпечного дизайну системи Internet Of Things із відображенням атак та

вимоги безпеки, які необхідні для кожного з них. Подана таблиця 2.1 ілюструє перелік методів для вирішення проблем безпеки під час безпечного дизайну системи Internet Of Things [18].

Для того, щоб продемонструвати вимоги до безпеки в дизайні Internet Of Things на прикладі, використаємо запропонований в розділі 1 розширений технологічний дизайн системи IoT, яка складається з рівнів: датчиків, локальних інтерфейсів, корпоративної комп'ютерної мережі та службового. Кожен з них має забезпечити сприяння чіткому процесу управління безпекою корпоративної комп'ютерної мережі, це забезпеченню контролю доступу, автентифікації та цілісності даних, також їх конфіденційності і наявності інструментів для захисту системи IOT від вірусів та атак.

Тож створювана модель безпечного дизайну системи Internet Of Things повинна мати можливість відстежувати кожен пристрій корпоративної комп'ютерної мережі, контролювати трафік та бути спроможною захистити або тимчасово обмежити використання пристрій/оїв аби значно зменшити (в ідеалі – унеможливити, пом'якшити) критичні наслідки для цілої екосистеми корпоративної комп'ютерної мережі, що містить IoT. Тепер коротко розглянемо запропонований в розділі 1 розширений технологічний дизайн системи IoT.

2.3.1 Безпека на рівні датчиків

Даний рівень розширений технологічний дизайн системи IoT можна охарактеризувати як сполучення трьох ланок, які забезпечують дані від:

— пристроїв збору інформації;

— місця розташування (функціонування) пристрою;

— безпосередньо від людей.

Для повноцінної реалізації функцій безпеки необхідно передбачене виробником виконання елементів безпеки в пристроях, тобто можливість аутентифікації, шифрування даних та обмеження в локальному збереженні

зібраної інформації. Зі сторони корпоративної комп'ютерної мережі та персоналу, що їх конфігурує – врахування особливостей роботи підприємства.

Складними питаннями безпеки на рівні датчиків технологічного дизайну системи IoT є:

— фізична безпека та захист пристроїв збору даних. Найкраще – це коли передбачено ускладнений або неможливий доступ до пристрою;

— недостатня модернізація апаратної частини та програмної складової, що обслуговує пристрій (наприклад, версії ОС або прошивка). Часто в пристроях (іноді адміністратори роблять це навмисно) немає передбаченої можливості для їх оновлення чи переналаштування. Нові вразливості можуть виникати постійно, тож якщо пристрій не буде мати доступу для оновлення своїх налаштувань, це може послабити безпеку системи.

2.3.2 Безпека на рівні локальних інтерфейсів

Цей рівень є посередником між IoT системою в місцях розташування датчиків і мережевими службами, додатками. Він надає підтвердження того що взаємодія між додатками і системою є легітимною. Потенційними проблемами на цьому рівні є:

— необхідність однотипних (часто – подібних) налаштувань конфігурації на всіх пристроях для досягнення сумісності з точки зору конфігурації;

— забезпечення безпеки зібраних даних на цьому рівні технологічного дизайну системи IoT;

— створення ефективних програмно-апаратних рішень безпеки задля оптимізації процесу взаємодії з легальними користувачами і зловмисниками.

Рекомендаціями для вирішення проблем безпеки даного рівня є дотримання конфіденційності, цілісності та доступності, регулярне оновлення ПЗ, аутентифікація та авторизація користувачів та адміністратора.

2.3.3 Безпека на рівні корпоративної комп’ютерної мережі

Мережевий рівень є надважливою частиною розширеного технологічного дизайну системи IoT, оскільки є каналом передавання даних між іншими рівнями. Зважаючи на те, що екосистема IOT складається з великої кількості побічних гібридних систем, фактор проблеми масштабованості корпоративної комп’ютерної мережі, її складності та безпеки передавання даних є значним.

Серед проблем, які виникають тут можуть бути:

— забезпечення класичних вимог інформаційної безпеки – конфіденційності, цілісності та доступності;

— фізична безпека (якщо пристрої які забезпечують передавання даних можуть бути у вільному доступі);

— надмірна кількість підключень до корпоративної комп’ютерної мережі, що створює додаткові складнощі в обслуговуванні, надмірні витрати мережевих ресурсів (як програмного, так і апаратного гатунку) та збільшення вразливостей внаслідок ймовірного зловмисного впливу;

— можливість запобіганню зловмисного роду атак, на зразок «Man-In-The-Middle» для перехоплення інформації, що передається між об’єктами корпоративної комп’ютерної мережі.

Основними викликами до безпеки на рівні корпоративної комп’ютерної мережі в розумінні розширеного технологічного дизайну системи IoT є мінімізація можливості впливу зловмисників на екосистему та збільшення ефективності її роботи та, водночас, покращення якості обслуговування (Qos).

2.3.4 Безпека на службовому рівні

Службовий рівень розширеного технологічного дизайну системи IoT забезпечує ефективну взаємодію використання апаратних та програмних ресурсів і можливість повторного використання цих ресурсів. На службовому

рівні відбувається аналіз отриманих даних від рівня датчиків, тож тут присутні служби обробки подій, служби інтеграції і аналітики тощо, які дозволяють обмін інформацією між сервісами та додатками, а також забезпечують виконання необхідних дій.

Виклики, які притаманні службовому рівню:

— забезпечення конфіденційності, цілісності та доступності;

— можливість недобросовісних маніпуляцій даними від служб та додатків службового рівня;

— створення захисту від різноманітних атак (на кшталт DoS та DDoS-атак);

— забезпечення аналізу трафіку для алміністраторів і обмеження для неавторизованих користувачів задля недопущення жодних маніпуляцій з даними.

Класичним підходом до вирішення і убезпечення від проблем на службовому рівні є відповідність стандартам та протоколам під час проектування та впровадженні дизайну системи IoT [26].

3 ОРГАНІЗАЦІЯ МЕРЕЖІ ЗА 4-РІВНЕВИМ ТЕХНОЛОГІЧНИМ ДИЗАЙНОМ INTERNET OF THINGS

У третьому розділі магістерської кваліфікаційної роботи покажемо підготовку до організації захисту мережі за 4-рівневим технологічним дизайном Internet Of Things.

Тут планується підготуватися до практичної реалізації компонентів екосистеми IoT в корпоративних комп’ютерних мережах в різних сферах та їх вплив на функціонування конкретних організацій, підприємств чи установ. Тут є опис процесу створення мережі, перерахування та найменування її структурних компонентів та їх розподіл за принципом рівнів технологічного дизайну системи Internet Of Things, який був визначений в попередніх частинах цього дослідження.

3.1 Базові поняття під час організації захисту

Під терміном «корпоративна мережа» розуміється приватна комп'ютерна мережа, яка об'єднує комп'ютери та інші пристрої в межах однієї організації або підприємства. Ця мережа створює можливість обміну даними та ресурсами між вузлами в безпечному та контрольованому середовищі. Корпоративні мережі використовуються для спільної роботи, обміну інформацією та управління бізнес-процесами.

Використання технологій і елементів IoT відіграє важливу роль у сучасних корпоративних мережах. Це дає можливість підключати фізичні пристрої та різноманітні сенсори до мережі, щоб збирати, аналізувати дані та використовувати їх для прийняття рішень. Технології IoT можуть бути використані для автоматизації процесів, моніторингу та управління ресурсами, а також для поліпшення безпеки та ефективності роботи.

Інтеграція IoT з корпоративною мережею дозволяє організаціям отримувати важливі дані в реальному часі, взаємодіяти між різними

пристроями, відстежувати та керувати ресурсами, а також вдосконалювати бізнес-процеси та аналізувати отримані дані для поліпшення обслуговування клієнтів та досягнення більшої продуктивності. Прикладами застосування технології Інтернету речей можуть бути моніторинг стану природного середовища, забезпечення безпеки об'єктів або територій загального користування, обслуговування протипожежної системи і т.д.

Як вже зазначалося у даній роботі, автор вирішив розширити стандартну модель безпечного дизайну системи Internet Of Things до 4 рівнів, вказавши їх функціональне призначення та відповідність конкретним технологіям. Це сприяє більш чіткому розподілу відповідальності та координації функцій управління безпекою для кожного елемента окремо, та в цілому.

3.2 Підготовчий етап, вибір обладнання відповідно об’єктам захисту

Реалізація захисту елементів IoT в цій корпоративній мережі відбувається на 4 рівнях технологічного дизайну системи IoT, а саме:

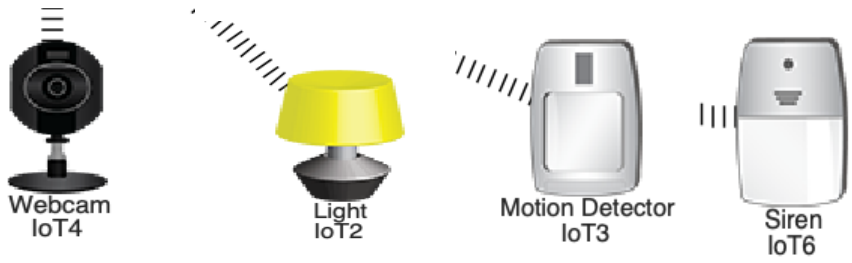
— рівні датчиків;
— рівні локальних інтерфейсів;
— рівні корпоративної комп’ютерної мережі;
— службовому рівні.

Кожен з цих перелічених рівнів відповідає за певну ділянку мережі. Зокрема, для реалізації рівня датчиків в цій магістерській роботі використано такі пристрої та елементи, як IoT5 (рис. 3.1, а), IoT1 (рис. 3.1, б), IoT7 (рис. 3.1, в), IoT4 (рис. 3.1, г), IoT2 (рис. 3.1, д), IoT3 (рис. 3.1, е), IoT6 (рис. 3.1, є).

а) IoT5

б) IoT1

в) IoT7



г) IoT4 д) IoT2 е) IoT3 є) IoT6

Рисунок 3.1 — Використані IoT пристрої та елементи

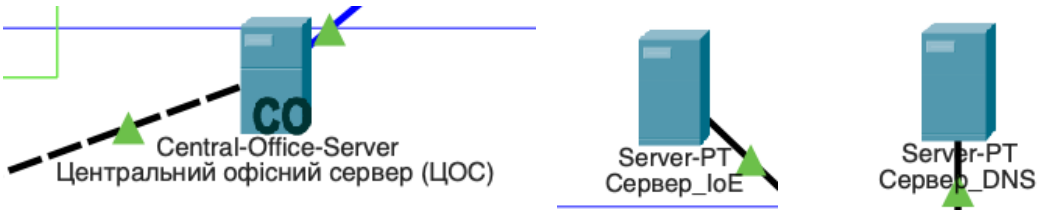
Для реалізації рівня локальних інтерфейсів в цій магістерській роботі використано такі пристрої, як Кабельний модем (рис. 3.2, а) та КОМ_Сер (рис. 3.2, б).

а) Кабельний модем б) КОМ_Сер

Рисунок 3.2 — Використані пристрої на рівні локальних інтерфейсів

Для реалізації рівня корпоративної комп'ютерної мережі рівня цій магістерській роботі використано такі пристрої та елементи, як Хмарне середовище / WAN (рис. 3.3, а), ЦЕНТР (рис. 3.3, б), Центральний офісний сервер (ЦОС) (рис. 3.3, в), Сервер_IoE (рис. 3.3, г), Сервер_DNS (рис. 3.3, д).

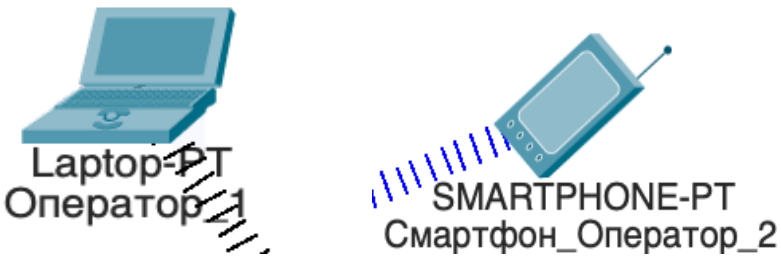
а) WAN б) ЦЕНТР



в) ЦОС г) Сервер_IoE д) Сервер_DNS

Рисунок 3.3 — Використані пристрої та елементи на рівні корпоративної комп’ютерної мережі

Для реалізації службового рівня в цьому проекті використано кінцеві пристрої користувачів та/або операторів мережі IoT, як Оператор_1 (рис. 3.4, а) та Смартфон_Оператор_2 (рис. 3.4, б).



а) Оператор_1 б) Смартфон_Оператор_2

Рисунок 3.4 — Кінцеві пристрої користувачів та/або операторів

Розробка загальної схеми корпоративної комп’ютерної мережі з елементами Internet Of Things передбачає таку фізичну топологію мережі із розподілом по рівням згідно запропонованого технологічного дизайну системи Internet Of Things та у відповідності із моделлю безпечного дизайну системи Internet Of Things. На рис. 3.5 акцент зроблений на рівні датчиків, на рис. 3.6 акцент зроблений на рівні локальних інтерфейсів.

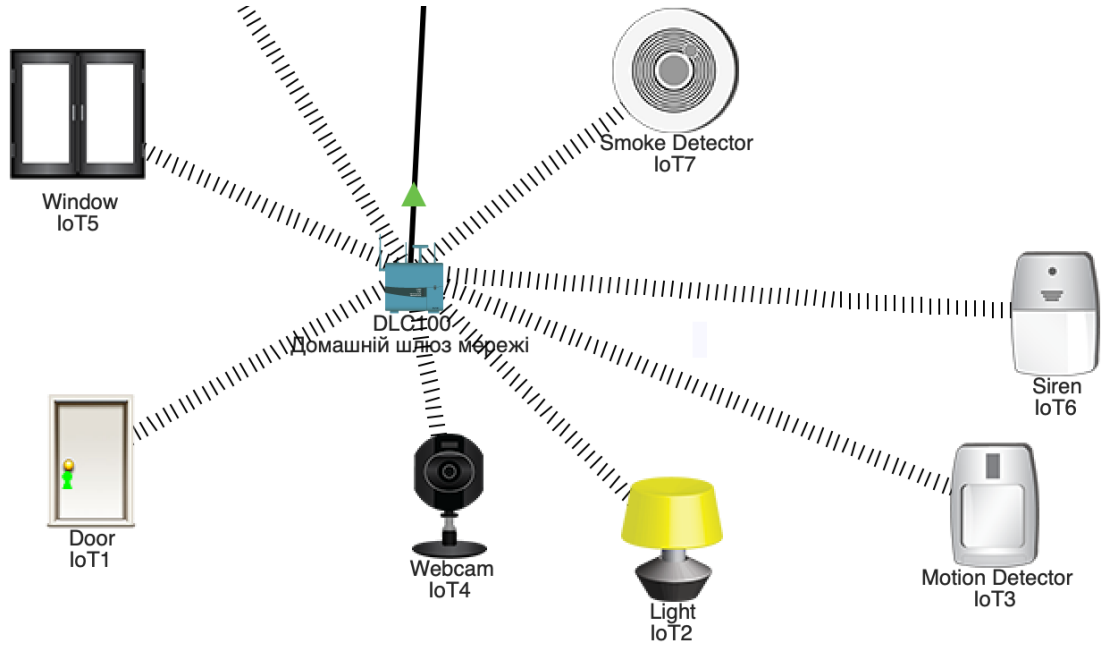


Рисунок 3.5 — Рівень датчиків

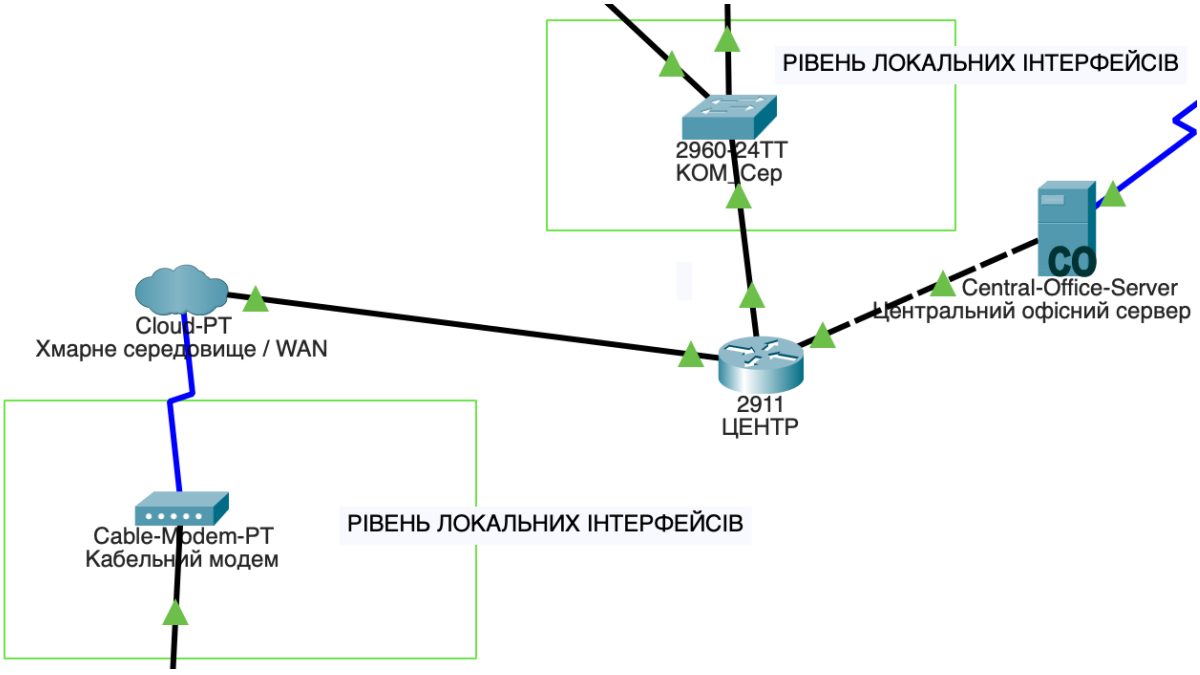


Рисунок 3.6 — Рівень локальних інтерфейсів

На рис. 3.7 акцент зроблений на рівні пристроїв корпоративної комп’ютерної мережі, а на рис. 3.8 акцент зроблений на службовому рівні.

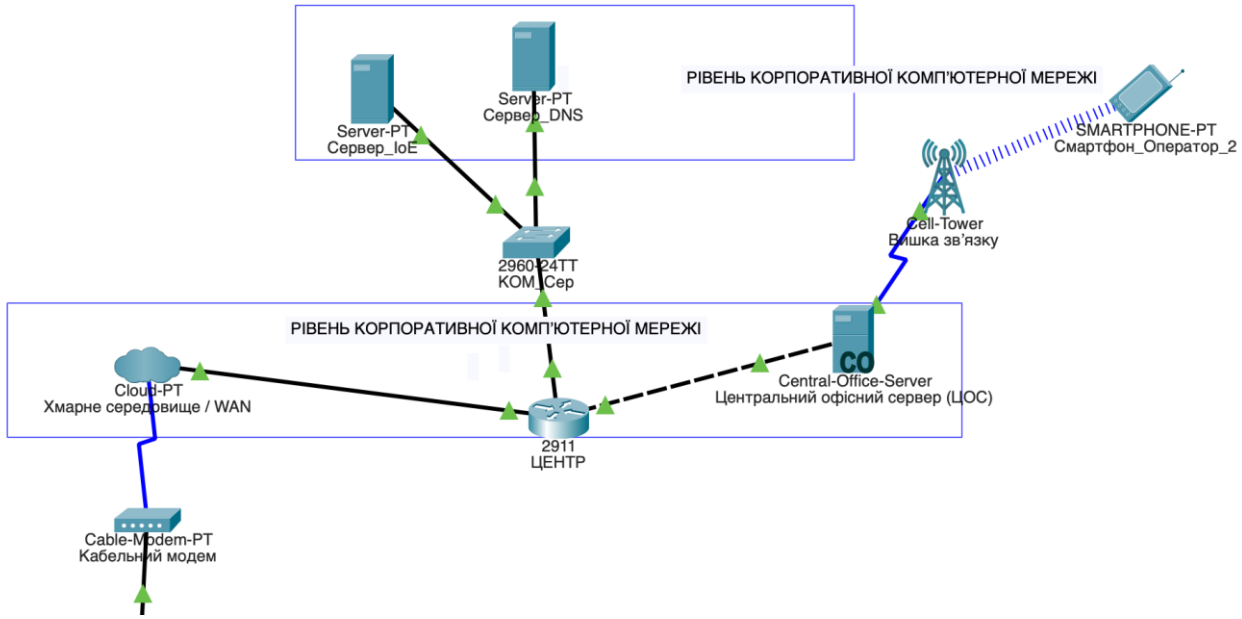


Рисунок 3.7 — Рівень пристроїв корпоративної комп’ютерної мережі

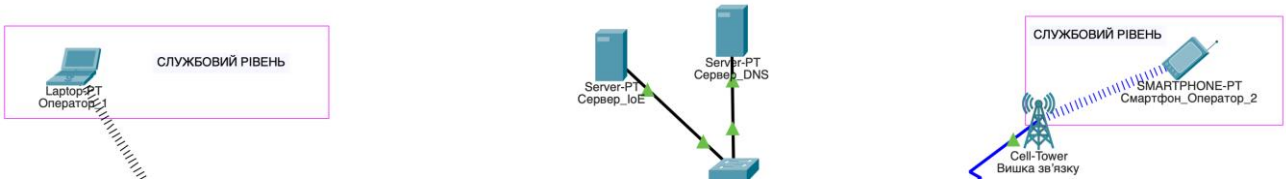


Рисунок 3.8 — Службовий рівень

На рис. 3.9 показано загальний вигляд розробленої корпоративної комп’ютерної мережі IoT з її структурними компонентами та їх розподілом за принципом рівнів технологічного дизайну системи Internet Of Things, який був визначений в попередніх частинах цього дослідження.

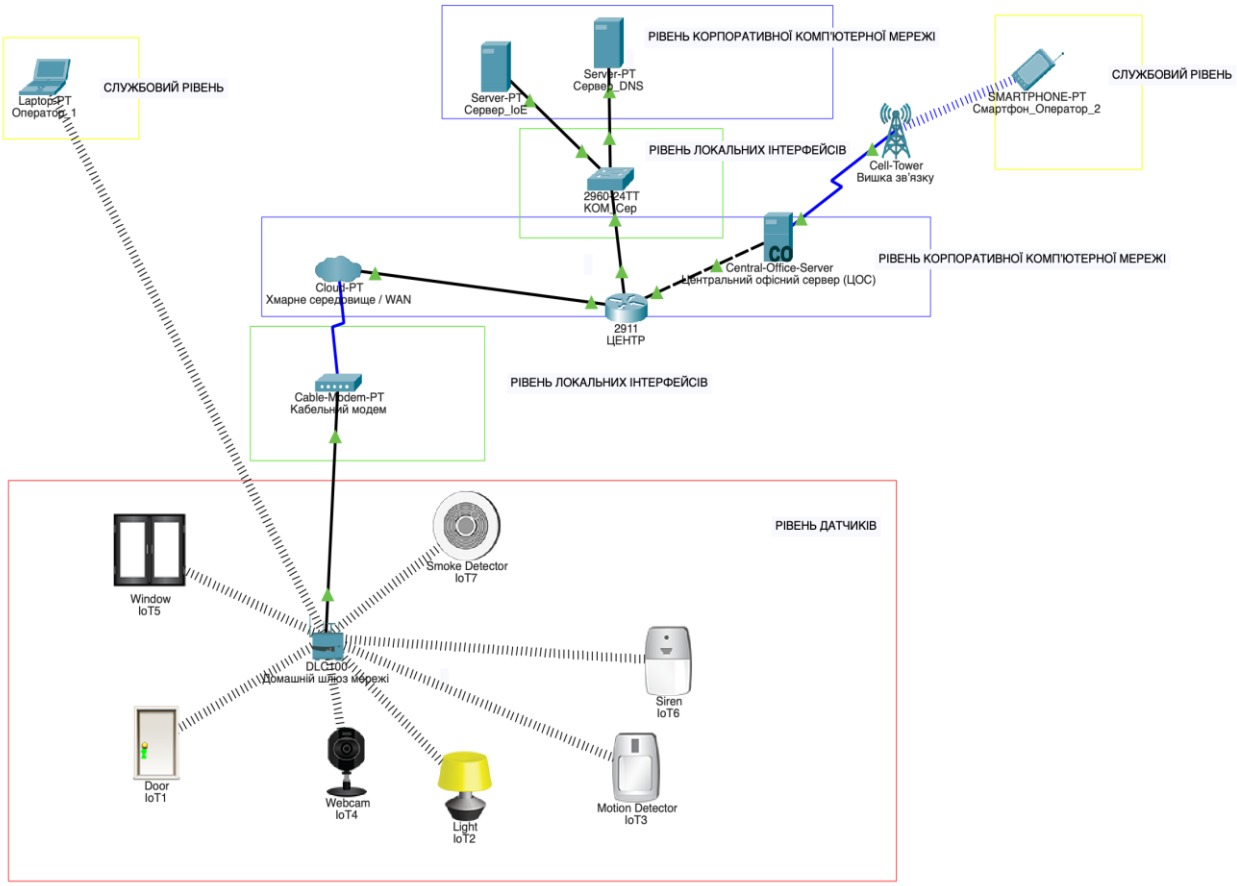


Рисунок 3.9 — Зображення загальної схеми корпоративної мережі

3.3 Ключові етапи налаштування мережі

Ключові етапи налаштування мережі передбачає такі кроки.

Сформуємо структуру мережі, об’єднаємо всі пристрої відповідними лініями зв’язку.

На пристрої «Домашній шлюз мережі» потрібно активувати режим WPA2-PSK та сформувати пароль (тут це bachelor). Сервіс DHCP, що налаштований на «Домашній шлюз мережі» автоматично забезпечує IP-адреси мережі. Активний інтерфейс має IP адресу 192.168.25.1/24.

Успішне виконання п.2 дозволяє активувати бездротовий зв’язок на ноутбуці «Оператор_1» шляхом додавання модулю бездротового зв’язку Linksys-WPC300N.

В режимі desktop ноутбука «Оператор_1» у вкладці «бездротове з’єднання» виконуємо підключення ноутбука «Оператор_1» із використанням заданого раніше паролю (bachelor).

В режимі налаштування веб-камери IoT4 змінюємо там SSID на назву нашої мережі «Домашній шлюз» (рис. 3.10). І повторюєм операцію із зміною режиму і введенням паролю на таких пристроях: IoT5, IoT1, IoT7, IoT2, IoT3, IoT6. Таким чином приводим всі пристрої системи Інтернету речей в режим спільних налаштувань. Надалі підключаємо поступово всі пристрої до «Домашній шлюз мережі» (із IP-адресою 192.168.25.1/24.). Нотатка: DHCP обслуговує усі пристрої IoT.

Рисунок 3.10 — Процес підключення ноутбука до бездротового зв’язку

Для зручності і візуального супроводу виконаємо структурування елементів та їх об’єднання по рівням Технологічного стеку системи Інтернету речей.

Налаштовуємо роутер «ЦЕНТР» — прописуємо адреси інтерфейсів: 10.0.0.1/24 (зона серверів), 209.165.201.225/27 (зона вишки та центрального офісного серверу «Центральний офісний сервер (ЦОС)»), 209.165.200.225/27 (зона пристроїв IoT).

Переходимо до налаштування центрального офісного серверу серверу «Центральний офісний сервер (ЦОС)». 172.16.1.1/24 — адреса підключення кабелю з боку вишки до серверу, а з боку роутера — налаштовуємо DHCP тут, щоб сервер мав наступні параметри:

— ip dhcp excluded-address 209.165.201.225 209.165.201.229;
— network 209.165.201.224 255.255.255.224;
— default-router 209.165.201.225;
— dns-server 10.0.0.254.

Налаштовуємо DHCP на роутері «ЦЕНТР» для пристрою «Домашній шлюз». Маємо такі параметри:

— ip dhcp excluded-address 209.165.200.225 209.165.200.229;
— network 209.165.200.224 255.255.255.224;
— default-router 209.165.200.225;
— dns-server 10.0.0.254;

Налаштовуємо хмарне середовище. Міняємо в налаштуваннях хмари в розділі «Ethernet» DSL на Cable. І добавляємо відповідну пару Coaxial+Ethernet в налашуваннях “Cable”. Це в свою чергу добавляє відповідні налаштування в пристрій «Домашній шлюз» через DHCP вкладки «Internet».

Перевіряємо налаштування DHCP в всіх пристроях, які бездротово підключені до «Домашній шлюз». Результат видно на рисунку 3.11.

Налаштовуємо статичну адресу на серверах «Сервер_DNS» та «Сервер_IoE» відповідно. Вмикаємо сервіс DNS та сервіс IoE на відповідних серверах: «Сервер_DNS», «Сервер_IoE». Результат видно на рисунку 3.12 (нотатка: а) – це «Сервер_DNS», б) – це «Сервер_IoE»).

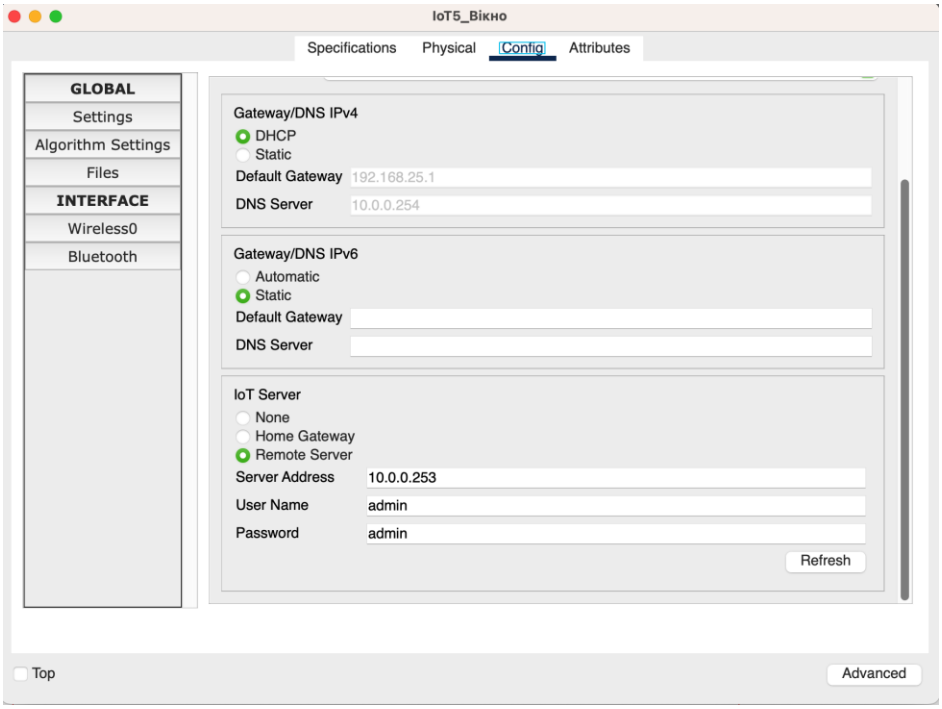
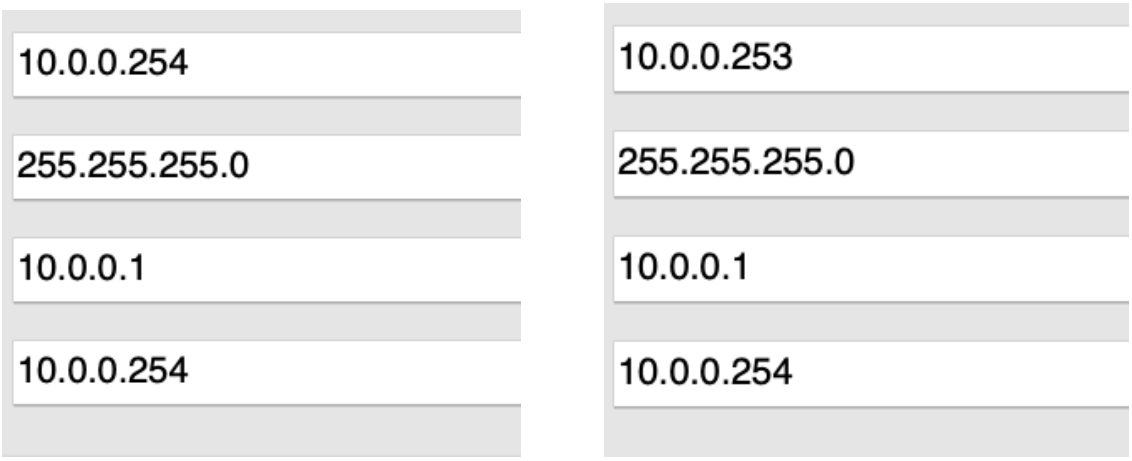


Рисунок 3.11 — Результат перевірки підключення сервісу DHCP



а) Сервер_DNS б) Сервер_IoE

Рисунок 3.12 — Результат налаштування статичної адреси на відповідних серверах

Налаштовуємо зв’язок всіх пристроїв Internet Of Things з сервером IoE. Результат параметрів налаштування видно на рисунку 3.13.

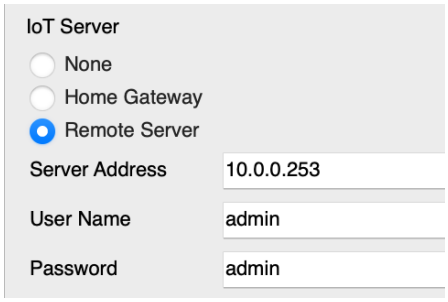


Рисунок 3.13 — Налаштування зв’язку пристроїв IoT з сервером «Сервер_IoE»

В режимі IoE monitor на ноутбуці «Оператор_1» виконуємо реєстрацію свого облікового запису там, оперуємо логіном, паролем і ще раз підключаємо всі пристрої до відповідного серверу. Тепер ми бачимо на ноутбуці всі пристрої, які вдалося підключити і якими можемо керувати.

В режимі сервісу DNS на пристрої «Сервер_DNS» вводимо: www.iot.org в поле name і 10.0.0.253 в поле address. І додаємо цей запис. Результат видно на рисунку 3.14.

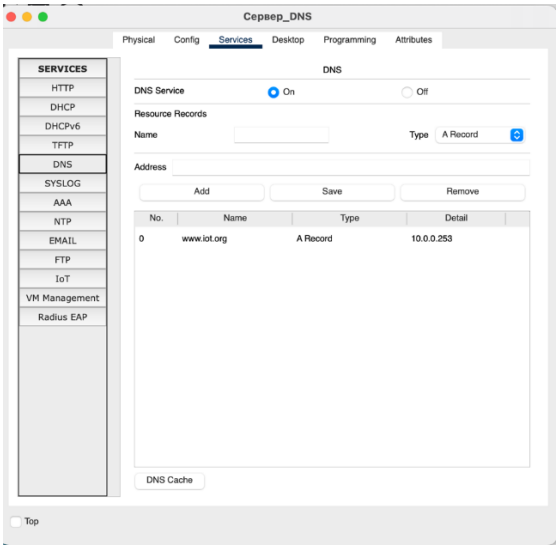


Рисунок 3.14 — Результат підключення DNS-сервісу

Створюємо на пристроях кластер інтернету для імітації корпоративної мережі.

4 ПРАКТИЧНА РЕАЛІЗАЦІЯ ЗАХИСТУ ЗА МОДЕЛЛЮ БЕЗПЕЧНОГО ДИЗАЙНУ СИСТЕМИ INTERNET OF THINGS

У четвертому розділі магістерської кваліфікаційної роботи покажемо практичну реалізацію захисту мережі за моделлю безпечного дизайну системи Internet Of Things.

Останнім елементом даного розділу є висновки відносно тестування дій, проведених автором у моделі корпоративної комп'ютерної мережі для захисту її компонентів за 4-рівневим технологічним дизайном Internet Of Things.

4.1 Реалізація безпеки на рівні датчиків

Тут реалізовуємо попередньо обрані та вже згадані у цій роботі елементи захисту на кожному з рівнів, з додатковим описом процесу їх впровадження та налаштування.

Ґрунтуючись на розробленій автором таблиці 2.1 яка є моделлю безпечного дизайну системи Internet Of Things, способом реалізації захисту елементів рівня датчиків є: забезпечення фізичного захисту для різноманітних пристроїв (датчиків, сенсорів, тощо) — передбачити можливість безперебійного живлення або автономного варіанту живлення, монтування GPS-міток для відстеження на випадок екстрених ситуацій; унеможливлення впливу зловмисників на них через забезпечення своєчасного оновлення програмного забезпечення; запобігання порушенню цілісності даних через можливий побічний вплив (як умисний, так і випадковий) – налаштування автентифікації за допомогою WPA-PSK2 на рисунку 4.1 з режимом шифрування AES, а також протидія «selfish»-загрозам шляхом встановлення чітких правил та постійної роботи з просвітництва щодо них серед членів колективу організації чи установи.

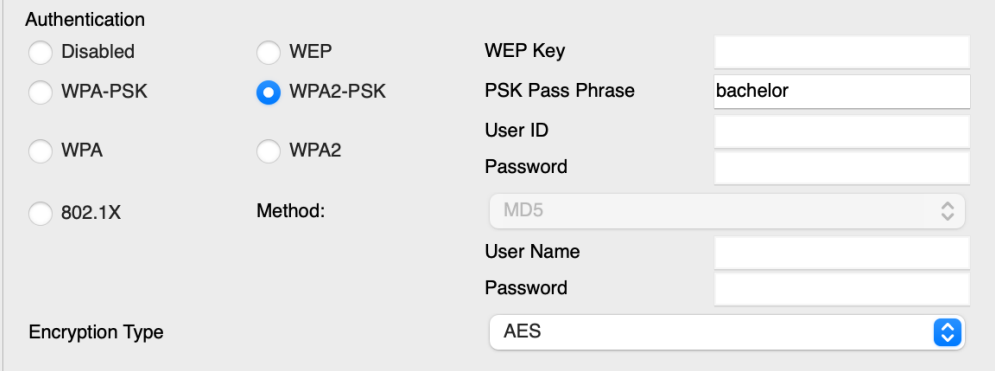


Рисунок 4.1 — Результат налаштування WPA-PSK2

4.2 Реалізація безпеки на рівні і локальних інтерфейсів

Об’єктом захисту на рівні локальних інтерфейсів є захист на рівні MAC-адрес, який передбачатиме унеможливлення несанкціонованого доступу зловмисника з його пристрою, де MAC-адреса відрізнятиметься від MAC-адреси легітимного хоста.

Засобом захисту на базі відповідності MAC-адрес на сенсорному рівні виконуватимемо засобами PortSecurity, що буде налаштований на свічі «КОМ_Сер».

Технологія Port security дозволяє контролювати підключення сторонніх пристроїв до мережі за допомогою їх MAC-адрес. Можна вручну вказати MAC адресу машини, яка має право підключатися до порту комутатора. Робиться це наступним чином:

```
Switch (config)#int fastEthernet 0/46
Switch (config-if)#switchport port-security mac-address X. X. X
```

Де X. X. X - 48-бітове значення MAC-адреси.

Такий варіант є вкрай незручний через те, що мережа абсолютно перестає бути мобільною і в разі збільшення її об’єму процес адміністрування стає все складнішим. Більш того, процес підробки MAC-адреси пристрою зараз вже не

є складним та недоступним процесом. Тому, є другий варіант застосування цієї технології, який виконується так:

```
Switch (config-if)#switchport port-security maximum 1
Switch (config-if)#switchport port-security violation restrict
Switch (config-if)#switchport port-security aging time 1
```

Застосовуючи цей покроковий процес налаштування, встановлюємо максимальне значення кількості MAC-адрес, які можуть бути підключені до порту за певний час. В разі використання однієї робочої станції немає необхідності вказувати цифру більше 1.

При порушенні даного правила активний порт не закривається, а лише відсікає всі дії з певної MAC-адреси, яка і спричинила підозру про недотримання правил.

Наступним кроком вказуємо власне той час, протягом якого інформація про джерело стає вже не актуальною і можна підключити інший пристрій, не порушивши правило (рис. 4.2).

В даному випадку це значення дорівнює 1 (одна хвилина).

```
Switch(config-if)#int f0/2
Switch(config-if)#switchport port-security maximum 1
Switch(config-if)#switchport port-security violation restrict
Switch(config-if)#switchport port-security aging time 1
Switch(config-if)#
```

Рисунок 4.2 — Імплементація Port security на свічі «КОМ_Сер»

4.3 Реалізація безпеки на рівні корпоративної комп’ютерної мережі

Задля захисту цього рівня застосовується механізм SSH — захищений протокол, який використовує порт TCP 22. Він забезпечує захищене (або зашифроване) підключення до певного віддаленого пристрою. Він допомагає замінити Telnet для підключень до пристрою з метою керування. Забезпечує

безпеку віддалених підключень, надаючи послугу стійкого шифрування під час автентифікації пристрою (ім’я користувача та пароль), а також під час передавання даних між комунікаційними пристроями.

Спершу вводимо команду «ip ssh version 2» для використання останньої версії протоколу.

Встановлюємо «hostname» та назву домену.

```
Router(config)#hostname R1
R1(config)#ip domain-name vinnica.com
```

Згенеруємо відкритий та закритий ключі RSA.

```
R1(config)#crypto key generate rsa
```

Налаштовуємо локальне ім'я користувача, привілеї доступу та пароль (рис. 4.3).

```
R1(config)#service password-encryption
R1(config)#username bachelor privilege 15 password bachelor
R1(config)#aaa new-model
```

```
username bachelor privilege 15 password 7 08234D4D011C091800
!
!
license udi pid CISCO2911/K9 sn FTX15246VW4-
!
```

Рисунок 4.3 — Результат налаштування паролю та локального ім’я користувача на роутері «ЦЕНТР»

Далі потрібно ввімкнути доступ SSH до пристрою. Це робиться так:

```
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#logging synchronous
R1(config-line)#exec-timeout 60 0
```

R1(config-line)#exit

R1(config)#exit

Наступну команду *ssh -l bachelor 209.165.200.225* вводиться для перевірки правильності налаштування і зв'язку пристрою з роутером (рис. 4.4).

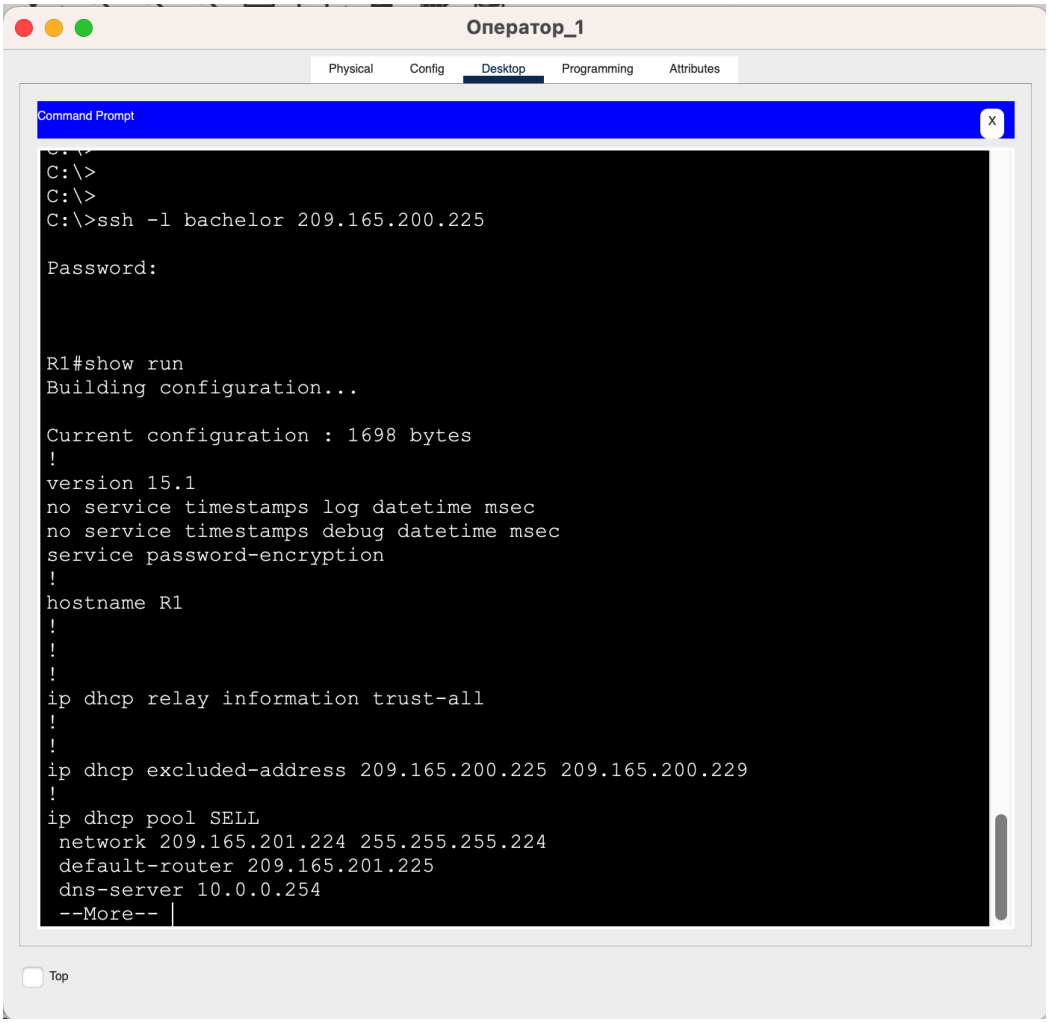


Рисунок 4.4 — Результат підключення пристрою по Shh до роутера «ЦЕНТР»

Для того щоб заборонити доступ інших пристроїв по ssh виконуються дії зображені на рисунках нижче за допомогою ACL (рис. 4.5 — 4.6).

```
!
access-list 130 permit tcp host 192.168.25.101 host 209.165.200.225 eq 22
access-list 130 deny tcp any any eq 22
access-list 130 permit ip any any
```

Рисунок 4.5 — Процес заборони доступу інших пристроїв по ssh

```
!
interface GigabitEthernet0/0
 ip address 10.0.0.1 255.255.255.0
 ip access-group 130 in
 duplex auto
 speed auto
```

```
!
interface GigabitEthernet0/2
 ip address 209.165.201.225 255.255.255.224
 ip access-group 130 in
 duplex auto
 speed auto
```

Рисунок 4.6 — Активація ACL на інтерфейсах

Також на даному рівні застосовуємо захист від SYN-атак шляхом імплементації механізму SYN-Protection. Зловмисники можуть використовувати мережеві порти для здійснення атак на пристрій/ої під час атаки «SYN», яка використовує ресурси TCP та потужність центрального процесора.

Першочергово трафік TCP до центрального процесора є обмеженим, але в випадку якщо один або кілька портів знаходяться під надсиланням великої кількості SYN-пакетів, процесор, в результаті, отримує лише пакети зловмисника з підробленої ip-адреси, створюючи таким чином ситуацію відмови в обслуговуванні для решти користувачів.

Щоб запобігти потенційній атаці такого типу, варто виконати такі дії.

Дозволити всі встановлені підключення через список керування доступом (ACL) за допомогою встановленого ключового слова established.

Встановлене ключове слово established вказує, що пакети належать до існуючого з’єднання, якщо дейтаграма протоколу керування передачею (TCP) має встановлений біт підтвердження (ACK) або скидання (RST).

Переконатись, що трафік системи доменних імен (DNS) (порт 53 протоколу дейтаграм користувача [UDP]) дозволено через ACL. В іншому

випадку користувачі не матимуть можливості переглядати мережу Інтернет за доменним іменем. Подібна логіка застосовується і в ситуації з DHCP (рис. 4.7).

```
R1(config)#access-list 140 permit udp any any eq 53
R1(config)#access-list 140 permit tcp any any eq 53
R1(config)#access-list 140 permit udp any any eq 67
R1(config)#access-list 140 permit udp any any eq 68
R1(config)#access-list 140 permit tcp any any established
R1(config)#
```

```
access-list 140 permit udp any any eq domain
access-list 140 permit tcp any any eq domain
access-list 140 permit udp any any eq bootps
access-list 140 permit udp any any eq bootpc
access-list 140 permit tcp any any established
!
```

Рисунок 4.7 — Створення ACL для запобігання SYN-атакам

Асоціювати список контролю доступом (ACL) з інтерфейсом (рис. 4.8).

```
R1(config)#int gi 0/1
R1(config-if)#ip access-group 140 out
R1(config-if)#
```

```
!
interface GigabitEthernet0/1
 ip address 209.165.200.225 255.255.255.224
 ip access-group 140 out
 duplex auto
 speed auto
!
```

Рисунок 4.8 — Активація ACL на інтерфейсах

4.4 Реалізація безпеки на службовому рівні

На даному рівні стеку імплементовано механізм захисту від атак «starvation DHCP» метою якої є створити відмову в обслуговуванні (DoS) для вже існуючих та потенційних клієнтів, які надсилають запити на здійснення тих чи інших дій.

Цим механізмом є впровадження «DHCP snooping». DHCP Snooping не покладається на вихідні MAC-адреси, а визначає, чи приходить повідомлення DHCP з адміністративно налаштованого довіреного або ж з ненадійного джерела. Потім цей механізм фільтрує повідомлення DHCP і обмежує швидкість трафіку DHCP [24] з ненадійних джерел. Для впровадження цього методу також необхідно налаштувати сервер DHCP і створити VLAN на свічі, прив'язавши його до інтерфейсів (рис. 4.9).

Процес налаштування серверу DHCP описаний в пункті 9 опису загальних налаштувань мережі, який розташований в пункті 3.2 даного розділу. Наступним кроком відбувається процес налаштування VLAN [23].

```
Switch(config)#vlan 10
Switch(config-vlan)#name student
Switch(config-vlan)#end
Switch(config)#int f0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#end
Switch(config)#int f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#end
Switch(config)#int g0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
```

```
Switch#sh vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/2
10   student                          active    Fa0/1, Fa0/2, Gig0/1
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Рисунок 4.9 — Створення VLAN

І вже фінально, відбувається налаштування безпосередньо DHCP Snooping (рис. 4.10 — 4.11).

```
Switch(config)#ip dhcp snooping
Switch(config)#int fa0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#int fa0/2
Switch(config-if)#ip dhcp snooping trust
Switch(config)#ip dhcp snooping vlan 10
Switch(config)#int g0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#ip dhcp snooping vlan 10
Router(config)#ip dhcp relay information trust-all
```

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping tr
Switch(config)#ip dhcp snooping tr
Switch(config)#ip dhcp snooping trust
                              ^
% Invalid input detected at '^' marker.

Switch(config)#int fa0/1
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#int fa0/2
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#ex
Switch(config)#ip dhcp snooping vlan 10
Switch(config)#
```

Рисунок 4.10 — Створення dhcp snooping

```
Switch#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
------------------------   -------    ----------------
FastEthernet0/1            yes        unlimited
FastEthernet0/2            yes        unlimited
GigabitEthernet0/1         yes        unlimited
```

Рисунок 4.11 — Підтвердження коректності налаштування dhcp snooping

4.5 Ефективність заходів безпеки

На кінцевому етапі тестування розробленої корпоративної комп’ютерної мережі, що створена для підтримки пристроїв та системи IoT було налаштовано певні методи захисту (або протоколи) які дають можливість додатково захистити процес передачі та обробки інформації. Це відбулось на

всіх 4-х рівнях ново запропонованого в даній роботі безпечного дизайну системи Internet Of Things.

Зокрема, на першому рівні — рівні датчиків було налаштовано аутентифікацію за допомогою технології WPA-PSK2 з режимом шифрування AES, а також запропоновано рішення для вирішення проблем фізичного доступу, актуальності програмного забезпечення та протидії «selfish»-загрозам. На другому рівні — рівні локальних інтерфейсів реалізовано механізм захисту на базі MAC-адрес, що запобігає несанкціонованому доступу зловмисників з неавторизованого пристрою, де фактична MAC-адреса відрізняється від санкціонованої. Імплементовано це було за допомогою технології Port Security. Третій рівень — рівень корпоративної комп'ютерної мережі. На ньому створено захист за допомогою механізму SSH — який є захищеним протоколом, що використовує порт TCP 22, який надає захищений канал підключення до певного пристрою на віддалі та допомагає замінити Telnet в цьому випадку. Та застосовано механізм захисту від SYN-атак — SYN-Protection. Останній четвертий рівень — службовий містить захист від атак «starvation DHCP» метою якої є створити відмову в обслуговуванні (DoS) за допомогою механізму «DHCP snooping». Цей механізм визначає з довіреного чи ні джерела надходить повідомлення DHCP. Після прийняття відповідного рішення, фільтрує повідомлення та обмежує трафік для ненадійного джерела інформації.

5 ЕКОНОМІЧНА ЧАСТИНА

5.1 Комерційний та технологічний аудит науково-технічної розробки

Метою даного розділу є проведення технологічного аудиту, в даному розробки моделі корпоративної мережі в програмному середовищі Packet Tracer з захистом у відповідності до запропонованого технологічного дизайну системи IoT. Метою дослідження є підвищення безпеки та захисту пристроїв Інтернету речей всередині корпоративної мережі від НСД. Це досягається за допомогою вдосконаленого технологічного дизайну системи IoT. Особливістю розробки є те, що розроблено безпековий технологічний дизайн системи IoT із урахуванням запропонованого рівня інтерфейсів, що надає подібність до принципів побудови сервіс-орієнтованої архітектури. Аналогом може бути розробки можуть бути Xiaomi Система розумний дім 17 829,00 грн. або адаптивна безпека Fortinet FortiSOAR для SOC-команд — 73 313,00 грн. Для проведення аудиту залучають не менше 3-х незалежних експертів. Оцінювання науково-технічного рівня розробки та її комерційного потенціалу рекомендується здійснювати із застосуванням 5-бальної системи оцінювання за 12-ма критеріями (табл. 5.1).

Таблиця 5.1 — Рекомендовані критерії оцінювання комерційного потенціалу розробки та їх можлива бальна оцінка

Бали (за 5-ти бальною шкалою)					
Критерій	0	1	2	3	4
Технічна здійсненність концепції					
1	Достовірність концепції не підтверджена	Концепція підтверджена експертними висновками	Концепція підтверджена розрахунками	Концепція перевірена на практиці	Перевірено роботоздатність продукту в реальних умовах

Продовження табл. 5.1

Ринкові переваги					
2	Багато аналогів на малому ринку	Мало аналогів на малому ринку	Кілька аналогів на великому ринку	Один аналог на великому ринку	Продукт не має аналогів на великому ринку
3	Ціна продукту значно вища за ціни аналогів	Ціна продукту дещо вища за ціни аналогів	Ціна продукту приблизно дорівнює цінам аналогів	Ціна продукту дещо нижче за ціни аналогів	Ціна продукту значно нижче за ціни аналогів
4	Технічні та споживчі властивості продукту значно гірші, ніж в аналогів	Технічні та споживчі властивості продукту трохи гірші, ніж в аналогів	Технічні та споживчі властивості продукту на рівні аналогів	Технічні та споживчі властивості продукту трохи кращі, ніж в аналогів	Технічні та споживчі властивості продукту значно кращі, ніж в аналогів
5	Експлуатаційні витрати значно вищі, ніж в аналогів	Експлуатаційні витрати дещо вищі, ніж в аналогів	Експлуатаційні витрати на рівні експлуатаційних витрат аналогів	Експлуатаційні витрати трохи нижчі, ніж в аналогів	Експлуатаційні витрати значно нижчі, ніж в аналогів
Ринкові перспективи					
6	Ринок малий і не має позитивної динаміки	Ринок малий, але має позитивну динаміку	Середній ринок з позитивною .	Великий стабільний ринок	Великий ринок з позитивною динамікою
7	Активна конкуренція великих компаній на ринку	Активна конкуренція	Помірна конкуренція	Незначна конкуренція	Конкурентів немає
Практик на здійсненність					
8	Відсутні фахівці як з технічної, так і з комерційної реалізації ідеї	Необхідно наймати фахівців або витрачати значні кошти та час на навчання наявних фахівців	Необхідне незначне навчання фахівців та збільшення їх штату	Необхідне незначне навчання фахівців	Є фахівці з питань як з технічної, так і з комерційної реалізації ідеї
9	Потрібні значні фінансові ресурси, які відсутні. Джерела фінансування ідеї відсутні	Потрібні незначні фінансові ресурси. Джерела фінансування відсутні	Потрібні значні фінансові ресурси. Джерела фінансування є	Потрібні незначні фінансові ресурси. Джерела фінансування є	Не потребує додаткового фінансування

Продовження табл. 5.1

10	Необхідна розробка нових матеріалів	Потрібні матеріали, що використовуються у військово-промисловому комплексі	Потрібні дорогі матеріали	Потрібні досяжні та дешеві матеріали	Всі матеріали для реалізації ідеї відомі та давно використовуються у виробництві
12	Необхідна розробка регламентних документів та отримання великої кількості дозвільних документів на виробництво та реалізацію продукту	Необхідно отримання великої кількості дозвільних документів на виробництво та реалізацію продукту, що вимагає значних коштів та часу	Процедура отримання дозвільних документів для виробництва та реалізації продукту вимагає незначних коштів та часу	Необхідно тільки повідомлення відповідним органам про виробництво та реалізацію продукту	Відсутні будь-які регламентні обмеження на виробництво та реалізацію продукту

Усі дані по кожному параметру занесено в таблиці 5.2

Таблиця 5.2 — Результати оцінювання комерційного потенціалу розробки

Критерії оцінювання	ПІБ експертів		
	Експерт 1	Експерт 2	Експерт 3
	Бали		
Технічна здійсненність концепції	3	3	4
Наявність аналогів на ринку	3	3	4
Цінова політика	3	4	3
Технічні та споживчі властивості виробу	4	3	4
Експлуатаційні витрати	3	4	3
Ринок збуту	4	3	4
Конкурентоспроможність	3	4	3
Фахівці з технічної і комерційної реалізації	4	3	4
Фінансування	4	4	3
Матеріально-технічна база	3	3	3
Термін реалізації ідеї	4	3	3
Супровідна документація	3	3	4
Сума	41	40	42
Середньоарифметична сума балів	(41+40+42) / 3 = 41		

За даними таблиці 5.2 можна зробити висновок щодо рівня комерційного потенціалу даної розробки. Для цього доцільно скористатись рекомендаціями, наведеними в таблиці 5.3.

Таблиця 5.3 — Рівні комерційного потенціалу розробки

Середньоарифметична сума балів, розрахована на основі висновків експертів	Рівень комерційного потенціалу розробки
0-10	Низький
11-20	Нижче середнього
21-30	Середній
31-40	Вище середнього
41-48	Високий

Як видно з таблиці, рівень комерційного потенціалу розроблюваного нового програмного продукту є високим, що досягається за рахунок підвищення безпеки та захисту пристроїв Інтернету речей всередині корпоративної мережі від несанкціонованого доступу. Особливістю розробки є те, що розроблено безпековий технологічний дизайн системи IoT із урахуванням запропонованого рівня інтерфейсів, що надає подібність до принципів побудови сервіс-орієнтованої архітектури.

5.2 Прогнозування витрат на виконання науково-дослідної (дослідно-конструкторської) роботи

5.2.1 Основна заробітна плата розробників, яка розраховується за формулою:

$$З_о = \frac{M}{T_р} \cdot t, \tag{5.1}$$

де М — місячний посадовий оклад конкретного розробника (дослідника), грн.;
$T_р$ — число робочих днів за місяць, 22 днів;
t — число днів роботи розробника (дослідника).

Результати розрахунків зведемо до таблиці 5.4.

Таблиця 5.4 — Основна заробітна плата розробників

Найменування посади	Місячний посадовий оклад, грн.	Оплата за робочий день, грн.	Число днів роботи	Витрати на заробітну плату, грн.
Керівник проекту	40000	1818,18	35	63636,364
Програміст	35000	1590,91	35	55681,818
Всього				119318,18

Так як в даному випадку розробляється програмний продукт, то розробник виступає одночасно і основним робітником, і тестувальником розроблюваного програмного продукту.

5.2.2 Додаткова заробітна плата розробників, які брати участь в розробці обладнання/програмного продукту.

Додаткову заробітну плату прийнято розраховувати як 15 % від основної заробітної плати розробників та робітників:

$$З_д = З_о \cdot 15\ \% / 100\ \% \qquad (5.2)$$

$$З_д = (119318{,}18 \cdot 15\ \% / 100\ \%) = 17897{,}73\ \text{(грн.)}$$

5.2.3 Нарахування на заробітну плату розробників.

Згідно діючого законодавства нарахування на заробітну плату складають 22 % від суми основної та додаткової заробітної плати.

$$Н_з = (З_о + З_д) \cdot 22\ \% / 100\% \qquad (5.3)$$

$$Н_з = (119318{,}18 + 17897{,}73) \cdot 22\ \% / 100\ \% = 30187{,}50\ \text{(грн.)}$$

5.2.4. Оскільки для розроблювального пристрою не потрібно витрачати матеріали та комплектуючи, то витрати на матеріали і комплектуючі дорівнюють нулю.

5.2.5 Амортизація обладнання, яке використовувалось для проведення розробки.

Амортизація обладнання, що використовувалось для розробки в спрощеному вигляді розраховується за формулою:

$$A = \frac{Ц}{Тв} \cdot \frac{t_{вик}}{12} \text{ [грн.].} \quad (5.4)$$

де Ц — балансова вартість обладнання, грн.;

Т — термін корисного використання обладнання згідно податкового законодавства, років;

$t_{вик}$ — термін використання під час розробки, місяців.

Розрахуємо, для прикладу, амортизаційні витрати на комп'ютер балансова вартість якого становить 21000 грн., термін його корисного використання згідно податкового законодавства – 2 роки, а термін його фактичного використання – 1,59 міс.

$$A_{обл} = \frac{21000}{2} \times \frac{1{,}59}{12} = 1392{,}045 \ грн.$$

Аналогічно визначаємо амортизаційні витрати на інше обладнання та приміщення. Розрахунки заносимо до таблиці 5.5. Так як вартість ліцензійної ОС та спеціалізованих ліцензійних нематеріальних ресурсів менше 20000 грн, то даний нематеріальний актив не амортизується, а його вартість включається у вартість розробки повністю, $B_{нем.ак.}$ = 10000 грн (Microsoft Windows 10 — 10000 грн. + Packet Tracer (від компанії CISCO — безкоштовно).

Таблиця 5.5 — Амортизаційні відрахування на матеріальні та нематеріальні ресурси для розробників

Найменування обладнання	Балансова вартість, грн.	Строк корисного використання, років	Термін використання обладнання, місяців	Амортиза-ційні відрахуван-ня, грн.
Комп'ютер та комп'ютерна периферія	21000	2	1,59	1392,045
Офісне обладнання (меблі)	30000	4	1,59	994,318
Приміщення	900000	20	1,59	5965,909
Всього				8352,27

5.2.6 Тарифи на електроенергію для непобутових споживачів (промислових підприємств) відрізняються від тарифів на електроенергію для населення. При цьому тарифи на розподіл електроенергії у різних постачальників (енергорозподільних компаній), будуть різними. Крім того, розмір тарифу залежить від класу напруги (1-й або 2-й клас). Тарифи на розподіл електроенергії для всіх енергорозподільних компаній встановлює Національна комісія з регулювання енергетики і комунальних послуг (НКРЕКП). Витрати на силову електроенергію розраховуються за формулою:

$$В_е = В \cdot П \cdot Ф \cdot К_п, \qquad (5.5)$$

де В – вартість 1 кВт-години електроенергії для 1 класу підприємства, В = 6,2 грн./кВт;

П – встановлена потужність обладнання, кВт. П = 0,4 кВт;

Ф – фактична кількість годин роботи обладнання, годин;

$К_п$ – коефіцієнт використання потужності, $К_п$ = 0,9.

$$В_е = 0,9 \cdot 0,4 \cdot 8 \cdot 35 \cdot 6,2 = 624,96 \text{ (грн.)}$$

5.2.7 Інші витрати та загальновиробничі витрати.

До статті «Інші витрати» належать витрати, які не знайшли відображення у зазначених статтях витрат і можуть бути віднесені безпосередньо на собівартість досліджень за прямими ознаками. Витрати за статтею «Інші витрати» розраховуються як 50…100% від суми основної заробітної плати дослідників:

$$I_в = (З_о + З_р) \cdot \frac{Н_{ів}}{100\%}, \quad (5.6)$$

де $Н_{ів}$ — норма нарахування за статтею «Інші витрати».

$$I_в = 119318{,}18 * 90\% / 100\% = 107386{,}4 \text{ (грн.)}$$

До статті «Накладні (загальновиробничі) витрати» належать: витрати, пов’язані з управлінням організацією; витрати на винахідництво та раціоналізацію; витрати на підготовку (перепідготовку) та навчання кадрів; витрати, пов’язані з набором робочої сили; витрати на оплату послуг банків; витрати, пов’язані з освоєнням виробництва продукції; витрати на науково-технічну інформацію та рекламу та ін. Витрати за статтею «Накладні (загальновиробничі) витрати» розраховуються як 100…150% від суми основної заробітної плати дослідників:

$$Н_{нзв} = (З_о + З_р) \cdot \frac{Н_{нзв}}{100\%}, \quad (5.7)$$

де $Н_{нзв}$ — норма нарахування за статтею «Накладні (загальновиробничі) витрати».

$$Н_{нзв} = 119318{,}18 * 135\ \% / 100\ \% = 161080 \text{ (грн.)}$$

5.2.9 Витрати на проведення науково-дослідної роботи.

Сума всіх попередніх статей витрат дає загальні витрати на проведення науково-дослідної роботи:

$B_{заг}$ = 119318,18+17897,73+30187,50+8352,27+10000+624,96+107386,4+ +161080 = 454846,55 грн.

5.2.10 Розрахунок загальних витрат на науково-дослідну (науково-технічну) роботу та оформлення її результатів.

Загальні витрати на завершення науково-дослідної (науково-технічної) роботи та оформлення її результатів розраховуються за формулою:

$$ЗВ = \frac{B_{заг}}{\eta} \text{ (грн)}, \quad (5.8)$$

де η — коефіцієнт, який характеризує етап (стадію) виконання науково-дослідної роботи.

Так, якщо науково-технічна розробка знаходиться на стадії: науково-дослідних робіт, то η=0,1; технічного проектування, то η=0,2; розробки конструкторської документації, то η=0,3; розробки технологій, то η=0,4; розробки дослідного зразка, то η=0,5; розробки промислового зразка, то η=0,7; впровадження, то η=0,9. Оберемо η = 0,5, так як розробка, на даний момент, знаходиться на стадії дослідного зразка:

$$ЗВ = 454846,55 / 0,5 = 909693 \text{ грн.}$$

5.3 Розрахунок економічної ефективності науково-технічної розробки за її можливої комерціалізації потенційним інвестором

В ринкових умовах узагальнювальним позитивним результатом, що його може отримати потенційний інвестор від можливого впровадження результатів тієї чи іншої науково-технічної розробки, є збільшення у

потенційного інвестора величини чистого прибутку. Саме зростання чистого прибутку забезпечить потенційному інвестору надходження додаткових коштів, дозволить покращити фінансові результати його діяльності, підвищить конкурентоспроможність та може позитивно вплинути на ухвалення рішення щодо комерціалізації цієї розробки.

Для того, щоб розрахувати можливе зростання чистого прибутку у потенційного інвестора від можливого впровадження науково-технічної розробки необхідно:

— вказати, з якого часу можуть бути впроваджені результати науково-технічної розробки;

— зазначити, протягом скількох років після впровадження цієї науково-технічної розробки очікуються основні позитивні результати для потенційного інвестора (наприклад, протягом 3-х років після її впровадження);

— кількісно оцінити величину існуючого та майбутнього попиту на цю або аналогічні чи подібні науково-технічні розробки та назвати основних суб’єктів (зацікавлених осіб) цього попиту;

— визначити ціну реалізації на ринку науково-технічних розробок з аналогічними чи подібними функціями.

При розрахунку економічної ефективності потрібно обов’язково враховувати зміну вартості грошей у часі, оскільки від вкладення інвестицій до отримання прибутку минає чимало часу. При оцінюванні ефективності інноваційних проектів передбачається розрахунок таких важливих показників:

— абсолютного економічного ефекту (чистого дисконтованого доходу);

— внутрішньої економічної дохідності (внутрішньої норми дохідності);

— терміну окупності (дисконтованого терміну окупності).

Аналізуючи напрямки проведення науково-технічних розробок, розрахунок економічної ефективності науково-технічної розробки за її можливої комерціалізації потенційним інвестором можна об’єднати, враховуючи визначені ситуації з відповідними умовами.

5.3.1 Розробка чи суттєве вдосконалення програмного засобу (програмного забезпечення, програмного продукту) для використання масовим споживачем.

В цьому випадку майбутній економічний ефект буде формуватися на основі таких даних:

$$\Delta П_i = (\pm \Delta Ц_0 \cdot N + Ц_0 \cdot \Delta N)_i \cdot \lambda \cdot \rho \cdot (1 - \frac{\vartheta}{100}), \quad (5.9)$$

де $\pm\Delta Ц_o$ — зміна вартості програмного продукту (зростання чи зниження) від впровадження результатів науково-технічної розробки в аналізовані періоди часу;

N — кількість споживачів які використовували аналогічний продукт у році до впровадження результатів нової науково-технічної розробки;

$Ц_o$ — основний оціночний показник, який визначає діяльність підприємства у даному році після впровадження результатів наукової розробки, $Ц_o = Ц_б \pm \Delta Ц_o$;

$Цб$ — вартість програмного продукту у році до впровадження результатів розробки;

ΔN — збільшення кількості споживачів продукту, в аналізовані періоди часу, від покращення його певних характеристик;

λ — коефіцієнт, який враховує сплату податку на додану вартість. Ставка податку на додану вартість дорівнює 20%, а коефіцієнт $\lambda = 0{,}8333$;

p — коефіцієнт, який враховує рентабельність продукту;

ϑ — ставка податку на прибуток, у 2023 році ϑ =18%.

Припустимо, що при прогнозованій ціні 7500 грн. за одиницю виробу, термін збільшення прибутку складе 3 роки. Після завершення розробки і її вдосконалення, можна буде підняти її ціну на *500* грн. Кількість одиниць реалізованої продукції також збільшиться: протягом першого року — на 1500 шт., протягом другого року – на 1800 шт., протягом третього року на 2000 шт. До моменту впровадження результатів наукової розробки реалізації продукту не було:

$$\Delta П_1 = (0*500 + (7500 + 500)*1500)* 0{,}8333* 0{,}45) * (1 - 0{,}18) = 3459374{,}862 \text{ грн.}$$

$$\Delta П_2 = (0*500 + (7500 + 500)*(1500+1800)* 0{,}8333* 0{,}45) * (1 - 0{,}18) = 8117999{,}675 \text{ грн.}$$

$$\Delta П_3 = (0*500 + (7500 + 500)*(1500+1800+2000)* 0{,}8333* 0{,}45) * (1 - 0{,}18) = 13037999{,}478 \text{ грн.}$$

Отже, комерційний ефект від реалізації результатів розробки за три роки складе 24615374,02 грн.

5.3.2 Розрахунок ефективності вкладених інвестицій та періоду їх окупності.

Розраховуємо приведену вартість збільшення всіх чистих прибутків *ПП*, що їх може отримати потенційний інвестор від можливого впровадження та комерціалізації науково-технічної розробки:

$$ПП = \sum_{1}^{T} \frac{\Delta П_i}{(1+\tau)^t}, \qquad (5.10)$$

де $\Delta П_i$ — збільшення чистого прибутку у кожному із років, протягом яких виявляються результати виконаної та впровадженої науково-дослідної (науково-технічної) роботи, грн;

Т — період часу, протягом якою виявляються результати впровадженої науково-дослідної (науково-технічної) роботи, роки;

τ — ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні, $\tau = 0,05...0,15$;

t — період часу (в роках).

Збільшення прибутку ми отримаємо, починаючи з першого року:

$$ПП = (3459374,862/(1+0,1)^1)+(8117999,675/(1+0,1)^2)+(13037999,478/$$
$$/(1+0,1)^3) = 3144886,24 + 6709090,641 + 9795641,982 = 19649618,86 \text{ грн.}$$

Далі розраховують величину початкових інвестицій *PV*, які потенційний інвестор має вкласти для впровадження і комерціалізації науково-технічної розробки. Для цього можна використати формулу:

$$PV = k_{інв} * ЗВ, \quad (5.11)$$

де $k_{інв}$ — коефіцієнт, що враховує витрати інвестора на впровадження науково-технічної розробки та її комерціалізацію. Це можуть бути витрати на підготовку приміщень, розробку технологій, навчання персоналу, маркетингові заходи тощо; зазвичай $k_{інв}=2...5$, але може бути і більшим;

ЗВ — загальні витрати на проведення науково-технічної розробки та оформлення її результатів, грн.

$$PV = 2 * 909693 = 1819386,20 \text{ грн.}$$

Тоді абсолютний економічний ефект $E_{абс}$ або чистий приведений дохід *(NPV, Net Present Value)* для потенційного інвестора від можливого впровадження та комерціалізації науково-технічної розробки становитиме:

$$E_{абс} = ПП - PV, \quad (5.12)$$

$$E_{абс} = 19649618,86 - 1819386,20 = 17830232,66 \text{ грн.}$$

Оскільки $E_{абс} > 0$ то вкладання коштів на виконання та впровадження результатів даної науково-дослідної (науково-технічної) роботи може бути доцільним.

Для остаточного прийняття рішення з цього питання необхідно розрахувати внутрішню економічну дохідність або показник внутрішньої норми дохідності (IRR, Internal Rate of Return) вкладених інвестицій та порівняти її з так званою бар'єрною ставкою дисконтування, яка визначає ту мінімальну внутрішню економічну дохідність, нижче якої інвестиції в будь-яку науково-технічну розробку вкладати буде економічно недоцільно.

Розрахуємо відносну (щорічну) ефективність вкладених в наукову розробку інвестицій $E_в$. Для цього використаємо формулу:

$$E_в = \sqrt[T_ж]{1 + \frac{E_{абс}}{PV}} - 1, \tag{5.13}$$

$T_ж$ — життєвий цикл наукової розробки, роки.

$$E_в = \sqrt[3]{(1 + 17830232{,}66/1819386{,}20} - 1 = 1{,}210$$

Визначимо мінімальну ставку дисконтування, яка у загальному вигляді визначається за формулою:

$$\tau = d + f, \tag{5.14}$$

де d — середньозважена ставка за депозитними операціями в комерційних банках; в 2023 році в Україні d = (0,09…0,14);

f — показник, що характеризує ризикованість вкладень; зазвичай, величина f = (0,05...0,5).

$$\tau_{\min} = 0{,}14 + 0{,}05 = 0{,}19.$$

Так як $E_в > \tau_{min}$, то інвестор може бути зацікавлений у фінансуванні даної наукової розробки.

Розрахуємо термін окупності вкладених у реалізацію наукового проекту інвестицій за формулою:

$$T_{ок} = \frac{1}{E_в}, \tag{5.15}$$

$$T_{ок} = 1 / 1{,}210 = 0{,}83 \text{ р.}$$

Оскільки $T_{ок}$ < 3-х років, а саме термін окупності рівний 0,83 роки, то фінансування даної наукової розробки є доцільним.

ВИСНОВКИ

Потреба у аналізі та покращення захисту IoT в корпоративній комп'ютерній мережі стало підставою для написання даної магістерської роботи.

У даній магістерській роботі досягнуто підвищення безпеки та захисту пристроїв Internet Of Things всередині корпоративної комп'ютерної мережі від несанкціонованого доступу за допомогою вдосконаленого технологічного дизайну системи IoT.

Отже, було проведено аналіз існуючих програмних та протокольних рішень для обгрунтування забезпечення роботи запропонованого розширеного технологічного дизайну системи IoT. В результаті цього аналізу, було впроваджено відповідні сучасні технології в чотирирівневий дизайн системи IoT. Був наданий опис кожного рівня запропонованого розширеного технологічного дизайну системи IoT та припасували його структуру до стандартів відомих моделі OSI та протокольного стеку TCP/IP. Додатково, була створена модель безпечного дизайну системи Internet Of Things, із врахуванням компонентів та функцій на кожному рівні безпеки, і відобразили потенційні атаки, проблеми та вимоги щодо безпеки.

Описано підготовку до організації захисту мережі за 4-рівневим технологічним дизайном Internet Of Things. Виокремлення базових понять під час організації захисту дозволило підготуватися до вибору обладнання відповідно об'єктам захисту та реалізувати ключові етапи налаштування мережі.

В результаті аналітичного дослідження вдалося проаналізувати архітектуру і ключові компоненти екосистеми Internet Of Things та особливості роботи технології IoT з точки зору взаємодії, обробки даних та розподілу інформації в системах IoT і виконати грунтовний аналіз загроз інформаційній безпеці IoT. Внаслідок вдалося спроектувати 4-рівневий технологічний дизайн

системи Internet Of Things із урахуванням запропонованого рівня інтерфейсів, що надає подібність до принципів побудови сервіс-орієнтованої архітектури.

Запропоновано розподіл загроз безпеці по рівням технологічного дизайну системи Internet Of Things та вмонтовано цю ідею в модель безпечного дизайну системи Internet Of Things урахуванням 4-рівневого дизайну системи Internet Of Things. В результаті спроектовано модель корпоративної комп'ютерної мережі в програмному середовищі Packet Tracer з захистом у відповідності до запропонованого технологічного дизайну системи IoT.

Економічна частина даної роботи містить розрахунок витрат на розробку нового програмного продукту, сума яких складає 909693 гривень. Було спрогнозовано орієнтовану величину витрат по кожній з статей витрат. Також розраховано чистий прибуток, який може отримати виробник від реалізації нового технічного рішення, розраховано період окупності витрат для інвестора та економічний ефект при використанні даної розробки. В результаті аналізу розрахунків можна зробити висновок, що розроблений програмний продукт за ціною дешевший за аналог і є висококонкурентоспроможним. Період окупності складе близько 0,83 роки.

Наукова новизна полягає у такому:

— вдосконалена відома трирівнева модель системи Internet Of Things за рахунок приведення її до архітектури IoT від CISCO, що надає новій архітектурі подібність до принципів побудови сервіс-орієнтованої архітектури (SOA);

— запропоновано розширений технологічний дизайн системи IoT, що містить такі рівні: датчиків, локальних інтерфейсів, корпоративної комп'ютерної мережі та службовий і це дає можливість поглибити безпекові аспекти в контексті IoT;

— розширено методологічну базу методів та засобів захисту IoT в межах корпоративної комп’ютерної мережі за рахунок приведення технологічного дизайну системи Internet Of Things до відомих стандартів;

— розширено методологічну базу методів та засобів захисту IoT в межах корпоративної комп’ютерної мережі за рахунок розподілу загроз безпеці по рівням технологічного дизайну системи IoT;

— запропоновано вдосконалену модель безпечного дизайну системи Internet Of Things.

Практична цінність полягає у такому:

— розроблено прототип корпоративної комп’ютерної мережі в програмному середовищі Packet Tracer (від компанії CISCO), яка враховує безпекові аспекти запропонованого технологічного дизайну системи IoT.

Особистий внесок студента полягає у розширенні методологічної бази методів та засобів захисту IoT в межах корпоративної комп’ютерної мережі, що може стати поштовхом для подальшого удосконалення процесів захисту елементів IoT в корпоративній комп’ютерній мережі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1) Сайт компанії IBM [Електронний ресурс] – Режим доступу: https://www.ibm.com/cloud/internet-of-things?mhsrc=ibmsearch_a&mhq=iot.

2) Сайт компанії Intel [Електронний ресурс] – Режим доступу: https://www.intel.com/content/www/us/en/internet-of-things/overview.html.

3) Сайт компанії Google [Електронний ресурс] – Режим доступу: https://cloud.google.com/iot-core.

4) Сайт компанії Cisco [Електронний ресурс] – Режим доступу: https://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html.

5) Сайт компанії Microsoft [Електронний ресурс] – Режим доступу: https://azure.microsoft.com/en-us/services/iot-central/.

6) Сайт компанії Amazon [Електронний ресурс] – Режим доступу: https://aws.amazon.com/iot-core/.

7) Сайт компанії Siemens [Електронний ресурс] – Режим доступу: https://new.siemens.com/global/en/products/automation/topic-areas/industrial-iot.html.

8) Цифрова трансформація бізнесу / Інтернет речей [Електронний ресурс] – Режим доступу: https://www.it.ua/knowledge-base/technology-innovation/internet-veschej-internet-of-things-iotXXX.

9) Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року, (GDPR) [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text.

10) Introduction to IoT. [Електронний ресурс] – Режим доступу: https://lms.netacad.com/course/view.php?id=744659.

11) Технології інтернету речей. Навчальний посібник [Електронний ресурс]: навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології», спеціалізація «Інформаційне забезпечення робототехнічних систем» / Б. Ю. Жураковський, І.О. Зенів; КПІ ім. Ігоря Сікорського. –

Електронні текстові дані (1 файл: 12,5Мбайт). – Київ: КПІім. Ігоря Сікорського, 2021. – 271 с.

12) Комп'ютерні мережі: навчальний посібник / Т. І. Коробейнікова, С. М. Захарченко. – Львів: Видавництво Львівської політехніки (НУЛП), 2022. – 228 с.

13) Технології захисту локальних мереж на основі обладнання CISCO : навч. посібник / Т. І. Коробейнікова, С. М. Захарченко. – Львів: Видавництво Львівської політехніки (НУЛП), 2021. 232 с.

14) Литвиненко Д. С. Модель безпеки інформаційної системи на базі технологій IoT : пояснювальна записка до кваліфікаційної роботи здобувача вищої освіти на другому (магістерському) рівні, спеціальність 123 Комп’ютерна інженерія / Д. С. Литвиненко ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків, 2021. – 81 с.

15) Jing, Qi & Vasilakos, Athanasios & Wan, Jiafu & Lu, Jingwei & Qiu, Dechao. (2014). Security of the Internet of Things: Perspectives and challenges. Wireless Networks. 20. 2481-2501. 10.1007/s11276-014-0761-7.

16) Побудова захищених мереж на базі обладнання компанії Cisco. // Захарченко С.М., Трояновська Т. І., Бойко О.В. Навчальний посібник. Вінниця : ВНТУ, 2017. – 133 с.

17) Бобовніков.Є. Методи безпеки даних та пристроїв інтернету речей : дипломна робота здобувача вищої освіти на першому (бакалаврському) рівні, спеціальність 125 Кібербезпека / В. Є. Бобовніков ; М-во освіти і науки України, Київ. нац. авіаційний університет. – Київ, 2021. – 60 с.

18) Інтернет речей: мережева архітектура та архітектура безпеки [Електронний ресурс] – Режим доступу до ресурсу: https://www.bizmaster.xyz/2020/12/internet-rechei-merezheva-arkhitektura-ta-arkhitektura-bezpeky.html.

19) Литвиненко Д. С. Модель безпеки інформаційної системи на базі технологій IoT : пояснювальна записка до кваліфікаційної роботи здобувача

вищої освіти на другому (магістерському) рівні, спеціальність 123 Комп’ютерна інженерія / Д. С. Литвиненко ; М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. – Харків, 2021. – 81 с.

20) Савицька Л.А., Коробейнікова Т.І. Удосконалений метод розробки API підвищеної швидкодії Інформаційні технології та комп`ютерна інженерія 2021: - №1 (50). - С. 31–35.

21) Савицька Л. А. Програмний модуль попереднього діагностування пацієнтів на основі нейронної мережі Кохонена [Текст] / Л. А. Савицька, Н. В. Добровольська, В. О. Кондратюк // Інформаційні технології та комп`ютерна інженерія. – 2023. – № 1. – С. 66-74.

22) ЗАСОБИ ЗАХИСТУ INTERNET OF THINGS В КОРПОРАТИВНІЙ КОМП’ЮТЕРНІЙ МЕРЕЖІ [Текст] / Савицька, Т.І. Коробейнікова, О.І. Костюк, І. С. Колесник // Інформаційні технології та комп`ютерна інженерія. – 2023. – № 2. – С. 61-70.

ДОДАТОК А

Технічне завдання

Міністерство освіти і науки України
Вінницький національний технічний університет
Факультет інформаційних технологій та комп’ютерної інженерії
Кафедра обчислювальної техніки

ЗАТВЕРДЖУЮ
Завідувач кафедри ОТ
проф., д.т.н.. Азаров О.Д..
“29” вересня 2023 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання магістерської кваліфікаційної роботи
“Розподілена система з підтримки функціонування автопаркінгу”
08-54.МКР.029.00.000 ПЗ

Науковий керівник: к.т.н., доцент каф.ОТ
_____ Савицька Л. А.
Студент групи 2КІ-22м
_____ Костюк . О. В

ВНТУ 2023

1. Підстава для виконання магістерської кваліфікаційної роботи (МКР)

1.1 Актуальність роботи полягає у проведенні аналізу та покращенні захисту IoT в корпоративних комп’ютерних мережах у зв’язку із експоненційним зростанням кількості пристроїв підключених до інтернету, що створює значні ризики для безпеки інформації, яка обробляється, передається та зберігається цими пристроями.

1.2 Наказ № 247 від 18.09.2023.

2. Мета МКР і призначення розробки

2.1 Мета роботи — підвищення безпеки та захисту пристроїв Internet Of Things всередині корпоративної комп’ютерної мережі від несанкціонованого доступу.

2.2 Призначення розробки — визначається потребою у розробці системи, спрямованої на підвищення рівня безпеки та захисту пристроїв Internet of Things в корпоративній комп'ютерній мережі, запобігаючи несанкціонованому доступу.

3. Вихідні дані для виконання МКР

3.1 Огляд ключових проблем та загроз безпеці пристроїв в корпоративних мережах IoT.

3.2 Вивчення методів та засобів захисту IoT-пристроїв у корпоративному середовищі..

3.4 Проведення перевірки та аналізу отриманих результатів.

3.5 Виконання економічних розрахунків для оцінки доцільності впровадження нової розробки.

4. Вимоги до виконання МКР

Головна вимога — підвищення безпеки та захисту пристроїв Internet Of Things всередині корпоративної комп’ютерної мережі.

5. Етапи МКР та очікувані результати

Етапи роботи та очікувані результати приведено в Таблиці А.1.

Таблиця А.1 — Етапи МКР

№ етапу	Назва етапу	Термін виконання		Очікувані результати
		початок	кінець	
1	Актуальний стан справ у сфері Internet of Things	19.09.2023	28.09.2023	Розділ 1
2	Технологічний дизайн системи iot	5.10.2023	10.10.2023	Розділ 2
3	Організація мережі за 4-рівневим технологічним дизайном Internet of Things	12.10.2023	18.10.2023	Розділ 3
4	Практична реалізація захисту за моделлю безпечного дизайну системи Internet of Things	20.10.2023	23.10.2023	Розділ 4
4	Підготовка економічної частини	2.11.2023	11.11.2023	Розділ 5
5	Оформлення пояснювальної записки, графічного матеріалу і презентації	13.11.2023	20.11.2023	ПЗ, графічний матеріал і презентація
6	Апробація та впровадження результатів дослідження	1.12.2023	8.12.2023	Тези доповідей
7	Підготовка і підпис супроводжуючих документів, нормоконтроль та тест на плагіат	8.12.2023	11.12.2023	Оформленні документи

6. Матеріали, що подаються до захисту МКР

До захисту подаються: пояснювальна записка МКР, графічні і ілюстративні матеріали, протокол попереднього захисту МКР на кафедрі, відгук наукового керівника, відгук опонента, протоколи складання державних екзаменів, анотації до МКР українською та іноземною мовами.

7. Порядок контролю виконання та захисту МКР

Виконання етапів графічної та розрахункової документації МКР контролюється науковим керівником згідно зі встановленими термінами. Захист МКР відбувається на засіданні Екзаменаційної комісії, затвердженої наказом ректора.

8. Вимоги до оформлювання та порядок виконання МКР

8.1 При оформлюванні МКР використовуються:

— ДСТУ 3008: 2015 «Звіти в сфері науки і техніки. Структура та правила оформлювання»;

— ДСТУ 8302: 2015 «Бібліографічні посилання. Загальні положення та правила складання»;

— ГОСТ 2.104–2006 «Єдина система конструкторської документації. Основні написи»;

— методичні вказівки до виконання магістерських кваліфікаційних робіт зі спеціальності 123 — «Комп’ютерна інженерія»;

— документи на які посилаються у вище вказаних.

8.2 Порядок виконання МКР викладено в «Положення про кваліфікаційні роботи на другому (магістерському) рівні вищої освіти СУЯ ВНТУ–03.02.02 П.001.01:21

ДОДАТОК Б

Загальна схема мережі

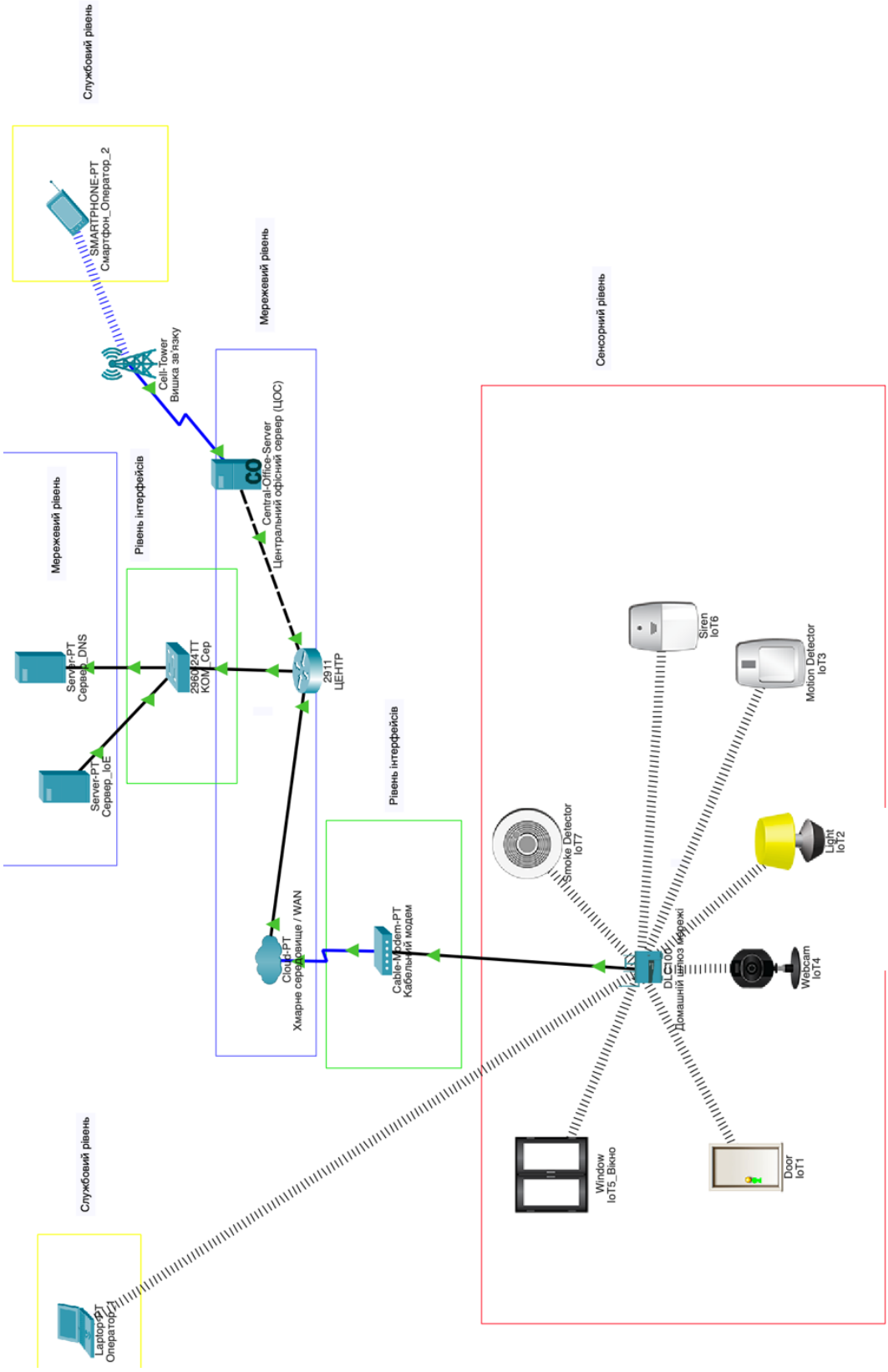
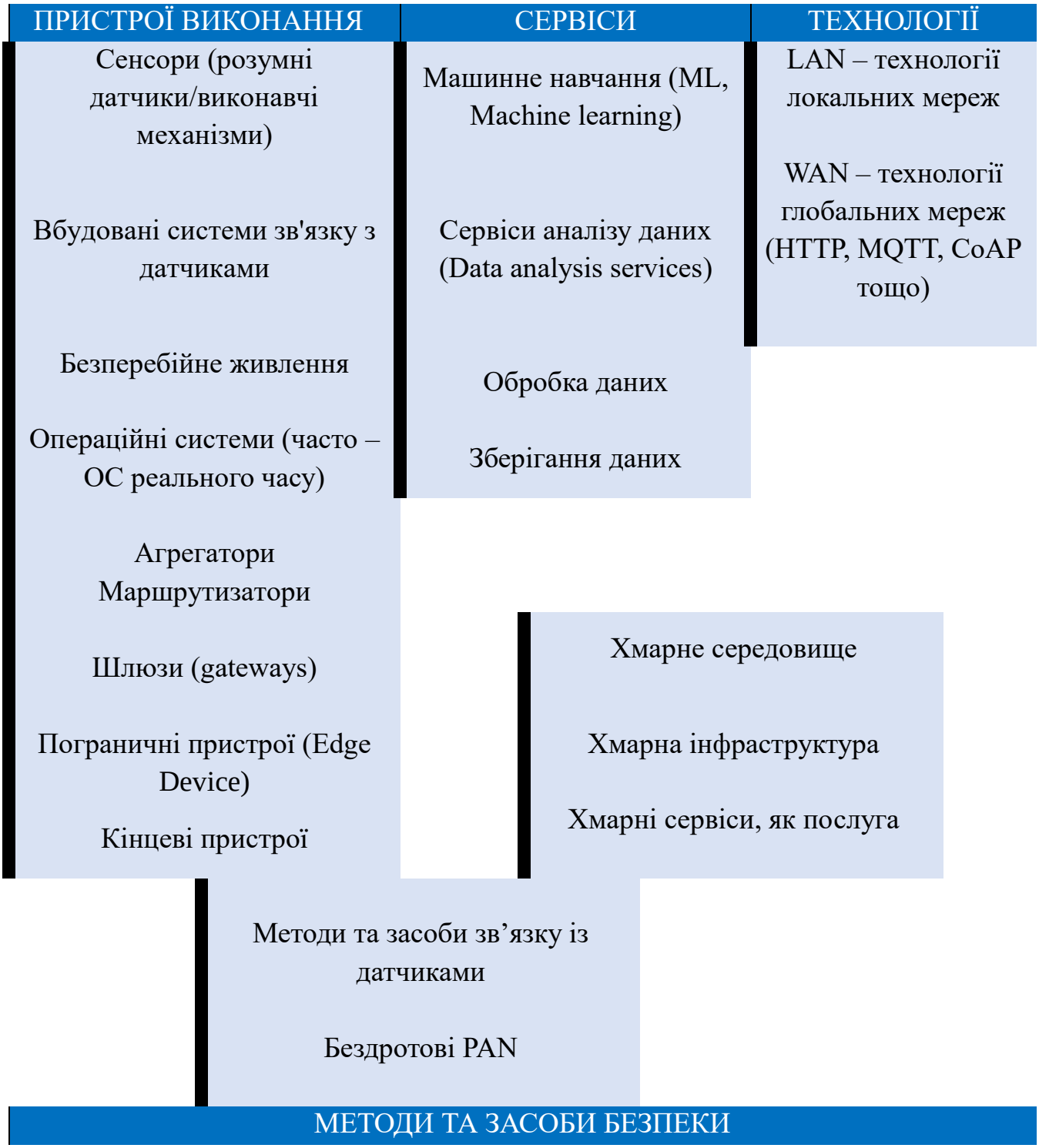


Рисунок Б.1 — загальна схема мережі

ДОДАТОК В

Розроблений безпековий технологічний дизайн системи Internet Of Things



Таблиця В.1 — розроблений безпековий технологічний дизайн системи Internet Of Things

ДОДАТОК Г

Розроблена модель безпечного дизайну системи Internet Of Things

OSI	TCP/IP	ДИЗАЙН IOT	ОБ'ЄКТ ЗАХИСТУ (ПРОТОКОЛ, ТЕХНОЛОГІЯ, ТОЩО)	МЕТОД ЗАХИСТУ	ОПИС
7 6 5	Додатків	СЛУЖБОВИЙ РІВЕНЬ	DHCP, SSH, CoAP, AMQP, XMPP, masquerad	DHCP snooping, RSA, ACL, IPS, брандмауер, шифрування,	Хмарні послуги, сервіси аналізу даних, машинне навчання, зв'язок з пристроями (частково), безпека додатків
4	Транспортний	РІВЕНЬ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ	DDoS, DoS, IPv4, IPv6, MQTT та DDS, TLS / SSL, MITM, TCP, UDP	SYN protection, 6LowPAN,	Зв'язок з пристроями, провідні та безпровідні мережі, протоколи передавання даних (частково), корпоративні мережні пристрої (частково)
3	Інтернету				
2	Мережевого доступу	РІВЕНЬ ЛОКАЛЬНИХ ІНТЕРФЕЙСІ	MAC, MIM, DNS, ARP, Адресні spoofing, STP, RFID, WSN, PKI, VLAN	PortSecurity, DAI, BPDU Guard IPSG, PortFast	Мережні пристрої (частково), протоколи передавання даних (частково), міжплатформне ПЗ
1		РІВЕНЬ ДАТЧИКІВ	selfish загроза, фізична безпека, порушення цілісності даних, зловмисне ПЗ	IPsec, IEEE 802.11 AH	Датчики, безперебійне живлення, ОС реального часу, безпека, GPS, Bluetooth

Таблиця Г.1 — розроблена модель безпечного дизайну системи Internet Of Things

ДОДАТОК Д

Конфігураційні файли ключових пристроїв

Роутер «ЦЕНТР»:

```
R1>en
R1#sh run
Building configuration...

Current configuration : 1653 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R1

!
ip dhcp relay information trust-all

ip dhcp excluded-address 209.165.200.225 209.165.200.229
!
ip dhcp pool SELL
network 209.165.201.224 255.255.255.224
default-router 209.165.201.225
dns-server 10.0.0.254
ip dhcp pool IOT
network 209.165.200.224 255.255.255.224
default-router 209.165.200.225
dns-server 10.0.0.254
aaa new-model
ip cef
no ipv6 cef
!
username bachelor privilege 15 password 7 08234D4D011C091800
license udi pid CISCO2911/K9 sn FTX15246VW4-
!
ip ssh version 2
ip domain-name nulp.com
spanning-tree mode pvst
interface GigabitEthernet0/0
ip address 10.0.0.1 255.255.255.0
ip access-group 130 in
duplex auto
speed auto
```

```
!
interface GigabitEthernet0/1
ip address 209.165.200.225 255.255.255.224
ip access-group 140 out
duplex auto
speed auto
!
interface GigabitEthernet0/2
ip address 209.165.201.225 255.255.255.224
ip access-group 130 in
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
router rip
!
ip classless
!
ip flow-export version 9

access-list 130 permit tcp host 192.168.25.101 host 209.165.200.225 eq 22
access-list 130 deny tcp any any eq 22
access-list 130 permit ip any any
access-list 140 permit udp any any eq domain
access-list 140 permit udp any any eq bootps
access-list 140 permit udp any any eq bootpc
access-list 140 permit tcp any any established
!
line con 0
!
line aux 0
!
line vty 0 4
exec-timeout 60 0
logging synchronous
transport input ssh

!
end
R1#
```

Свіч «КОМ_Сер»:

```
Switch>en
Switch#sh run
Building configuration...

Current configuration : 1647 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
ip dhcp snooping vlan 10
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
interface FastEthernet0/1
switchport access vlan 10
ip dhcp snooping trust
switchport mode access
switchport port-security violation restrict
switchport port-security aging time 1
spanning-tree bpduguard enable
!
interface FastEthernet0/2
switchport access vlan 10
ip dhcp snooping trust
switchport mode access
switchport port-security violation restrict
switchport port-security aging time 1
spanning-tree bpduguard enable
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
```

```
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
switchport access vlan 10
ip arp inspection trust
ip dhcp snooping trust
switchport mode access
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
shutdown
!
```

```
line con 0
!
line vty 0 4
login
line vty 5 15
login
!
end
Switch#
```

ДОДАТОК Е

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Засоби захисту internet of things в корпоративній Комп'ютерній мережі

Тип роботи: магістерська кваліфікаційна робота
(БДР, МКР)

Підрозділ кафедра обчислювальної техніки
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 91,4% Схожість 8,6%

Аналіз звіту подібності (відмітити потрібне):

✓ Запозичення, виявлення у роботі, оформлені коректно і не містять ознак плагіату.

□ Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

□ Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Захарченко С.М.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Костюк О. В.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Савицька Л. А.
(підпис) (прізвище, ініціали)