**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ**

**ІМЕНІ ТАРАСА ШЕВЧЕНКА**

ФАКУЛЬТЕТ РАДІОФІЗИКИ ЕЛЕКТРОНІКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ

Кафедра радіотехніки та радіоелектронних систем

До захисту допущено: «На правах рукопису»
Завідувач кафедри _____ Ігор АНІСІМОВ
18 травня 2023 р.

# КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему:

# «**Побудова та проектування мобільної мережі в програмному застосунку**»

**Виконав:**
студент 2-го курсу магістратури
денної форми навчання
спеціальності 172 Телекомунікації та радіотехніка
ОНП «Інформаційна безпека телекомунікаційних систем і мереж»
Хавік Костянтин Андрійович _____

**Науковий керівник**:
к.т.н., ас. Муштак Аль Шурайфі _____

**Рецензент:**
д. т. н., проф. Хлапонін Юрій Іванович _____

Засвідчую, що у цій магістерській роботі
немає запозичень з праць інших авторів без
відповідних посилань
Студент _____

Робота допущена до захисту в ЕК рішенням кафедри радіотехніки та радіоелектронних систем від 18 травня 2023 р., протокол № 18.

Завідувач кафедри радіотехніки та радіоелектронних систем,
доктор фіз.-мат. наук, професор
Анісімов Ігор Олексійович _____

Київ – 2023

# ЗМІСТ

# ВСТУП

Інтернет речей – одна з актуальних областей інженерії, що розвивається, це насамперед інформаційно-керуюча система, що працює на основі даних від фізичних предметів, забезпечених датчиками. Пристрої Інтернету речей, з одного боку, мають інтерфейс з комунікаційною мережею, а з іншого – інтерфейс, що забезпечує фізичну взаємодію датчиків та виконавчих механізмів.

**Актуальність роботи.** У наш час фермери можуть розміщувати на рослинах датчики, які їм підкажуть, коли рослини потрібно полити, скільки води необхідно і коли час збирати врожай. За допомогою цієї інформації можна отримати максимально високий та якісний урожай. Шахтарі можуть розміщувати у шахті датчики, які виявляють найменші концентрації небезпечних газів. Ця інформація буквально рятує життя.

Інтернет речей описує зростаючий ринок цифрових технологій, пов’язаних з Інтернетом і дозволяє покращити життя кожної людини на планеті. Ми можемо тільки гадати, скільки, і які типи робочих місць він може створити?!

Вступ до Інтернету речей пояснює, що таке Інтернет речей, які його функції, яке місце у цифровій трансформації він займає і яким чином можна стати частиною всього цього. Можна дізнатися про експоненційне збільшення кількості інтелектуальних пристроїв підключених до Інтернету та навчитися програмувати будь-який з цих пристроїв. У цій дипломній роботі розглядаються технології штучного інтелекту та вплив автоматизації на наше майбутнє. Крім того, усвідомлюється важливість конфіденційності та інформаційної безпеки у світі Інтернету речей.

**Об’єкт роботи.** Дослідження та аналіз безпеки в інтелектуальній мережі IoT.

**Предмет роботи**. Конструювання мобільної мережі у програмному застосунку Cisco Packet Tracer 8.2.

**Мета роботи.** Спроектувати та змоделювати зв’язок між двома офісами за рахунок використання внутрішніх базових станцій та розумних пристроїв.

# РОЗДІЛ 1. ІНФРАСТРУКТУРА IoT

## 1.1. Що таке Інтернет речей?

Системи Інтернету речей стали з’являтися наприкінці XX ст. Пристрій, будову якого сьогодні ми можемо назвати першою стемою Інтернету речей, розробили студенти у 1982 р.: вони встановили камеру навпроти автомата з Coca-Cola та підключили її до локальної мережі, щоб перевіряти, чи не закінчився в автоматі прохолодний напій. У 1990 р. випускник Массачусетського технологічного інституту Джон Ромкі (John Romkey) підключив до Інтернету свій тостер, який став першим, офіційно зареєстрованим об’єктом зі світу Інтернету речей. Потім був розумний пилосос, розумна кавоварка та інші пристрої, керування якими здійснюється в автоматичному або в автоматизованому режимі з використанням Інтернету для передачі даних.

Колись словосполучення «Інтернет речей» здавалося нам абсурдним і сприймалося як продаж речей через мережу Інтернет. Цей термін ввів британський інженер Кевін Ештон (Kevin Ashton) у 1999 р. як опис системи, в якій Інтернет пов’язаний з фізичним світом через датчики. У даний час ми маємо на увазі під цим терміном цілий комплекс цифрових технологій.

Передумовами для виникнення систем Інтернету речей стали: зменшення розмірів обчислювальних пристроїв; стандартизація протоколів; зниження вартості електроніки, зв’язку та обчислювальних потужностей; поява бездротових технологій зв’язку з низьким споживанням енергії.

Згодом, люди почали застосовувати системи Інтернету речей у сучасному мегаполісі. У великих містах встановлюють розумні комплекси зупинки, які знають, коли підійде той чи інший транспорт. Незабаром, на нас чекають розумні перехрестя та розумні транспортні системи, розумні побутові прилади, розумні рослини, тварини та навіть розумні об’єкти мистецтва. Всі ці автоматизовані системи Інтернету речей повинні зробити наше життя кращим, простішим і комфортнішим.

Інтернет речей (IoT, Internet of Things) – це не просто система, сьогодні так називається концепція, що поєднує безліч технологій для розробки систем автоматизації на основі даних які взаємодіють між собою із використанням мережевих рішень.

Сучасний індустріальний світ, у свою чергу, поринає у промисловий Інтернет речей (IIoT, Industrial Internet of Things) з можливістю віддаленого контролю ресурсів підприємства та керування ними в автоматизованому режимі. За допомогою систем Інтернету речей можна отримувати інформацію про доступність обладнання, його технічний стан, завантаження, технологічні порушення, графік технічного обслуговування тощо. Промисловий Інтернет речей дозволяє оперативно, у режимі реального часу, отримати інформацію з усього обладнання на підприємстві, за секунди розрахувати його коефіцієнт корисної дії (ККД), а із застосуванням прогнозуючої аналітики та нейронних мереж – спрогнозувати графік планово-попереджувальних робіт, ремонту та завантаження.

Застосування Інтернету речей у промисловості створює нові можливості для розвитку виробництва та вирішує низку найважливіших завдань: підвищення продуктивності обладнання; зниження матеріальних та енергетичних витрат; підвищення якості, оптимізація та покращення умов праці співробітників компанії; зростання рентабельності виробництва та конкурентоспроможності на світовому ринку.

Інтернет речей (IoT) – це з’єднання мільйонів інтелектуальних пристроїв та датчиків, підключених до Інтернету. Підключені пристрої та датчики спочатку збирають дані, потім обмінюються ними для оцінки багатьма організаціями, включаючи як і різні компанії, міста, урядові організації, лікарні так і окремих людей. Розвиток Інтернету речей став можливим, зокрема, завдяки появі недорогих процесорів та бездротових мереж. Пасивні об’єкти вже у минулому, такі як дверні ручки або лампи

розжарювання, тепер оснащуються інтелектуальними датчиками, які можуть збирати дані та передавати їх по мережі Інтернет.

За оцінками аналітиків, щомісяця до Інтернету підключається понад трьох мільйонів нових пристроїв. Також прогнозується, що за чотири роки у світі буде понад тридцять мільярдів підключених пристроїв.

Імовірно, третину цих пристроїв будуть складати комп'ютери, смартфони, планшети та розумні телевізори (Smart TV). Дві третини, що залишилися, припадуть на частку інших типів «речей», такі як датчики, актуатори та нові інтелектуальні пристрої, які відстежують, контролюють, аналізують та оптимізують наш світ.

Приклади інтелектуальних підключених датчиків – розумні дверні дзвінки, двері гаражів, термостати, спортивні аксесуари, електрокардіостимулятори, світлофори, місця для паркування тощо. Типи об'єктів, які можуть стати інтелектуальними датчиками, обмежуються лише нашою уявою.

## 1.2. Автоматизація IoT.

У структурі будь-якої системи Інтернету речей можна умовно виділити чотири частини: мікроконтролерна система збору даних, система мережевої взаємодії, система зберігання даних, система керування та моніторингу даних (рис. 1.1).

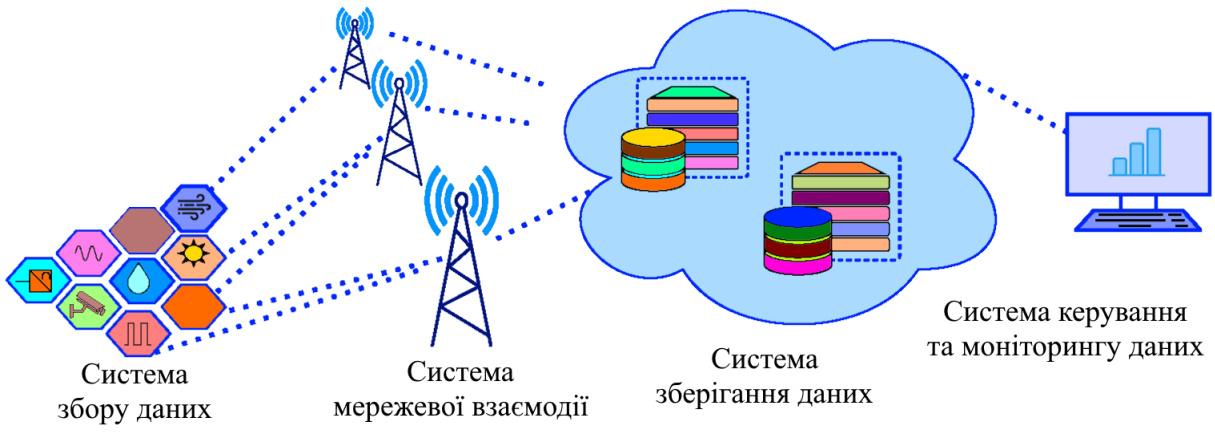


*Рис. 1.1. Структура системи Інтернету речей*

У систему збору даних (рис. 1.2) входять такі пристрої: сенсори (датчики), контролер або мікрокомп’ютер, актуатор та модуль передачі даних.

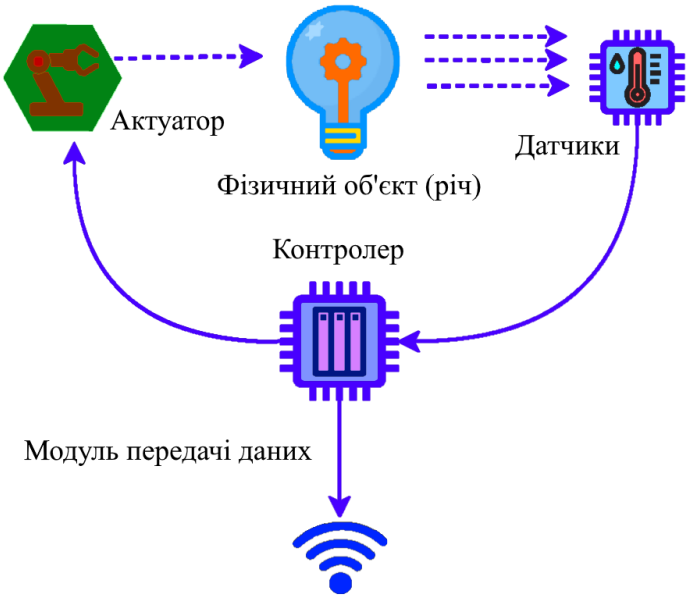


*Рис. 1.2. Система збору даних*

Як розумний пристрій IoT підключається до мережі Інтернет?

Датчик повинен бути підключений до мережі, щоб зібрані дані можна було передати та розповсюдити. Для цього потрібне дротове (Ethernet) або бездротове (Wi-Fi, Bluetooth тощо) підключення до контролера. Контролери відповідають за збір даних із датчиків та забезпечують підключення до мережі Інтернет. Контролери можуть самостійно приймати негайні рішення або надсилати дані для коригування до більш потужного комп’ютера. Такий потужніший комп’ютер або знаходиться у тій же локальній мережі що і контролер, або доступний через Інтернет-з’єднання.

Датчики часто працюють разом із пристроєм, який називається актуатором. Актуатори приймають вхідні електричні сигнали та перетворюють їх у фізичну дію.

Для більшості нових пристроїв, таких як фітнес-аксесуари, імплантовані електрокардіостимулятори, повітроміри у шахтах та водоміри на фермерських полях, не потрібне бездротове підключення. Так як багато датчиків працюють «у польових умовах» і живляться від акумуляторів або сонячних панелей, особливу

увагу слід приділяти потужності, що споживається. Необхідно використовувати малопотужні варіанти підключення для оптимізації та подовження ресурсу дії датчика.

1.3. Переваги підключення розумних пристроїв IoT.

Компанії мають більше інформації про продукти які вони продають та хто їх купує. Озброївшись цим типом даних, вони можуть оптимізувати виробництво своєї цільової продукції, маркетингу та реклами у конкретних галузях або аудиторії; сприяти створенню нових можливостей для бізнесу та маркетингових ідей.

Уряди контролюють екологічні проблеми, цільове фінансування з соціальних питань та інформують про контроль за виходом електроенергії.

Міста мають можливість контролювати моделі трафіку, засновані на часі доби або великих подіях, контролювати сміття та утилізацію, стежити за здоров'ям та житловими потребами, оцінювати майбутні вимоги до транспортування.

Фізичні особи можуть отримувати покращені переваги для здоров'я та фітнесу, кращу домашню та сімейну безпеку, а також знизити витрати на енергоносії та системи опалення. Вони можуть насолоджуватися різноманітними розвагами, обмежувати швидкість руху авто підліткового водія або навіть контролювати здоров'я старшого члена сім'ї за кермом свого автомобіля.

1.4. Розвиток цифрової трансформації.

Якщо зізнатися... Хто з людей може прожити день без свого смартфона?

У світі інтелектуальних пристроїв більше, ніж людей. Дедалі більше людей цілодобово підключено до глобальної мережі Інтернет тим чи іншим способом. Постійно зростає кількість людей, які використовують три чи більше інтелектуальних пристроїв. Це можуть бути смартфони, фітнес-монітори та монітори стану здоров'я, електронні книги та планшети.

Яким чином з’єднується така велика кількість пристроїв?

Все це можливо завдяки сучасним цифровим мережам. Світ швидко огортається мережами, які забезпечують можливість з’єднання та передачі даних між цифровими пристроями. Уявіть, що мережа – це цифрова оболонка, що оточує планету. Саме за її допомогою підключаються мобільні пристрої, електронні датчики, електронні вимірювальні пристрої, медичні пристрої та різні прилади. Ці пристрої забезпечують моніторинг, обмін даних та оцінюють їх, а в деяких випадках вони автоматично налаштовуються відповідно до даних, що збираються і передаються.

У міру того, як суспільство все ширше використовує цифрові пристрої, зростають і цифрові мережі по всьому світу. А разом із зростанням економічних переваг цифровізації ми спостерігаємо цифрову трансформацію. Цифрова трансформація – це застосування цифрових технологій для підтримки інновацій у бізнесі та промисловості. Сьогодні цифрові інновації охоплюють усі аспекти суспільства.

1.5. Використання та програмування пристрою Arduino.

Arduino – платформа для створення прототипів, за допомогою якої користувачі можуть створювати програми для керування апаратним забезпеченням. Нижче вивчалось використання Arduino та Arduino IDE для керування частотою миготіння світлодіодного індикатора.

Для розуміння роботи пристрою Arduino, необхідно було мати такі пристрої:

- Arduino Redboard або Uno;
- USB-кабель для підключення до ПК;
- 1 індикатор.

Спочатку, потрібно було перейти на спеціальну сторінку у браузері, а саме: https://www.arduino.cc/en/Main/Software. Вибрати у правій панелі Windows Installer, щоб завантажити програмне забезпечення. Натиснути «JUST DOWNLOAD» (Тільки завантажити), потім натиснути Save File (Зберегти файл)

та зберегти його у папці Downloads (Завантаження). Після завершення завантаження перейти до папки, до якої було завантажено файл. Відкрити папку Downloads (Завантаження).

Потім потрібно було встановити Arduino, відкривши файл ardinio-x.x.x windows.exe, де x позначає номер версії. Натиснути кнопку «Yes» (Так) у діалоговому вікні User Account Control (Керування обліковими записами користувачів). Натиснути кнопку «I Agree» (Погоджуюсь з умовами використання), щоб продовжити інсталяцію та дотримуватись інструкцій на екрані, щоб завершити інсталяцію.

У відповідь на запит, дозволити встановлення драйвера та програмного забезпечення Arduino USB (рис. 1.3).

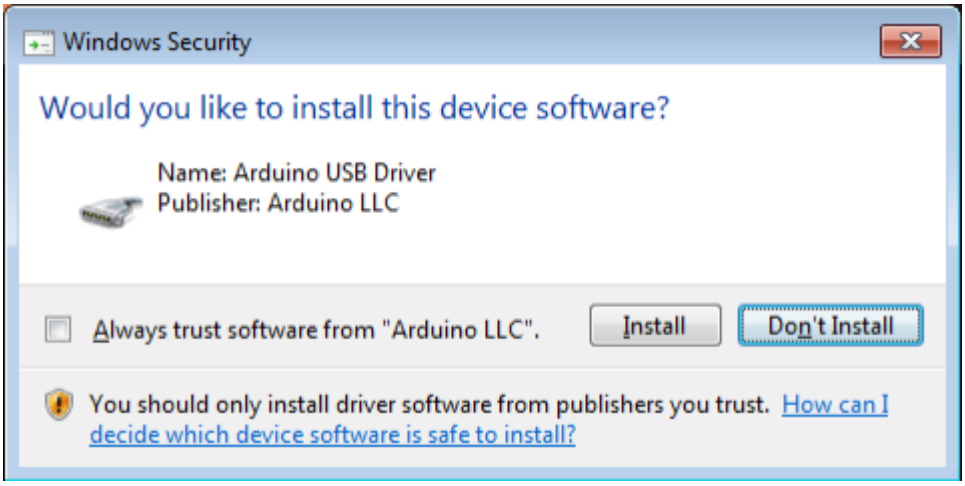


*Рис. 1.3. Вікно запитання на встановлення драйверів Arduino*

Після встановлення натиснути кнопку «Close» (Закрити).

У цій частині підключаємо плату Arduino до комп’ютера через USB-порт. Для керуванням світлодіодним індикатором на контакті 13 плати Arduino буде використовуватись приклад програми.

- Спочатку потрібно підключити USB-кабель до плати Arduino та USB-порту на комп’ютері і, за потреби підключити плату до зовнішнього джерела живлення. Якщо живлення подається, горить зелений індикатор.
- Відкрити диспетчер пристроїв, щоб знайти порт, який використовується Arduino.
- Розгорнути розділ «Порти» (COM & LPT).

➢ Звернути увагу на розташування послідовного USB-порту. На рис. 1.4 йому призначено номер COM8.

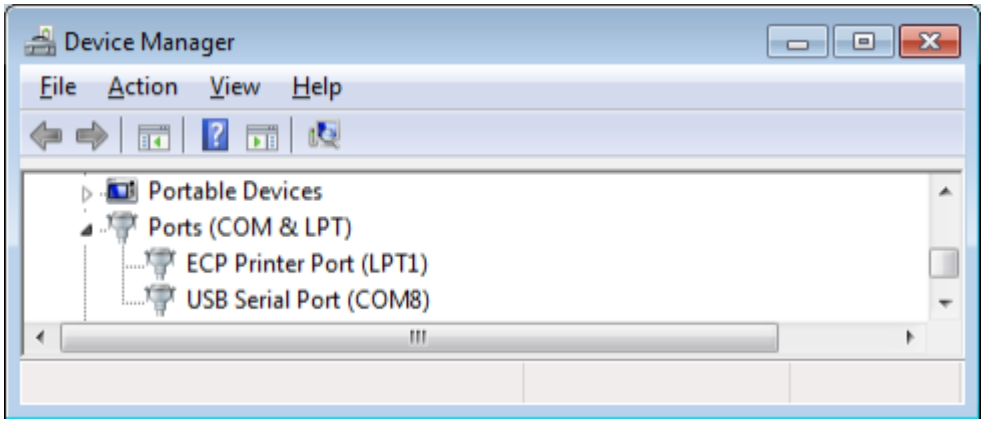


*Рис. 1.4. Порти COM та LPT у диспетчері пристроїв*

На деяких моделях плати Arduino є інтегрований світлодіодний індикатор, підключений до цифрового контакту 13. Якщо на платі є вбудований світлодіодний індикатор, він буде розташований поруч із індикатором живлення. Цей інтегрований світлодіодний індикатор можна використовувати під час виконання будь-яких завдань. Якщо на платі немає вбудованого світлодіодного індикатора або Ви хочете використовувати інший світловий індикатор, тоді можна прикріпити такий індикатор до плати. Наведені нижче дії необов'язкові, якщо на платі є вбудований індикатор.

Для встановлення індикатора потрібно знайти на платі контакт 13 та контакт заземлення (GND). На рис. 1.5, як приклад, показано плату Arduino RedBoard.


*Рис. 1.5. Зображення плати Arduino RedBoard*

Потім треба підключити світлодіодний індикатор до контакту 13 та контакту заземлення. Світлодіодні індикатори повинні встановлюватися у певному напрямку, та довжина їх контактів повинна різнитися. Коротке плече вставляється в отвір, позначений GND, а довге – в отвір 13.

Для виконання коду спочатку потрібно запустити Arduino. Щоб використати один із прикладів програм, Blink, потрібно вибрати його у меню File > Examples > Basics > Blink (Файл > Приклади > Базові > Blink).

Рекомендую прочитати коментарі на початку програми. У розділі коментарів пояснюються функції програми та наводиться інша інформація про програму.

### 1.6. Програмування на основі мови Python.

Python – це дуже поширена мова, що забезпечує зручність читання та написання коду. Спільнота розробників Python розширює можливості мови, створюючи різні типи модулів та надаючи їх іншим програмістам.

Філософія цієї мови описана в документі The Zen of Python (Зена Пайтона):

- Гарне краще, ніж потворне.
- Явне краще, ніж неявне.
- Просте краще, ніж складне.
- Складне краще, ніж заплутане.
- Читання має значення.

Незважаючи на простоту мови Python, для її вивчення потрібен певний час. Для полегшення вивчення Python можна використовувати Blockly для закріплення навичок.

Хоча мови програмування мають різну семантику та синтаксис, програмна логіка залишається незмінною. Програмісти-початківці можуть використовувати Blockly, щоб легко створювати програми незалежно від мови, експортувати їх у вигляді коду Python і використовувати отриманий код для вивчення синтаксису, структури і семантики Python.

Python – мова, що інтерпретується, тому для аналізу і виконання коду Python необхідний інтерпретатор. Інтерпретатор Python розпізнає та виконує код мови Python. Код мови Python може бути створений у будь-якому текстовому редакторі. Інтерпретатори Python доступні для багатьох операційних систем. Розробники на Python можуть створювати та розгортати програми на Python практично у будь-якій операційній системі. Крім того, для упаковки вихідного коду Python у файл, що виконується, можна використовувати сторонні інструменти, такі як ***Py2exe*** і ***Pyinstaller***. Це усуває необхідність використання інтерпретатора під час виконання коду Python.

У комп'ютерах з ОС Linux інтерпретатор Python зазвичай встановлюється у папку ***/usr/bin/python*** або ***/usr/bin/python3*** (залежно від доступних версій Python у системі). При використанні нової програми встановлення Python у Windows, Python за замовчуванням встановлюється в головний каталог користувача. У комп'ютерах з ранніми версіями Windows Python часто міститься у каталозі ***C:\PythonXX*** (де XX – версія Python). Після встановлення інтерпретатор Python працює подібно до оболонки Linux. Це означає, що під час виклику без аргументів він зчитує та виконує команди в інтерактивному режимі. При виклику, з ім'ям файлу як аргумент або з використанням файлу як стандартних вхідних даних, він зчитує та виконує сценарій із цього файлу.

Щоб запустити інтерпретатор, потрібно ввести ***python*** або ***python3*** у командному рядку оболонки.

У деяких старих системах, як і раніше, працює більш рання версія (Python 2), однак багато нових систем переходять до використання нової версії, Python 3. Версія Python вказується в першому рядку при запуску інтерпретатора (рис. 1.6).

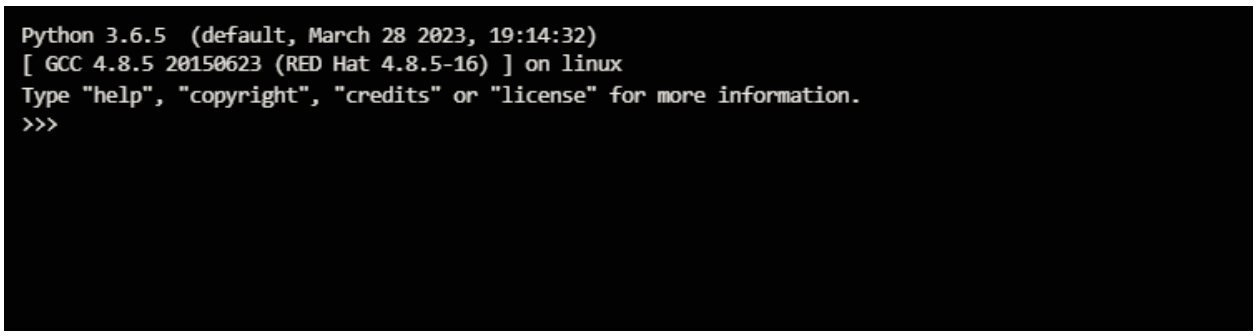


*Рис. 1.6. Інтерфейс командного рядка Python*

Якщо інтерпретатор Python викликається без аргументів, а команди вводяться з клавіатури, то кажуть, що інтерпретатор працює в інтерактивному режимі. У цьому режимі інтерпретатор очікує на введення команд.

Основне запрошення до введення команди складається із трьох символів «більше» (>>>). Рядки-продовження позначаються трьома точками (...). Продовження – це додаткове запрошення до введення команди за промовчанням.

Запрошення >>> вказує, що інтерпретатор перебуває у стані готовності та чекає на команди.

Ще один спосіб використання інтерпретатора – ***python -c command [arg]*** ..., при якому виконуються інструкції у команді. Так як інструкції Python часто містять прогалини або інші символи, що відносяться до оболонки; рекомендується укладати всю команду в одинарні лапки.

Інтерпретатор отримує та виконує інструкції в інтерактивному режимі. Інтерпретатор виступає як простий калькулятор. Потрібно ввести у ньому вираз, і він запише значення.

Синтаксис виразу дуже простий. Оператори +, -, * і / працюють так само, як і у більшості інших мов (наприклад, Pascal або C). Дужки (()) можна використовувати для групування, як показано на рис. 1.7.


*Рис. 1.7. Приклад використання дужок*

Змінні – це іменовані області пам’яті, які використовуються для зберігання даних під час виконання програми. Щоб визначити значення змінним у Python, потрібно використовувати знак рівності (=).

Числовий результат відображається перед наступним інтерактивним запрошенням до введення команди, як показано на рис. 1.8.


*Рис. 1.8. Приклад застосування змінної*

Функції є важливою частиною багатьох програмованих мов. Функції дозволяють призначити ім’я блоку коду та повторно використовувати його за потреби. На рис. 1.9 визначається функція, яка складає два числа та виводить результат.


*Рис. 1.9. Приклад розв'язання математичного виразу*

Python підтримує безліч корисних функцій та типів даних. Нижче наведені деякі з найважливіших.

***Range().*** Функція range() створює список чисел, які зазвичай використовуються для ітерацій циклів FOR.

- ***range ( stop )*** – це кількість створюваних цілих чисел, починаючи з нуля.
- ***range( [start], stop [, step ]*** – це перше число, останнє число та крок між двома сусідніми числами у послідовності.

***Кортежі.*** Кортеж – це послідовність незмінних об'єктів Python. Кортеж є послідовністю, укладеною у круглі дужки.

***Списки.*** Списки – це послідовність змінних об'єктів Python. Для створення списку потрібно розмістити розділені комами значення у квадратні дужки.

***Множини.*** Безліч є неупорядкованими наборами унікальних елементів. Ось деякі поширені варіанти використання множин: перевірка приналежності, видалення дублікатів із послідовності та виконання стандартних математичних операцій над множинами, таких як перетин, об'єднання, різниця та симетрична різниця.

***Словник.*** Словник – це список елементів, розділених комами. Кожен елемент є поєднанням значення і унікального ключа. Кожен ключ відокремлюється від свого значення двокрапкою. Весь словник полягає у фігурних дужках. Можна звертатися до елементів словника, змінювати їх та

видаляти. Також існує багато вбудованих функцій словника, наприклад, функція порівняння елементів різних словників, а також функція, яка підраховує загальну кількість елементів у словнику.

## 1.7. Висновки до розділу.

IoT просуває наше повсякденне життя та робить великий внесок у такі галузі, як сільське господарство, управління ланцюжками поставок, відстеження розташування, віддалений моніторинг, аналіз у реальному часі тощо.

Оскільки концепція Інтернету речей стає все більш актуальною, вона привертає велику увагу дослідників і промисловців з усього світу. Незважаючи на те, що Інтернет речей має велику кількість переваг, така система також має велику кількість потенційних проблем та недоліків. І однією з найважливіших проблем залишається безпека.

# РОЗДІЛ 2. АНАЛІЗ БЕЗПЕКИ ТЕХНОЛОГІЙ IoT

## 2.1. Проблеми безпеки Інтернету речей.

У даний час спостерігається збільшення кількості інцидентів (злочинів) у сфері інформаційної безпеки та інформаційних технологій. Цьому сприяє повсюдне поширення мережевих технологій зберігання даних та широке поширення IoT-речей: у 2018 році кількість підключених пристроїв оцінювалася у 22 млрд з перспективою зростання приблизно до 40 млрд до 2025 року. Ці пристрої можуть містити вразливості, якими можуть скористатися кіберзлочинці і у результаті поставити під загрозу конфіденційність користувача та громадську безпеку. Не випадково кібербезпека IoT викликає занепокоєння у 95% респондентів опитування, проведеного аналітиками IoT Analytics, причому майже 40% «дуже стурбовані» можливими вразливостями Інтернету речей. Таким чином, забезпечення безпеки є однією з основних проблем, пов’язаних з IoT.

Причиною цієї проблеми є той факт, що технології IoT, як і більшість споживчих технологій, розроблені без урахування вимог безпеки, оскільки основним завданням виробників було мінімізувати собівартість та час розробки, здешевити виробництво та збільшити обсяг продукції, що випускається. У результаті подібної політики розумні пристрої відчувають нестачу ресурсів. Через цей недолік більшість інструментів безпеки не можуть бути встановлені у пристроях IoT, що робить пристрої легкою мішенню для кіберзлочинів.

Хакери знаходять слабкості вбудованих систем захисту, їх уразливості та можуть використовувати пристрої IoT як інструменти для атак на інші системи або сайти. Кіберзлочинці, озброєні технологіями IoT, можуть, перебуваючи у віртуальному просторі, загрожувати безпеці і навіть життю людей; і кількість подібних злочинів зростає. Наприклад, Управління контролю якості харчових продуктів та лікарських препаратів США (FDA) повідомило, що деякі кардіостимулятори (пристрої, які посилають електричні

імпульси до серця, щоб встановити серцевий ритм) вразливі до злому. Це означає, що пацієнти з кардіостимулятором можуть потрапити під удар хакерів, які здатні захопити контроль над кардіостимулятором.

Цифрові дані IoT є багатим і часто недослідженим джерелом інформації. Більшість виробників IoT-пристроїв демонструють покупцям функціональність їх товару (функції що виконуються та його можливості), але не згадують про технологію програмного забезпечення (ПЗ), що керує цими функціями і не розкривають його вразливості. Наприклад, роботи-пилососи можуть прибирати кімнату самостійно та повідомляти про виконання завдання, тому що вони керуються за допомогою датчиків, що визначають розмір та форму забруднення. Дослідники компанії Check Point Software Technologies Ltd., постачальника рішень щодо кібербезпеки у всьому світі, 26 жовтня 2017 року виявили у мобільному та хмарному додатках робота-пилососа у процесі входу на портал вразливість, яка дозволила їм віддалено створити підроблений обліковий запис застосунку, а потім використовувати її, щоб оволодіти обліковим записом та розумними пристроями користувача і отримати контроль над пилососом та вбудованою в нього відеокамерою; таким чином оволодівши доступом до відеотрансляції в онлайн-режимі з дому. Це означає що зловмисник, отримавши контроль над обліковим записом конкретного користувача, може контролювати будь-який пристрій, пов’язаний з цим обліковим записом, включаючи пилососи, холодильники, плити, посудомийні та пральні машини, фени та кондиціонери. Подібні загрози висувають важливе питання: як користувачі розумних пристроїв можуть захистити себе?! Фахівці з безпеки рекомендують змінювати паролі, оновлювати програми та самі пристрої, захищати персональні дані.

## 2.2. Класифікація загроз IoT.

Екосистема IoT-технологій є комбінацією різних технологічних зон: зона IoT-пристроїв, мережева зона та хмарна зона. Ці зони можуть бути джерелом цифрових даних. Тобто дані можна збирати з розумного пристрою

або датчика внутрішньої мережі, такого як брандмауер або маршрутизатор, або із зовнішніх мереж (хмара або застосунок). Ці технологічні зони є об'єктом кримінального інтересу кіберзлочинців.

Для боротьби з кіберзлочинами було створено спеціальний розділ криміналістики – ***комп'ютерна криміналістика***, чи ***форензика*** (англ. Computer forensics), – *прикладна наука про розкриття злочинів, пов'язаних із комп'ютерною інформацією, про дослідження доказів у вигляді комп'ютерної інформації, методах пошуку, отримання та закріплення таких доказів. IoT-криміналістика (англ. IoT-forensics) як підрозділ форензики займається розслідуванням кіберзлочинів у системі IoT, дослідженням цифрових доказів.*

У ході розслідування комп'ютерних злочинів, пов'язаних із шахрайствами, або комп'ютерними атаками, засобами яких так чи інакше були мережеві з'єднання, проводять цифрову експертизу – спеціальне дослідження, що включає аналіз використання мережевих технологій.

Залежно від місця зберігання даних у системі IoT експерти у сфері IoT-криміналістики виділяють три небезпечні ділянки у ландшафті кіберзагроз: хмара, мережа і пристрій відповідно; також виділяються: хмарна криміналістика, мережева та криміналістика на рівні пристрою IoT.

Оскільки цінні дані часто зберігаються у хмарі, хмарна інфраструктура є однією з найважливіших цілей для зловмисників. Для проведення традиційної цифрової експертизи експерт-криміналіст спочатку отримує вилучене цифрове обладнання, а потім починає розслідування для отримання цифрових доказів (цифрових даних, які можна використовувати як доказ скоєння кіберзлочину). Однак, якщо дані зберігаються у хмарі, тоді використовується інший сценарій, тому що цифрові докази можуть бути розміщені у хмарних сховищах на різних серверах, з яких важко витягти дані. Крім того, у хмарі обмежений доступ до інфраструктури та інформації про точне місце зберігання даних. Під час розслідування інциденту, що стався у

хмарі, постачальник хмарних послуг може запитати інформацію про ім’я власника даних або місце зберігання відповідних даних.

Слід зазначити, що у хмарних сервісів які використовують віртуальні машини як сервери, дані можуть зберігатися саме на цих серверах. Реєстри запису або тимчасові Інтернет-файли на серверах можуть бути видалені, якщо вони не синхронізовані з пристроями зберігання, наприклад, якщо ці сервери перезапускаються або вимикаються.

Мережева криміналістика проводить дослідження всіх видів мереж, які використовуються IoT-пристроями для надсилання та отримання даних. До них відносяться домашні, промислові та локальні мережі (MAN, Metropolitan Area Network; та WAN, Wide Area Network). Наприклад, якщо інцидент пов’язаний з пристроями IoT, всі журнали, в яких відображено поток трафіку, такі як брандмауери або журнали IDS можуть бути потенційними доказами.

Експертиза на рівні пристрою включає всі потенційні цифрові докази, які можуть бути зібрані з IoT пристроїв, таких як графіка, аудіо, відео. Прикладом подібних цифрових доказів є відео та графіка з камери відеоспостереження або аудіозаписи з розумної колонки.

Існуючі інструменти у галузі цифрової криміналістики можуть не відповідати інфраструктурі середовища IoT. Через те, що більшість даних IoT зберігається у хмарі, воно стає одним із основних джерел доказів злочинів у IoT, і як зазначалося вище, знайти необхідні цифрові докази у хмарі навіть експерту-криміналісту складно. Крім того, на одному фізичному сервері можуть працювати декілька віртуальних машин, що можуть належати різним власникам. Великі хмарні сховища можуть бути недоступними після скоєння злочину. Усі ці проблеми вимагають вирішення та пошуку нових інструментів для розслідування кіберзлочинів у світі IoT.

Різні загрози несуть різні потенційні небезпеки, які різняться залежно від сценаріїв використання. Нижче наведено класифікацію загроз, характерних для IoT, з описом різних видів (таблиця 2.1).

| Таблиця 2.1. Класифікація загроз | |
|---|---|
| **Загроза** | **Опис** |
| **1. Навмисні дії** | |
| Шкідливе ПЗ | Програмне забезпечення, призначене для виконання небажаних та несанкціонованих дій у системі без згоди користувача. Це може призвести до пошкодження, модифікації чи крадіжки інформації. Його небезпека може бути високою. |
| Експлойт | Код, розроблений для використання вразливості з метою отримання доступу до системи. Цю загрозу важко виявити, і в середовищах IoT її небезпека варіюється від високої до критичної, залежно від порушених активів. |
| Цільова атака | Атака, призначена для конкретної мети, яка проводиться протягом тривалого періоду часу у кілька етапів. Основна мета злочинця – залишатися непоміченим та отримати якнайбільше конфіденційних даних, інформації або контролю. Хоча небезпека цієї загрози є середньою, її виявлення – зазвичай дуже складний та тривалий процес. |
| DDoS-атака (Distributed Denial of Service Attack) | У процесі DDoS-атаки кілька систем атакують одну ціль, щоб навантажити її та призвести до збою. Це можна зробити шляхом створення безлічі з'єднань, переповнення каналу зв'язку або багаторазового повторного відтворення одних і тих самих повідомлень. |
| Скомпрометований пристрій | Цю загрозу важко виявити, оскільки скомпрометований пристрій важко відрізнити від оригіналу. Ці пристрої зазвичай мають бекдори та можуть використовуватись для проведення атак на інші системи у навколишньому середовищі. |
| Втрата конфіденційності | Ця загроза небезпечна як втрата конфіденційності користувача, так і впливом стороннього персоналу на елементи мережі. |
| Модифікація інформації | У цьому випадку мета полягає не у пошкодженні пристрою, а у маніпуляції інформацією, щоб викликати хаос чи отримати грошовий прибуток. |
| **2. Перехоплення інформації** | |
| Атака «людина посередині» | Активна атака підслуховування, за якої зловмисник передає повідомлення від однієї жертви іншій, щоб змусити їх повірити, що вони розмовляють безпосередньо одна з одною. |

| | |
|---|---|
| Підключення до активної сесії | Взяття під контроль активного сеансу зв’язку між двома елементами мережі. Зловмисник може отримати важливу інформацію, у тому числі конфіденційну. |
| Перехоплення інформації | Несанкціоноване перехоплення та (іноді) модифікація приватної комунікації, наприклад, телефонних дзвінків, миттєвих повідомлень, повідомлень електронної пошти. |
| Мережева розвідка | Пасивне отримання внутрішньої інформації про мережу: підключені пристрої, використовуваний протокол, відкриті порти, використовувані служби тощо. |
| Перехоплення з’єднання | Крадіжка, з’єднання для передачі даних, при цьому незаконний хост діє як законний з метою крадіжки, зміни або видалення даних, що передаються. |
| **3. Вимкнення** | |
| Вимкнення живлення | Навмисне або випадкове переривання, збій у мережі. Залежно від порушеного сегменту мережі та часу, необхідного для відновлення, небезпека цієї загрози варіюється від високої до критичної. |
| Збій пристрою | Збій або вихід з ладу апаратного пристрою. |
| Збій системи | Збій програмних служб або програм. |
| Втрата сервісу підтримки | Недоступність послуг підтримки, необхідних для правильної роботи інформаційної системи. |
| **4. Технічний збій** | |
| Вразливості на програмному рівні | Пристрої IoT часто вразливі через слабкі паролі, незмінні паролі, встановлених за замовчуванням, програмних помилок та помилок конфігурації. |
| Сторонні помилки | Помилки в активному сегменті мережі, спричинені неправильним налаштуванням іншого сегменту, який має до нього пряме відношення. |
| **5. Катастрофи** | |
| Стихійні лиха | Повені, сильні вітри, сильні снігопади, зсуви ґрунту та інші стихійні лиха, що можуть пошкодити пристрої фізично. |
| Аварії у середовищі IoT | Аварії у середовищі розгортання IoT-обладнання, що можуть призвести до непрацездатності. |
| **6. Фізична атака** | |
| Модифікація пристрою | Модифікація пристрою, внесення змін до пристрою (наприклад, шляхом використання поганої конфігурації портів, використання відкритих портів). |
| Знищення пристрою | Псування, крадіжка тощо. |

## 2.3. Проблеми безпеки технологій індустріального Інтернету речей.

Перш ніж з’ясувати актуальні для IIoT загрози, необхідно визначити технології, які застосовані у цій галузі. У таблиці 2.2 наведено технології IIoT.

Таблиця 2.2. Технології індустріального Інтернету речей

| **Технологія** | **Опис** |
|---|---|
| Кінцеві пристрої IoT | Пристрої, які оснащені вбудованими технологіями збору, обробки, зберігання, передачі інформації, інтелектуального прийняття рішень. |
| Міжмашинний зв’язок (M2M) | Технологія, що полегшує прямий зв’язок між пристроями у мережі без участі людини. |
| Аналіз Big Data | Процес вивчення величезної кількості різних типів наборів даних, відео та аудіо, згенерованих у реальному часі інтелектуальними датчиками, пристроями, журналами. |
| Робототехніка | Удосконалені промислові роботи, наділені на вирішення складних завдань інтелектуальними можливостями, такими як здатність вчитися на своїх помилках та підвищувати свою продуктивність. |
| Штучний інтелект | Алгоритми, які дозволяють комп’ютерам та обчислювальним машинам виконувати завдання, які зазвичай виконують люди. |
| Машинне навчання | Алгоритми, які дозволяють комп’ютерам діяти та покращувати здатність прогнозувати без явного програмування. |
| Прогнозуюче обслуговування | Рішення, що відстежують стан обладнання, прогнозуючи, коли може статися збій, ефективного обслуговування з мінімально можливою частотою. |
| Моніторинг у режимі реального часу | Технології, що дозволяють збирати та об’єднувати дані про безпеку від компонентів системи, а також відстежувати та аналізувати події, що відбуваються в мережі. |
| Розширена аналітика збитків | Методи аналізу різних типів втрат, які можуть виникнути у середовищі, з метою їх усунення або зменшення. |
| Комп’ютерні обчислення | Рішення, що забезпечують доступ до загальних наборів ресурсів, таких як мережі, сервери та програми, з мінімальними вимогами до керування та взаємодії із постачальником послуг. |
| Доповнена реальність | Технології, які змінюють сприйняття реальності навколишнього середовища, інструмент для підвищення ефективності завдань (наприклад, ручної збірки). |

Проблеми IoT та IIoT багато у чому повторюють одна одну. Виходячи з перерахованих вище технологій можна виділити низку проблем безпеки IIoT:

- вразливість пристроїв та систем;
- складність керування процесами;
- конвергенція інформаційних та операційних технологій (IT/OT);
- складність ланцюжка поставок;
- застарілі промислові системи управління;
- небезпечні протоколи;
- людський фактор;
- невикористовувані функції;
- забезпечення безпеки продукту після його реалізації.

## 2.4. Класифікація загроз IIoT.


*Схема 2.1. Класифікація загроз IIoT*

Нижче наведено опис кожної небезпеки.

1. **Відмова або вихід з ладу елементів системи:**
   а) збій або вихід з ладу кінцевих IIoT-пристроїв виникає за умови неналежного обслуговування, недотримання посібників та інструкцій з експлуатації пристроїв;
   б) відмова або вихід з ладу систем керування може статися, якщо не забезпечується належне обслуговування, дотримання посібників та інструкцій з експлуатації пристроїв;
   в) експлуатація вразливостей програмного забезпечення стає можливою через відсутність оновлень, використання слабких паролів або паролів за промовчанням, а також неправильної конфігурації;
   г) відмова або збій у постачальників послуг тягне за собою порушення процесів, які залежать від сторонніх сервісів.
2. **Навмисна дія:**
   а) відмова в обслуговуванні;
   б) шкідливе ПЗ;
   в) керування програмним та апаратним забезпеченням;
   г) маніпулювання інформацією;
   д) цільова атака;
   е) витік персональних даних;
   ж) Brute-force атака.
3. **Правове порушення:**
   а) порушення законодавства, норм, правил та зловживання персональними даними;
   б) невиконання вимог документації.
4. **Ненавмисне ушкодження елементів системи:**
   а) ненавмисна зміна даних або конфігурації у системі ОТ;

б) некоректне використання або адміністрування пристроїв та систем IIoT/OT;

в) збитки, завдані третьою стороною.

**5. Фізична атака:**

а) крадіжка та вандалізм;

б) саботаж, диверсія.

**6. Вимкнення пристроїв:**

а) відключення мережі зв’язку;

б) відключення електроживлення;

в) втрата послуг підтримки.

**7. Підслуховування, перехоплення, крадіжка інформації:**

а) «людина посередині»;

б) перехоплення протоколу IoT;

в) перехоплення інформації;

г) мережева розвідка;

д) перехоплення сеансу;

е) збір інформації;

ж) повтор повідомлень.

**8. Катастрофа:**

а) стихійне лихо;

б) екологічна катастрофа.

2.5. Хмарна безпека.

Будова мобільної мережі складається з інфраструктури віртуалізації мережевих функцій, де апаратне забезпечення відокремлене від програмного, і вони не залежать одне від одного діями та операціями які для них поставлені. Однак важливий фактор безпеки у хмарі – багаторазова використовувана хмарна інфраструктура, наприклад центральна хмара, крайова хмара та хмара на дальній межі, щодо вимоги до затримки у випадку використання. Ключові особливості хмарної безпеки:

- захист хмарної інфраструктури мережі;
- захист інфраструктури хмарного забезпечення;
- захист програмного забезпечення від атак;
- захист віртуальних машини та сховищ;
- захист серверів, оновлення механізму сховищ кожного сервера.

2.6. Виявлення аномалій на основі функції аналітики мережевих даних.

В архітектурі на основі послуг мобільного зв'язку з'явилася нова функція аналітики, відома як NWDAF (Network Data Analytics Function). NWDAF надає аналітику про екземпляр сегменту мережі та рівень завантаження мережевих функцій, навантаження/перевантаження; також пов'язана і аналітика, пов'язана з продуктивністю мережі, яка корисна для виявлення аномалій. Раптове збільшення навантаження на систему може вказувати на потенційну проблему, а саме DDoS-атаку на мережу. Функція аналітики NWDAF дуже корисна у виявленні атак, які генеруються через внутрішню загрозу мережі.

2.7. IDS/IPS на границі мережі.

Система виявлення та запобігання вторгнень (IDS/IPS, Intrusion Detection and Prevention System) повинна бути реалізована на границі мережі та брандмауеру; вона повинна бути розміщена для реалізації обмежень. Тепер базова мобільна мережа має доступ до зовнішнього світу, шлях якої

побудований через API (Application Programming Interface). Він є дуже важливим аби система виявлення та запобігання вторгненням у з'єднанні між Інтернетом і ядром мобільної мережі не була зламана та виведена з ладу.

2.8. Контроль безпеки у мобільному середовищі.

Є випадки використання мобільного зв'язку, які вимагають дуже низької затримки та дуже високої надійності. Отже, більш поширеним є використання мобільних периферійних обчислень, де вузли радіокерування, користувальницька функція площини (UPF, User Plane Function) і функція застосування, реалізовані разом на одному сайті, відомий як мобільний периферійний сайт, а інші функції базової мережі знаходяться у центрі сайту і усі є підключеними. Необхідно запровадити належну реалізацію безпеки між центральним основним сайтом і мобільною граничною стороною, а також між мобільним граничним сайтом і зовнішнім світом. Будь-яке порушення безпеки на мобільному периферійному сайті не слід поширювати на центральний сайт.

2.9. Впровадження безпеки IoT через мобільну мережу.

Є багато випадків використання, які можна перевірити, використовуючи мобільну мережу як мережу яка має можливість підключати мільйони пристроїв, високу пропускну здатність, низьку затримку, надійний і безпечний зв'язок. GSMA (Groupe Speciale Mobile Association) мережа визначає випадки використання мобільної мережі для вертикальних площин і кожен варіант використання має певні вимоги щодо трафіку, надійності та безпеки.

## 2.10. Розумна мережа і розумні фабрики (Індустрія 4.0).

Електромережа – це критично важлива інфраструктура, яка включає виробництво, передачу, розподіл та споживання електроенергії. Є багато інших критичних інфраструктур які залежать від електроенергії для виконання своїх операцій, таких як телекомунікації, банківська справа, транспорт та багато іншого.

Однією з найбільших проблем для електромереж є відповідність виробництва електроенергії до споживання електроенергії. Коли виробництво електроенергії неоднакове (генерація електроенергії = споживання електроенергії є ідеальним сценарієм) до споживання електроенергії, або великі втрати для енергетичної компанії, або коливання напруги, то вини обладнання на стороні споживання у цьому немає. У такому разі споживання на виробництві зросте і буде потреба у розширенні живлення електроенергії, щоб була відповідність до підвищеного попиту. У більшості випадків потреба в електроенергії у годину напруженої роботи (годину пік) є високою, і для цього потрібна додаткова потужність, тобто необхідна генерація, яка не має користі протягом звичайних годин, але збільшує експлуатаційну вартість виробництва електроенергії під час її нестачі.

Найкращі способи зменшити різницю між виробництвом та споживанням електроенергії, та ще й зробити енергомережу більш стійкою – це застосувати використання інтелектуальної мережі, тобто систему, яка сама може реагувати на попит; вона реалізована за допомогою інфраструктури попереднього вимірювання (AMI, Advance Metering Infrastructure) та розумних лічильників. На першому кроці інтелектуальні лічильники повинні часто звітувати про споживання електроенергії, щоб ці дані можна було зібрати та обробити для подальшого створення звіту інформації про споживання; для того щоб можна було швидко регулювати виробництво електроенергії, споживання та вивчати тенденції споживання, щоб запропонувати клієнтам на основі часу ціноутворення для зменшення споживання у години напруженої

роботи. Ефективне впровадження інтелектуальної мережі вимагає комунікаційної мережі, яка забезпечує швидку передачу даних, має високу надійність, низьку затримку, підключення величезної кількості пристроїв і високу безпеку. Мобільна мережа – найкраща серед інтелектуальних розумних мереж.

Розумні електромережі вдосконалюються, і замість того, щоб просто звітувати про споживання, подача енергії може керуватися та її контроль може здійснюватися за допомогою шлюзу мережі. Сумісність споживача електроніки з системою енергоменеджменту є необхідною умовою. Шлюз керування – це інтерфейс між інфраструктурою попереднього вимірювання та побутовою технікою.

У цьому випадку можна зменшити споживання електроенергії не тільки регулюючи температуру або вимикаючи деякі пристрої у години підвищеного навантаження, є також можливість повідомити клієнта, якщо енергоспоживання певних пристроїв збільшилося. Безперервно, збираючи спожиту електроенергію побутовою електронікою пристроїв, інтелект можна покращити за допомогою аналітики даних і на їх основі спрогнозувати попит на електроенергію. Проаналізувавши дані, можна зробити висновок, що на основі використання електроенергії та її виробництва є можливість завчасно збільшити або зменшити витрати, тим самим зменшити експлуатаційні витрати.

Використання в інфраструктурах інформаційно-комунікаційних технологій та взаємопов’язаних систем у розумній мережі призведуть до великої поверхні для атак ззовні. Компроміс в інтелектуальній мережі може призвести до руйнівних наслідків і зупинити все місто. Отже, це має першочергове значення для реалізації безпеки інтелектуальної мережі на різних рівнях і мобільної мережі, де функції безпеки підвищать загальну безпеку інтелектуальної мережі.

Існують інші сфери інтелектуальної мережі, такі як виробництво електроенергії, мережа передачі, зберігання енергії, розподілені джерела енергії та розподілені генерування електроенергії. Також є багато варіантів використання, які можна реалізувати за допомогою доменів інформаційно-комунікаційних технологій, які підключені за допомогою мобільної мережі.

Мережева технологія мобільної мережі сприймається як засіб Індустрії 4.0 (схема 2.2) і розумних фабрик. У розумній фабриці існує багато різних кейсів, які незабаром будуть реалізовані за допомогою функцій мобільної мережі, таких як низька затримка та надійний зв'язок, підключення мільйонів пристроїв, висока пропускна здатність, високий рівень безпеки спілкування.

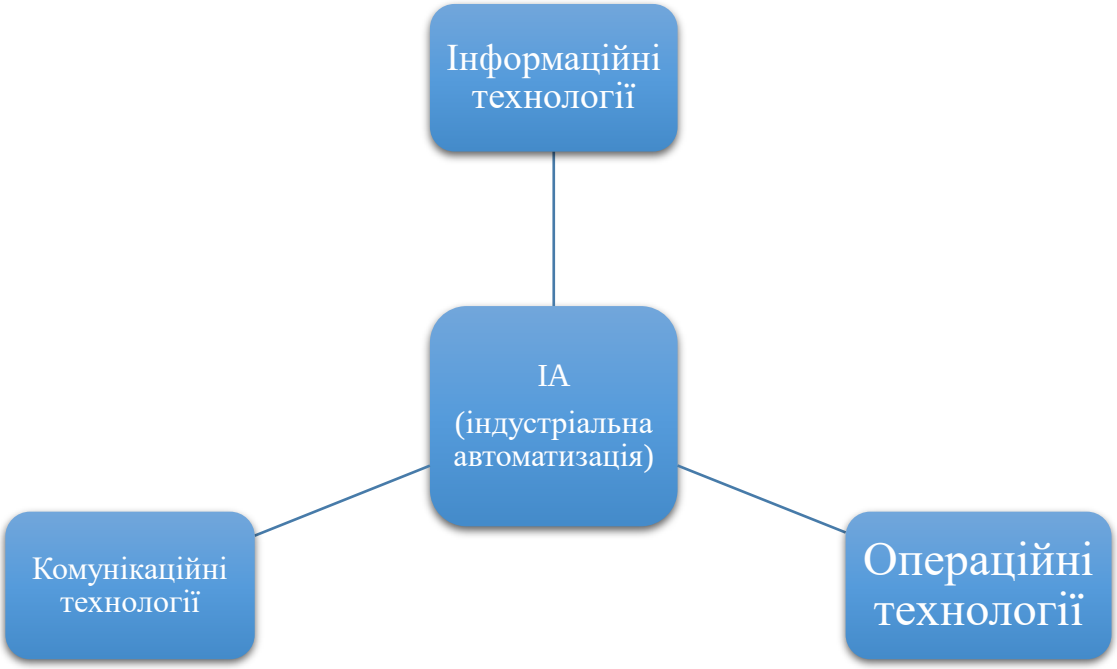


*Схема 2.2. Реалізація Індустрії 4.0 за допомогою промислової автоматизації*

Деякі з цих випадків використання згадані вище та описані нижче:

***Прогнозоване технічне обслуговування:*** датчики машин, прилади та польові пристрої надсилають дані до середовища та машинних додатків IoT через регулярні проміжки часу і, за допомогою цих пристроїв, температуру, тиск, вологість, швидкість, оберти, напругу, час обробки, знос інструменту та інші пов'язані дані, зібрані та засновані на цій аналітиці даних, можливо передбачити, коли і де потрібно технічне обслуговування. За допомогою збору

даних перехід від реактивного технічного обслуговування до проактивного планування технічного обслуговування, буде дуже корисним з точки зору економії операційних витрат і покращить безпеку шляхом мінімізації аварій.

***Постачання та відстеження доставки:*** постачання сировини від постачальника до промисловості та доставку продукції клієнтам можна відстежувати за допомогою служб на основі мобільного зв'язку, де доставка або постачальник оснащені спеціальним SIM-обладнанням (Subscriber Identification Module) для відстеження, яке надсилає дані про місцезнаходження через регулярні проміжки часу або запити від програми IoT. У багатьох випадках доставка або постачання з території, яка не охоплена галузевою мережею мобільного зв'язку, буде використовуватиметься технологія eSIM (Embedded Subscriber Identification Module) із можливістю роумінгу.

***Керування запасами:*** відстеження запасів за допомогою датчиків, встановлених у магазинах. Вони відстежують інвентаризацію сировини або готових товарів. Датчики, які встановлені на ящиках або стелажах, зберігають інформацію, надсилають статус кількості товару у застосунки IoT, які у подальшому відстежують інвентаризацію. Одним із подібних випадків використання є міські сміттєві баки, які оснащені пристроями відстеження, що надсилають інформацію до застосунку IoT про те, наскільки заповнений сміттєвий бак, і на основі цієї інформації компанія, до якої належить цей бак, буде вживати відповідних заходів щодо скорішого спустошення його від відходів.

***AGV і керування рухом роботів:*** сценарій використання автоматичних керованих транспортних засобів (AGV, Automatic Guided Vehicles) на розумній фабриці для транспортування і завантаження/розвантаження матеріалів у промисловості буде реалізовано найближчим часом за допомогою мобільних мереж. Використання роботів дуже поширене у промисловості, і керування рухами роботів за допомогою мобільної мережі з віддаленої

диспетчерської є відносно новою потребою. І AGV, і контроль руху робота вимагають дуже низької затримки, надійної та безпечної мережі зв’язку; тому мобільна мережа найкраще підходить для цих потреб.

Варіанти використання Індустрії 4.0 можуть бути реалізовані за допомогою всіх операційних технологій, комунікаційних та інформаційних. Варіанти використання розумних фабрик реалізуються для підвищення безпеки, продуктивності та ефективності у галузі. Основним фокусом усіх галузей є безпека людських ресурсів, захист активів, інформаційна безпека та стійкість.

Як згадувалося раніше, безпека є дуже пріоритетною на фабриці, оскільки порушення безпеки може призвести до втрати життя або шкоди людського здоров’я. Існує також компроміс між безпекою та затримкою. Затримка, додана механізмом захисту шифрування та цілісності. Функції безпеки мобільного зв’язку є дуже гнучкими і можуть бути реалізовані там де це потрібно.

2.11. Аналіз проблем забезпечення безпеки IoT-пристроїв.

***У ході аналізу було виявлено низку проблем безпеки IoT-пристроїв (схема 2.3).***

***Відсутність належного керування життєвим циклом продукту.***

У даний час жодного підходу до забезпечення безпеки в IoT, ні загальної моделі безпеки, розробленої за участю всіх зацікавлених сторін, не існує. Більшість компаній та виробників використовують власний підхід до забезпечення безпеки в IoT, що призводить до відсутності або, у кращому випадку, уповільненому прийняттю стандартів безпеки IoT. Варто враховувати і той факт, що у різних сферах застосування до технології висуваються різні вимоги безпеки.

Потрібно вирішити ще одну важливу проблему – відсутність відповідальності як моральної, так і юридичної. Її можна вирішити, змусивши виробників виконувати свої обов’язки щодо безпеки продуктів чи послуг. У

даний час неможливо забезпечити ідеальну ізоляцію між різними елементами екосистеми IoT, які розробляються різними виробниками та експлуатуються різними сторонами. У зв'язку з цим, необхідно уточнити відповідальність кожного учасника у разі виникнення загрози безпеці.

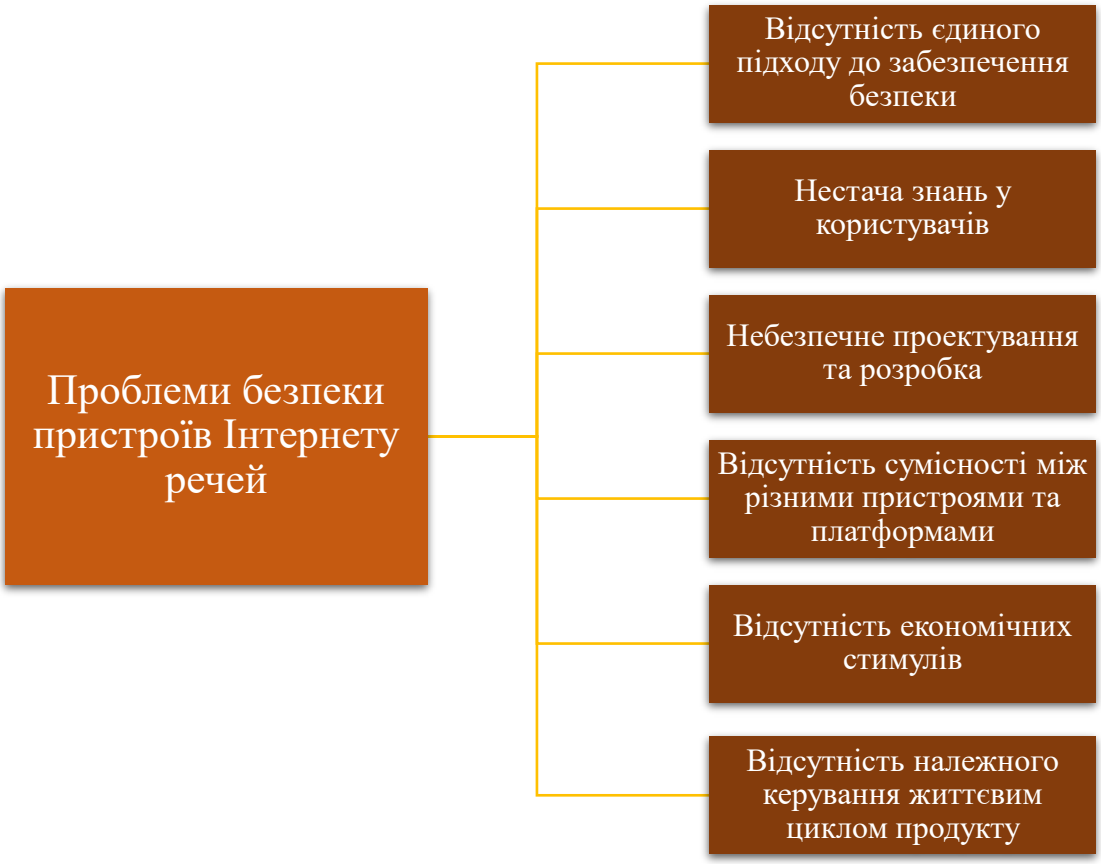


*Схема 2.3. Проблеми безпеки пристроїв IoT*

***Недолік проінформованості та знань у користувачів***.

У зв'язку з масштабним переходом до підключених пристроїв та взаємозалежних систем брак знань відчувається особливо гостро. Під час інтерв'ю з експертами в області IoT було виявлено, що у фундаментальній термінології існує різниця між поняттями «безпека» та «захищеність». Експерти з безпеки знайомі зазвичай з безпекою бізнес-IT, але не саме з безпекою IoT.

Загалом відсутнє розуміння необхідності забезпечення безпеки у пристроях IoT. Велику тривогу викликає відсутність знань про загрози, яким

піддаються ці пристрої – більшість споживачів IoT не мають базового уявлення про свої IoT-пристрої та принципи їх безпеки. Тому пристрої не оновлюються, що може спричинити порушення безпеки.

Компанії мають навчати своїх співробітників передовим методам забезпечення безпеки, усвідомлюючи, що технологічний досвід не завжди прирівнюється до досвіду у сфері безпеки. Загалом необхідно інформувати нове покоління споживачів, розробників, виробників тощо; про використання IoT та пов'язані з ним ризики безпеки. Багато інцидентів безпеки можна було б уникнути, якби розробники та виробники знали про ризики, з якими вони стикаються щодня. Необхідно підвищувати рівень знань про поточні загрози та ризики, інформуючи про те, як запобігати інцидентам, захищати IoT та діяти у разі виникнення загрози безпеки.

***Небезпечне проектування та розробка***.

У контексті проектування та розробки IoT, видаються особливо важливими наступні питання:

- відсутність стратегії глибокого захисту під час проектування системи, такої як безпечний процес завантаження, ізоляція довіреної обчислювальної бази, обмеження кількості відкритих портів, самозахист тощо;
- відсутність безпеки чи конфіденційності під час проектування. У деяких випадках відбувається обмін інформацією з третьою стороною, і слід переконатися, що за межі IoT-середовища експортується не більше інформації, ніж це необхідно;
- відсутність захисту зв'язку як на внутрішніх, так і на зовнішніх інтерфейсах;
- відсутність надійної аутентифікації та авторизації (немає перевірки чи підпису оновлень прошивки, оновлення програмного забезпечення без автентифікації сервера та достовірності файлів, механізмів безпечного завантаження);

- відсутність захисту у прошивці (не застосовуються технології запобігання передачі даних або пом’якшення наслідків атак, публічні вразливості не виправляються, деякі послуги відкриваються через різні точки входу, при цьому, нікому непотрібні комунікаційні порти залишаються відкритими – такі послуги, як Telnet або SSH, іноді прив’язані до всіх мережевих інтерфейсів, використовуються слабкі паролі або стандартні паролі (за замовчуванням), які залишені без змін).

***Відсутність сумісності між різними пристроями та платформами IoT.***

Переважна більшість IoT-екосистем включають пристрої IoT, які пов’язані із застарілими системами, особливо у критично важливих інформаційних інфраструктурах. Більше того, як згадувалося раніше, через відсутність єдиного підходу більшість компаній та виробників використовують власний підхід під час розробки пристроїв IoT, що призводить до проблем сумісності між пристроями різних виробників, а також до появи різних моделей безпеки, несумісних концепцій і т. д. Тому дуже важливо розробити заходи, які забезпечують правильне та безпечне з’єднання, взаємодію між середовищем IoT та успадкованими системами, а також іншими IoT-пристроями, виготовленими сторонніми виробниками.

Більшість IoT-пристроїв використовують власні протоколи зв’язку, які розроблені їх виробниками. Навіть якщо це не є проблемою для пристроїв одного виробника, це стає проблемою при з’єднанні пристроїв різних виробників. Необхідно розробляти та використовувати стандартні протоколи, які мають підтримуватись усіма виробниками для забезпечення гарного рівня сумісності з найменшими втратами ефективності та безпеки. Гарною практикою у цьому відношенні є відмова від використання протоколів із закритим вихідним кодом, оскільки їхню безпеку неможливо перевірити. Крім протоколів, у яких використання загальних рамок також може допомогти

підвищити ефективність та безпеку при з’єднанні кількох пристроїв різних виробників.

***Відсутність економічних стимулів***.

Основні виробники та постачальники IoT зазвичай вважають функціональність та зручність використання важливішими, ніж безпечне проектування та програмування. Не в їх економічних інтересах витрачати багато грошей на безпеку, а в деяких випадках вони взагалі не розглядають питання безпеки. Компанії не виділяють кошти на безпеку тому, що на загальну думку, ці кошти не повертаються, це можна пояснити складністю оцінки фінансових наслідків гіпотетичних недоліків у системі безпеки.

Ситуація посилюється відсутністю економічних стимулів, які б могли сприяти підвищенню безпеки, таких як економічні вигоди (наприклад, збільшення кількості грантів для забезпечення більшої безпеки у пристроях), ресурси, передбачувана репутація тощо.

Різні ризики, загрози та небезпеки зазвичай недооцінюються і не враховуються через бюджетні проблеми, бо існує тенденція вирішувати проблеми безпеки після інцидентів.

***Відсутність належного керування життєвим циклом продукту***.

Загалом, заходи безпеки виявляються недостатніми, починаючи з етапу проектування та закінчуючи її подальшою розробкою. Для різних активів, складових, дане IoT-середовище потребує належного керування життєвим циклом продукту, оскільки пристрої та мережі взаємопов’язані і, у більшості випадків, відкриті для доступу з глобальної мережі Інтернет, де вони можуть стати ціллю для безлічі різноманітних загроз.

IoT включає у себе таку різноманітність продуктів, що, якщо залишити їх поза увагою, вони зроблять уразливим весь ланцюжок постачань. IoT розширює глобальну поверхню атаки, і кожен виробник відповідає за керування ризиками. Різні пристрої і продукти повинні розвиватися безпечним

способом, щоб постійно забезпечувати протягом усього свого життєвого циклу рішення, для якого вони були створені.

У цей процес необхідно залучити постачальників, а оскільки саме вони відповідають за проектування та розробку пристроїв, це їхня прерогатива реалізувати необхідні зміни – вони можуть кваліфіковано і з мінімальними витратами включати нові функції чи характеристики безпеки. Але, однак, це залежить не тільки від виробників, які додають нові функції, а й від організацій, які приймають пов’язані з цим витрати, отже, баланс між безпекою та вартістю повинен бути збережений.

Протягом усього життєвого циклу IoT-пристрою він повинен мати можливість швидкого виправлення та оновлення, щоб забезпечити правильну роботу та усунути усі виявлені уразливості. Як згадувалося раніше, у більшості користувачів немає базових знань про IoT-пристрої та їх вплив на середовище, у результаті цього, пристрої не оновлюються і, відповідно, залишаються вразливими до нових загроз.

Крім того, одним із важливих етапів керування життєвим циклом пристрою є етап розгортання. Можна розробити рекомендації щодо розгортання IoT. Вони включатимуть рекомендації щодо конкретних конфігурацій пристроїв та мереж.

## 2.12. Висновки до розділу.

Інтернет речей стає новою тенденцією у наші дні. Оскільки підключення до глобальної мережі Інтернет стає все доступнішим, кожен може дозволити собі екосистему Інтернету речей прямо у себе вдома. При такому розвитку подій передача та зберігання інформації зіштовхуються із серйозними проблемами, такими як крадіжка даних з пристроїв IoT, використання таких пристроїв для DDoS-атак, стеження за користувачами і т. д. Тому безпека пристроїв Інтернету речей стає другорядним або може стати першорядним завданням при виробництві більшості таких пристроїв.

Щоб убезпечити Інтернет речей, крім використання досконаліших протоколів чи ліквідації вразливостей, необхідно досягти наступного: перше – використовувати окрему локальну мережу для підключення всіх пристроїв Інтернету речей між собою; і друге, складніше – змусити виробників «розумних речей» не використовувати загальнодоступні методи скидання налаштувань, облікові записи та паролі при виробництві таких пристроїв.

# РОЗДІЛ 3. ПОБУДОВА ТА ПРОЕКТУВАННЯ МОБІЛЬНОЇ МЕРЕЖІ В ПРОГРАМНОМУ ЗАСТОСУНКУ CISCO PACKET TRACER 8.2

## 3.1. Загальна схема мережі.

Було поставлено завдання розробити інтелектуальну мережу на основі двох офісів. Потрібно було під’єднати до базових станцій смартфони та налаштувати їх підключення конкретно до свого офісу. Спеціалізовано обладнаний комплекс, розміщений на території загальною площею 0,3 га, як показано на рис. 3.1. На даній території розміщено житловий двоповерховий будинок, в якому знаходяться два офіси на першому поверсі, в яких працюють по три особи у кожному. Всі службові кабінети обладнані під застосування технічних засобів підприємства.

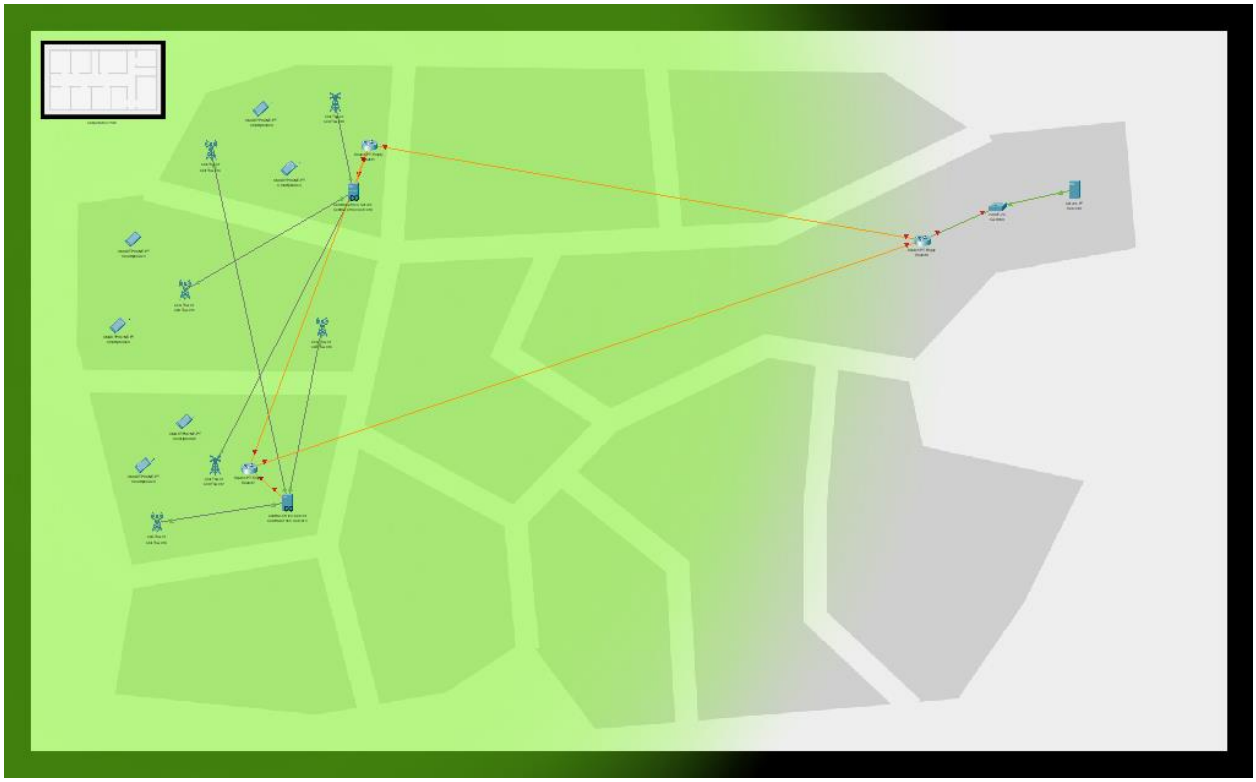

*Рис. 3.1. Загальна фізична схеми мережі*

На рисунку 3.1 зображена схема мережі двох офісів які з’єднані між собою комутаторами. У кожному офісі є по три внутрішні базові станції для рівномірного розподілу сигналу та навантаження між клієнтами мережі. Також у кожному офісі знаходяться по три смартфони, які підключені до кожної у своїх офісах внутрішніх базових станцій. У кожному офісі є свій

сервер, який отримує та обробляє дані усіх користувачів які до нього під’єднані та взаємодіють із ним.

3.2. Побудова мобільної мережі.

У кожного офісу був свій сервер, який був з’єднаний ззовні з роутером, який у подальшому був під’єднаний до іншиї двох ліній інших двох роутерів.

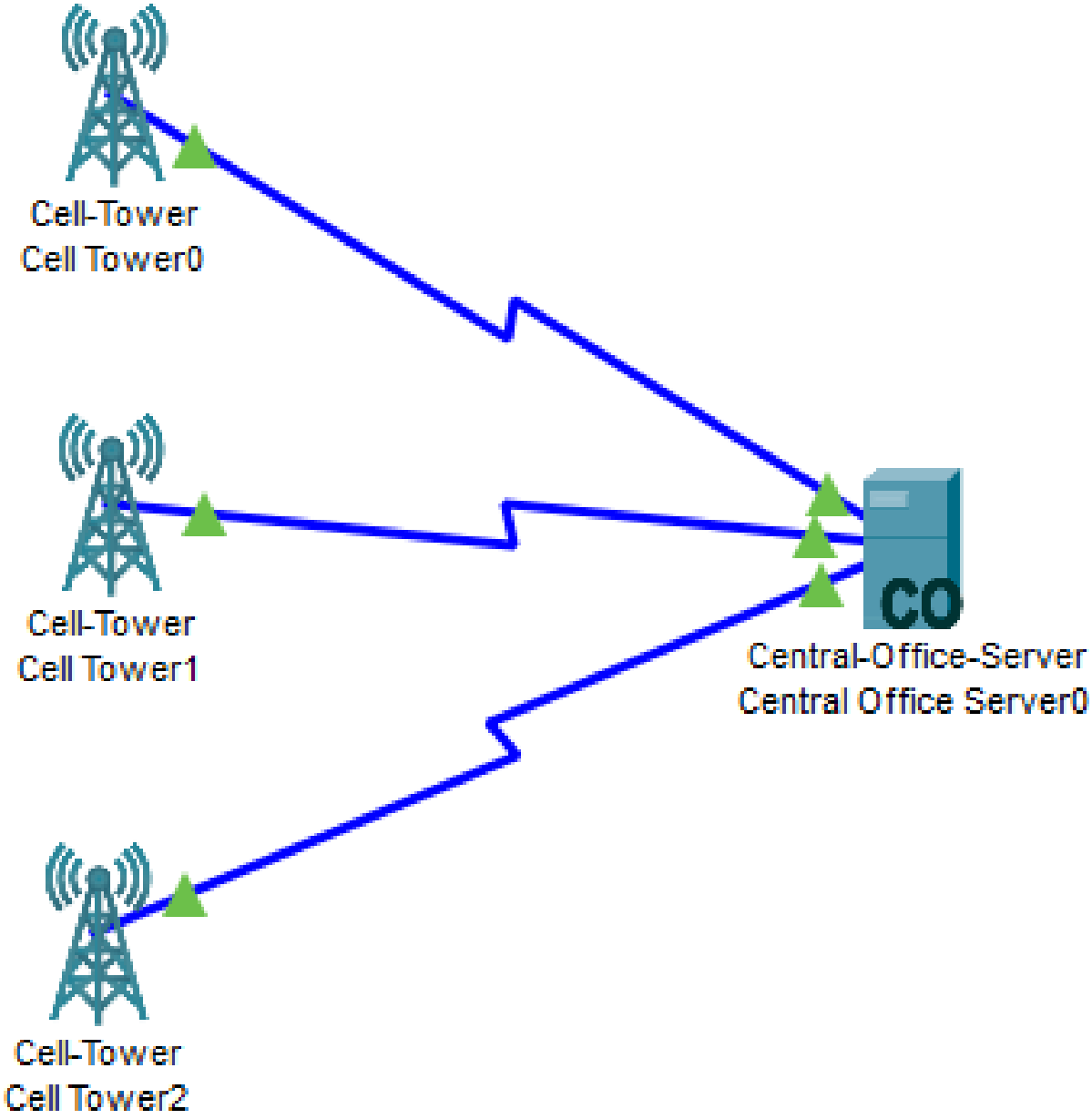


*Рис. 3.2. Проектування загальної логічної схеми першої мережі*

На рисунку 3.2 зображено три базові станції які підключені до сервера обробки даних.

Кожна базова станція має свою кодову назву провайдера, тому і на смартфонах було налаштоване підключення саме до тих базових станцій, які були розташовані у межах одного офісу, як показано на рис. 3.3.

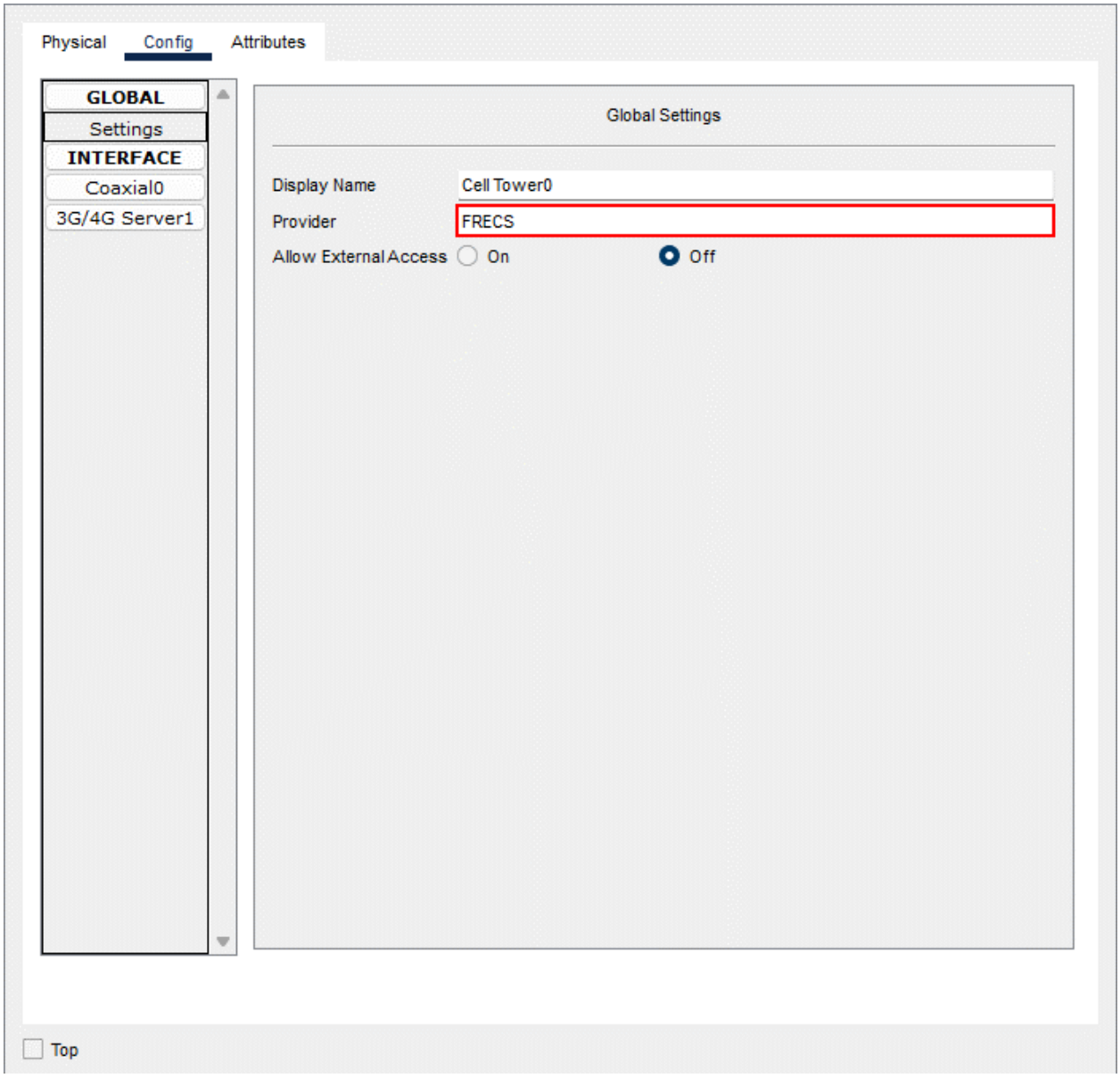


*Рис. 3.3. Зміна імені провайдера за замовчуванням (ptcellular) на FRECS*

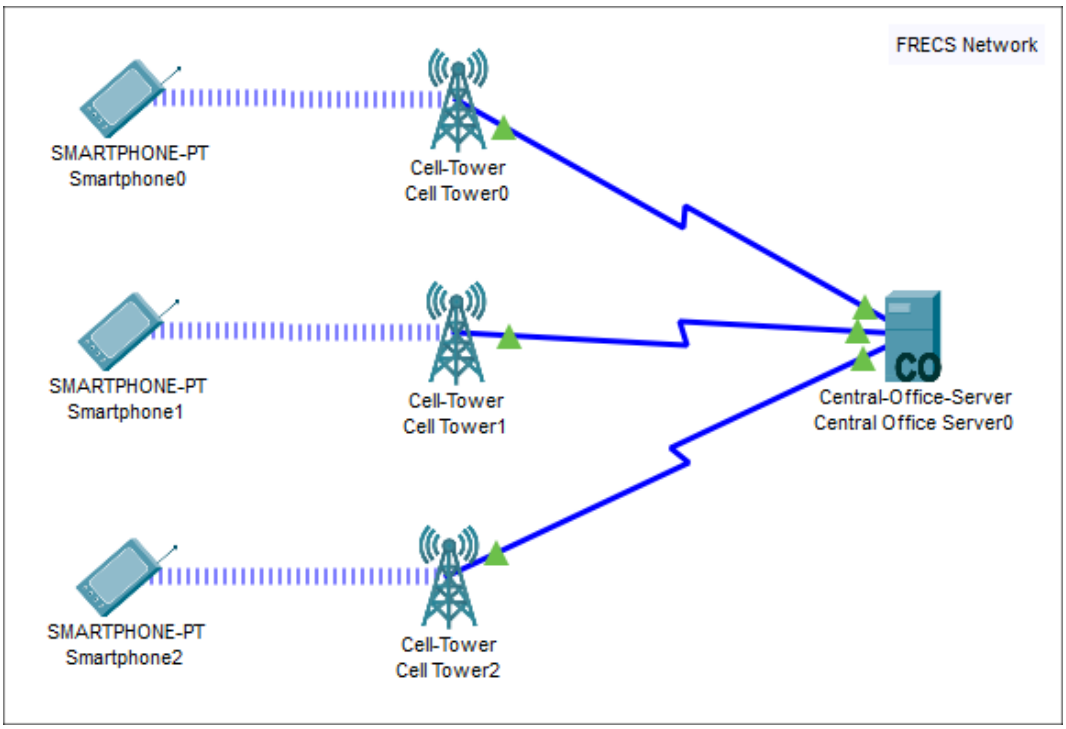


*Рис. 3.4. Додання трьох розумних пристроїв (смартфонів) до існуючої мережі*

На рис. 3.4 та рис. 3.5 додано по три смартфони співробітників офісу.

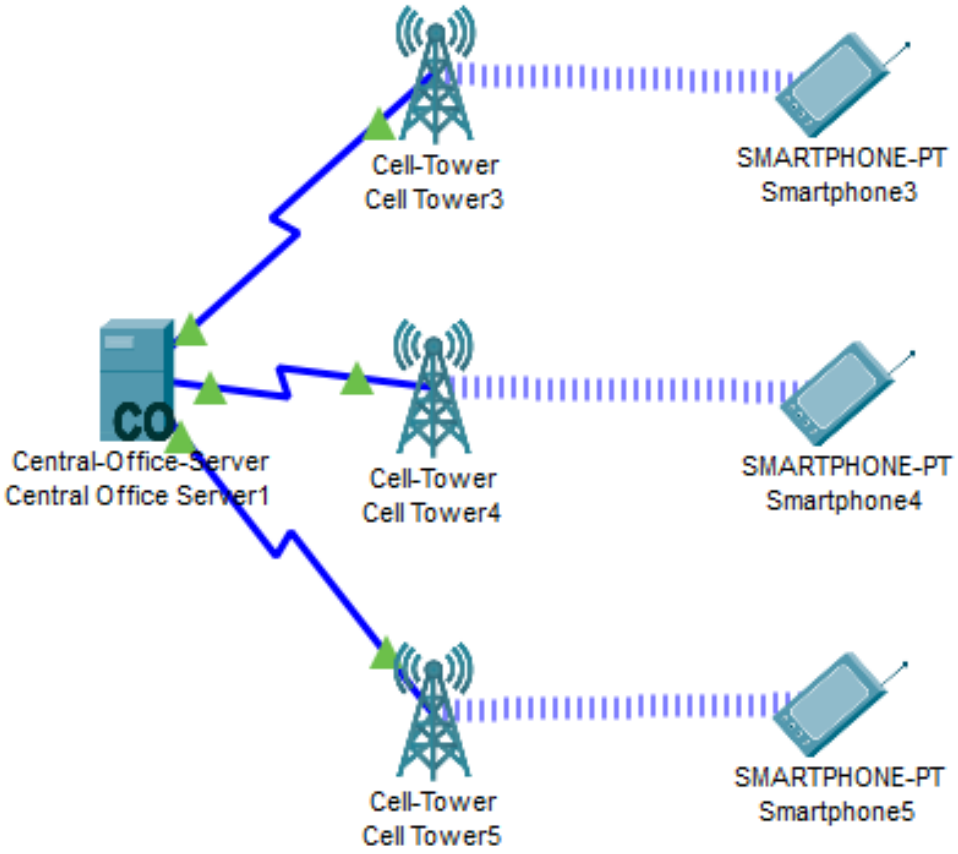


*Рис. 3.5. Проектування загальної логічної схеми другої мережі*

Потім було виконано додання першого роутера до другої мережі та його налаштування перед першим запуском.

Ще одним завданням було додавання портів на роутері, аби можна було встановити з’єднання між кожним із них та офісами (рис. 3.6).

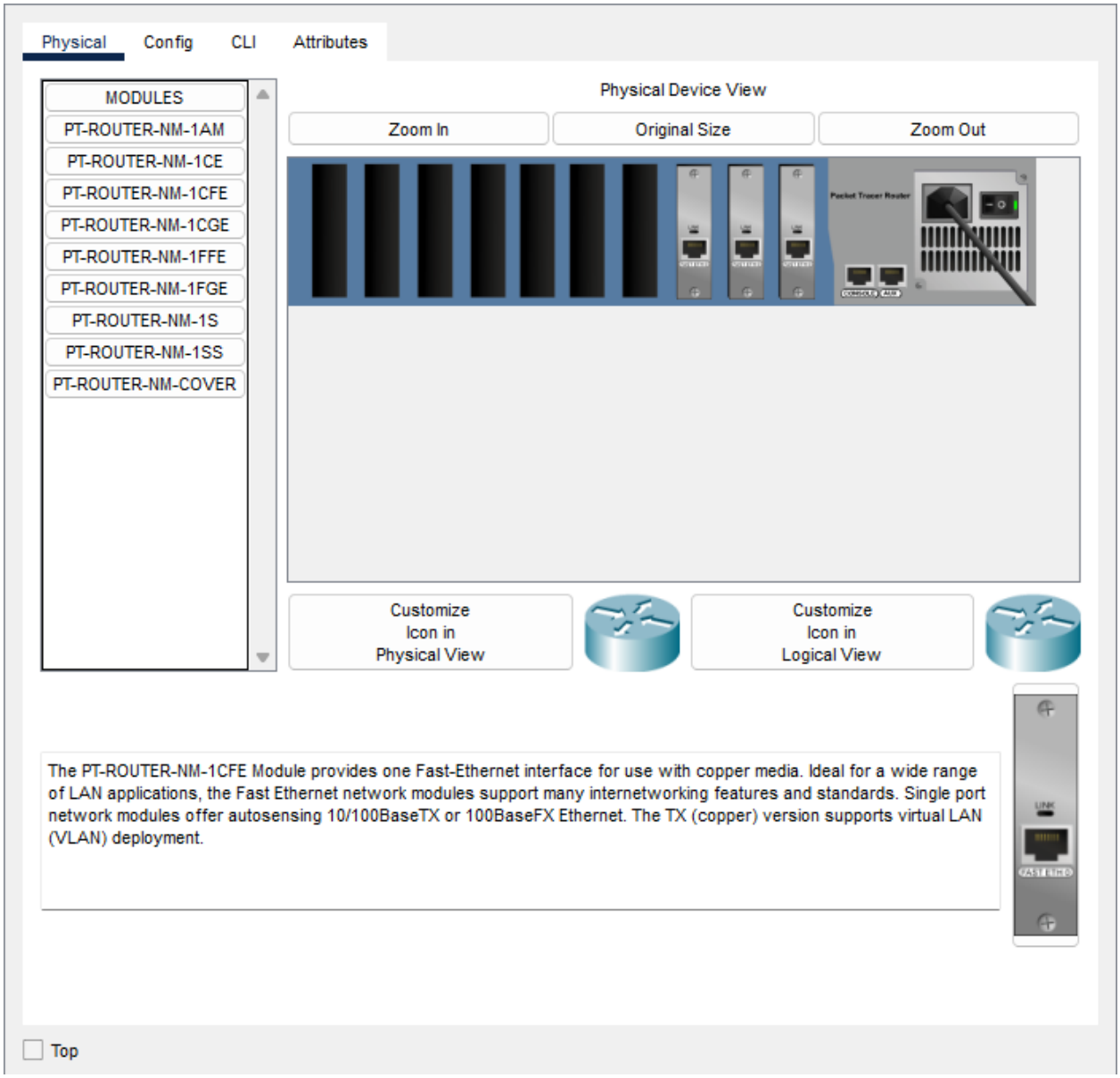


*Рис. 3.6. Додання трьох портів Ethernet до першого, другого та третього роутера другої мережі*

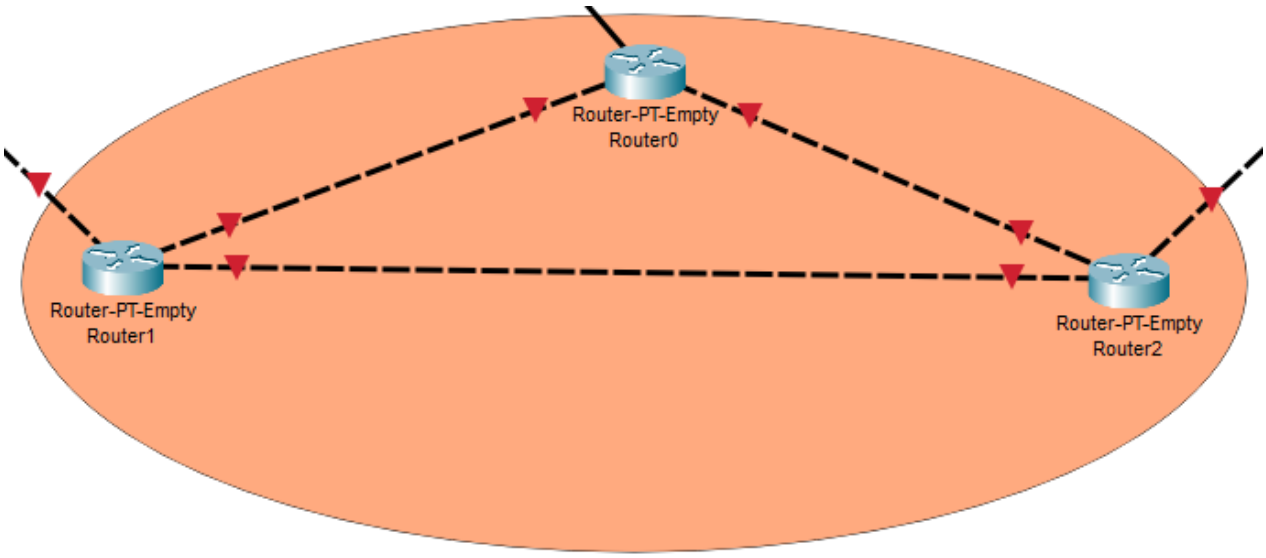


*Рис. 3.7. Налаштування з'єднання між трьома роутерами*

На рис. 3.7 було об'єднано три роутери в одну мережеву сітку для з'єднання між собою двох офісів.

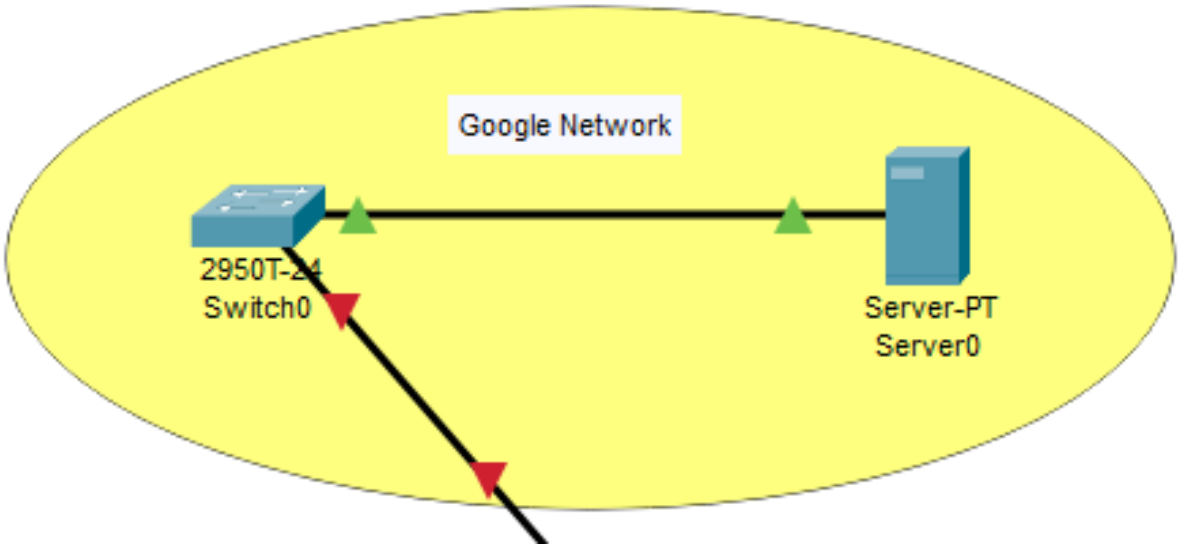


*Рис. 3.8. З'єднання мережі із сервером Google*

Завершальним етапом було підключення офісів до глобальної мережі Інтернет (рис. 3.8). Але перед самим виходом до глобальної мережі Інтернет було встановлено керований комутатор з функцією фільтрації трафіку від шкідливих запитів, а також була встановлена та налаштована система для захисту від DDoS-атак. Фінальний вигляд схеми зображений на рис. 3.9.

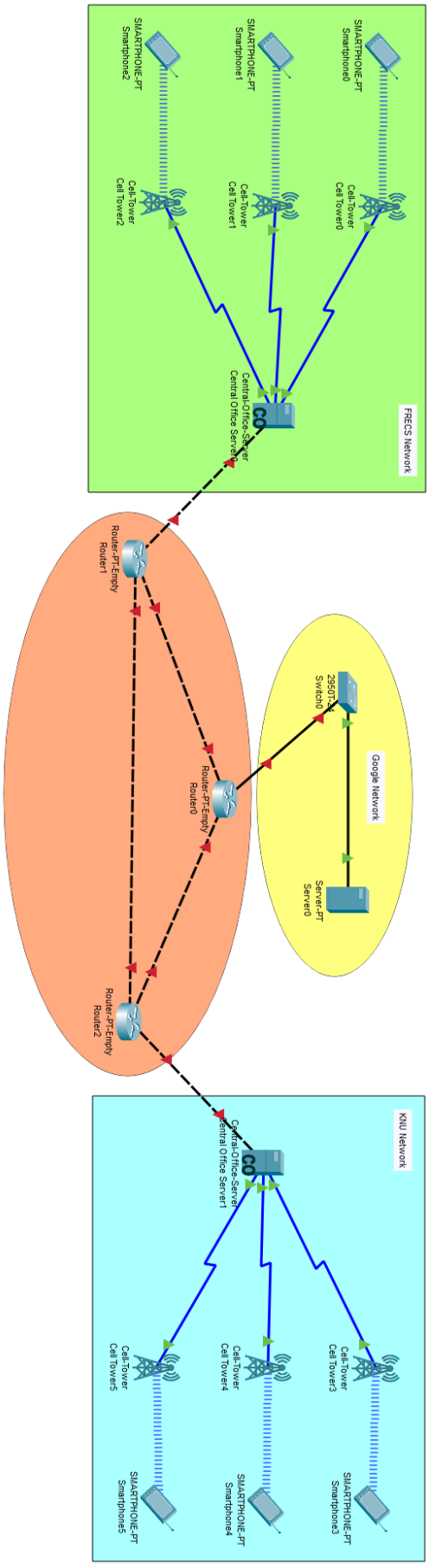


*Рис. 3.9. Загальний вигляд об'єднання двох мереж*

# ВИСНОВКИ

У даній роботі був представлений проведений аналіз проблем безпеки Інтернету речей. Визначено складові технології IoT, розглянуто сфери її застосування та складена класифікація загроз.

Також було розглянуто заходи та проведено дослідження по забезпеченню комплексної безпеки технологій Інтернету речей у бездротовому сегменті.

Питання забезпечення безпеки в IoT знаходиться на стадії розробки. Виявлені проблеми були визначені як найбільш значущі шляхом проведення порівняльного аналізу існуючих ресурсів безпеки IoT.

Кінцева мета усунення проблем захисту та безпеки IoT полягає у тому, щоб забезпечити пріоритет усіх технологій, зберегти необхідний рівень конфіденційності, а також досягти та підтримувати високий рівень стійкості до атак, таким чином забезпечуючи комплексну безпеку.

Головним завданням дипломної роботи було моделювання мережі між двома офісами та налаштування їх роботи з розумними пристроями (смартфонами). Було відокремлено кожний розумний пристрій до своєї зони та до своєї конкретної внутрішньої базової станції. Моделювання було успішно проведене та перевірене у роботі на симуляції передачі пакетів. Основним середовищем для розробки і проектування мережі двох офісів був програмний застосунок від відомої мережевої компанії Cisco, а саме Cisco Packet Tracer 8.2.

Правильна організація локальної мережі підприємства забезпечить значний розвиток як самого підприємства так і його співробітників, допоможе ефективніше організувати робочий процес, скоротить терміни перевірки даних, спростить завдання як керівникам так і співробітникам підприємства. Підвищить організованість, системність, цілісність підприємства та рівень спроможності співробітників.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Chui M., Löffler M., Roger R. The Internet of Things // McKinsey Quarterly: [magazine]. 2010.01 March URL: http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things (date of access: 04.03.2023).
2. Cisco, “Cisco Annual Internet Report 2018-2023”, 2020. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html (date of access: 12.03.2023).
3. Grover J. Android forensics: Automated data collection and reporting from a mobile device // Digital Investigation. 2013. Vol. 10, Supplement. P. S12–S20. doi: 10.1016/j.diin.2013.06.002.
4. I. Analytics, “State of the IoT 2018: Number of IoT devices now at 7B.” https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/ (date of access: 15.04.2023).
5. Internet of Things – From Research and Innovation to Market Deployment / O. Vermesan, P. Friess. Aalborg, Denmark: River Publishers, 2014. 373 p. (River Publishers Series in Communications). URL: https://www.riverpublishers.com/pdf/ebook/RP_E9788793102958.pdf (date of access: 22.04.2023).
6. Internet of Things Forensics – Challenges and a Case Study / S. Alabdulsalam [et al.] // Advances in Digital Forensics XIV / G. Peterson, S. Shenoi (eds.). Cham: Springer, 2018. P. 35–48. (IFIP Advances in Information and Communication Technology; vol. 532). https://doi.org/10.1007/978-3-319-99277-8_3.
7. M. Shrestha, C. Johansen, J. Noll, and D. Roverso, “A Methodology for Security Classification applied to Smart Grid Infrastructures,” Int. J. Crit. Infrastruct. Prot., vol. 28, p. 100342, 2020, doi: https://doi.org/10.1016/j.ijcip.2020.100342 (date of access: 29.04.2023).

8. Minerva R., Biru A., Rotondi D. Towards a definition of the Internet of Things (IoT). IEEE 2015 URL: http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf (date of access: 01.04.2023).
9. Nieto A., Roman R., Lopez J. Digital Witness: Safeguarding Digital Evidence by Using Secure Architectures in Personal Devices // IEEE Network. 2016. Vol. 30, no. 6. P. 34–41. doi:10.1109/MNET.2016.1600087NM.
10. Protecting digital data privacy in computer forensic examination / F. Y. W. Law [et al.] // Proceedings of the 2011 IEEE Sixth International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE). Oakland, CA, USA, 2011. P. 1–6. doi:10.1109/SADFE.2011.15.