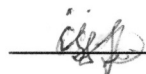


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Проект підсистеми захисту мережної інфра-
структури IoT-системи»

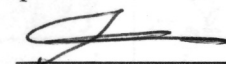
Виконав студент 4-го курсу групи КБ-19-1
спеціальності 125 «Кібербезпека»

 Ілля Савченко

Керівник доцент кафедри КІ та КБ, к.т.н, доцент,

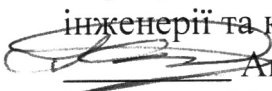
 Юрій Бродський

Рецензент доцент кафедри КІ та КБ, к.т.н, доцент,

 Юрій Россінський

Житомир – 2023

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ
Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки
 Андрій Єфіменко
1 березня 2023 р.

ЗАВДАННЯ
на випускню кваліфікаційну роботу бакалавра

Студент: Савченко Ілля Васильович

Тема роботи: «Проект підсистеми захисту мережної інфраструктури IoT-системи»

затверджена Наказом університету від 1 березня 2023 р. № 98/с

Термін здачі студентом закінченої роботи 30 червня 2023 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

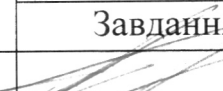
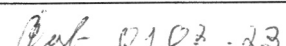
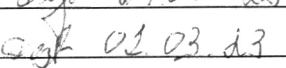
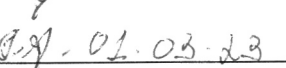
-IoT-системи;

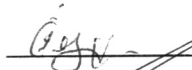
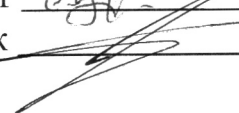
-Мережева інфраструктура;

Обладнання та програмне забезпечення:

1. Емулятор Cisco Packet tracer.
2. Емулятор GNS3.

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Юрій Бродський	 01.03.23	 01.03.23
2	Юрій Бродський	 01.03.23	 01.03.23
3	Юрій Бродський	 01.03.23	 01.03.23

Студент  Савченко Ілля
Керівник  Юрій Бродський

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	01.03.2023	Виконано
2	Визначення цілей та обсягу проєкту	16.03.2023	Виконано
3	Аналіз сучасних технологій захисту IoT-систем	10.04.2023	Виконано
4	Вибір та налаштування VPN-рішення	25.04.2023	Виконано
5	Дослідження наукових статей	05.05.2023	Виконано
6	Аналіз результатів та оцінка ефективності	15.05.2023	Виконано
7	Захист мережевих вузлів та серверів	20.05.2023	Виконано
8	Розробка механізму аутентифікації для IoT-систем	28.05.2023	Виконано
9	Тестування та аналіз безпеки	15.06.2023	Виконано
10	Оформлення документації	30.06.2023	Виконано

Студент  Савченко Ілля

Керівник  Юрій Бродський

АНОТАЦІЯ

Кваліфікаційна робота складається з проекту підсистеми захисту мережної інфраструктури IoT-системи розробленого в двох частинах основний проект в GNS3 та безпроводна його частина в Cisco Packet Tracer, його реалізації та пояснювальної записки до нього. Пояснювальна записка містить 58 сторінок та 19 ілюстрацій.

Метою роботи є розробити проект підсистеми захисту мережної інфраструктури IoT-системи.

В роботі розкрита структура, сфери застосування та кіберзагрози для IoT-систем. Розроблений проект підсистеми захисту мережної інфраструктури IoT-системи в розумному будинку.

Ключові слова: IOT, VPN, NAT, МЕРЕЖНА ІНФРАСТРУКТУРА, СИСТЕМА ЗАХИСТУ, КІБЕР ЗАГРОЗИ.

ККІКБ.КР.Б – 125 – 15 – ПЗ

Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Савченко І.В.		29.06.23	Проект підсистеми захисту мережної інфраструктури IoT-системи	Літ.	Арк.
Керівник		Бродський Ю. Б.		29.06.23			Аркушів
Реценз.		Росініський Ю. М.		29.06.23			4
Н. контр.		Бродський Ю. Б.		29.06.23		ФІКТ, Гр. КБ-19-1	
Затверд.		Єфіменко А.А.		29.06.23			

ANNOTATION

The qualification paper consists of a project on the subsystem for securing the network infrastructure of an IoT system, developed in two parts: the main project in GNS3 and its wireless component in Cisco Packet Tracer, along with its implementation and explanatory report. The explanatory report comprises 58 pages and includes 19 illustrations.

The aim of this work is to develop a project for the subsystem to secure the network infrastructure of an IoT system.

The paper explores the structure, application areas, and cybersecurity threats for IoT systems. The project for the subsystem to secure the network infrastructure of an IoT system is specifically designed for a smart home.

Keywords: IoT, VPN, NAT, NETWORK INFRASTRUCTURE, SECURITY SYSTEM, CYBER THREATS.

		Савченко І.В			KKIKB.KP.B – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1 АНАЛІЗ ЗАСТОСУВАННЯ ТА БЕЗПЕКИ МЕРЕЖ ІОТ.....	10
1.1 Загальний огляд стану ІоТ систем	10
1.2 Критичні сфери застосування ІоТ.....	13
1.3 Джерела загроз безпеці в ІоТ	18
1.4 Висновки до розділу 1	24
РОЗДІЛ 2 ВИБІР ТИПУ ІОТ-СИСТЕМИ ТА ПРОЕКТУВАННЯ ЇЇ	
ПІДСИСТЕМИ ЗАХИСТУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ	26
2.1 Вибір обладнання	26
2.2 Вибір модельного прикладу ІоТ-системи.....	31
2.3 Загальний опис розробленої мережі та топології	33
2.4 Висновки до розділу 2.....	37
РОЗДІЛ 3 НАЛАШТУВАННЯ ПРОЄКТУ ПІДСИСТЕМИ ЗАХИСТУ	
МЕРЕЖНОЇ ІНФРАСТРУКТУРИ ІОТ-СИСТЕМИ НА ПРИКЛАДІ РОЗУМНОГО	
БУДИНКУ	39
3.1 Налаштування Мережевих екранів	39
3.2 Перевірка прецедентності	48
3.3 Висновки до розділу 3.....	51
ВИСНОВКИ.....	53
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	55
ДОДАТКИ.....	57

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IoT – Internet of things

VPN – virtual private network

NAT – Network Address Translation

CBS – Cyber-physical systems

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Обрана тема проєкту підсистеми захисту мережної інфраструктури Інтернету речей (IoT) є надзвичайно важливою з кількох причин. IoT-системи займають все більш вагому роль у нашому повсякденному житті, застосовуючись у різних галузях, включаючи медицину, транспорт, енергетику та багато інших.

Проєкт підсистеми захисту мережної інфраструктури IoT-системи має на меті вирішення цих проблем. Шляхом розробки та впровадження механізмів захисту, таких як шифрування, аутентифікація, контроль доступу та виявлення вразливостей, можна підвищити рівень безпеки IoT-систем. Це допоможе запобігти атакам, зберегти конфіденційність особистих даних, забезпечити надійність роботи системи та зберегти довіру користувачів до Інтернету речей.

Отже, обрана тема є важливою, оскільки вона спрямована на забезпечення безпеки, приватності та надійності IoT-систем, що є основними складовими для успішного розвитку та прийняття цієї технології у всіх сферах нашого життя.

Метою кваліфікаційної роботи є розробка та впровадження ефективної підсистеми захисту мережної інфраструктури Інтернету речей (IoT-системи). Ця мета передбачає виконання наступних завдань:

- Розробку механізмів і методик, що забезпечують ідентифікацію та усунення потенційних загроз кібербезпеці в IoT-системах.
- Впровадження рішень та технологій для захисту приватності та конфіденційності даних, зібраних в IoT-системах.
- Розробку та впровадження заходів безпеки для бездротових підключень в IoT-системах. Зв'язок між пристроями в IoT-мережах зазвичай здійснюється через бездротові канали зв'язку, такі як Wi-Fi, Bluetooth або Zigbee. Проєкт підсистеми захисту мережної інфраструктури IoT-системи включатиме розробку механізмів шифрування, аутентифікації та захисту від атак, що спрямовані на бездротові підключення, з метою забезпечення безпеки та доступності для несанкціонованих осіб.

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		8

Отже, в рамках кваліфікаційної роботи будуть вирішуватись завдання з розробки та впровадження підсистеми захисту мережної інфраструктури Інтернету речей, що сприятиме забезпеченню безпеки, приватності та надійності IoT-систем.

Об'єктом дослідження є сфера захисту мережної інфраструктури в контексті Інтернету речей (IoT). Ця ширша область охоплює усі аспекти безпеки, приватності та надійності в IoT-системах, включаючи архітектуру мережі, протоколи зв'язку, бездротові технології, обробку та передачу даних, а також захист від кібератак і несанкціонованого доступу. Проєкт підсистеми захисту мережної інфраструктури IoT-системи концентрується саме на цій проблематиці та досліджує специфічні аспекти безпеки в IoT-мережах для створення ефективних рішень та заходів захисту.

Предметом дослідження є проєкт підсистеми захисту мережної інфраструктури Інтернету речей (IoT-системи). Дослідження зосереджується на аналізі, розробці та впровадженні механізмів та рішень, спрямованих на забезпечення безпеки зв'язків у IoT-системах. Основні аспекти, що досліджуються, включають механізми шифрування, аутентифікації, захист від атак та несанкціонованого доступу в IoT-мережах.

У процесі виконання кваліфікаційної роботи було розроблено проєкт підсистеми захисту мережної інфраструктури IoT-системи в розумному будинку.

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 АНАЛІЗ ЗАСТОСУВАННЯ ТА БЕЗПЕКИ МЕРЕЖ ІОТ

1.1 Загальний огляд стану IoT систем

Темп з'єднання фізичних пристроїв навколо нас з Інтернетом швидко зростає. Згідно з останнім звітом IoT Analytics у 2022 році очікувалось, що ринок Інтернету речей зросте на 18% до 14,4 мільярда активних підключень. Очікується, що до 2025 року, коли обмеження пропозиції зменшаться, а зростання прискориться, буде приблизно 27 мільярдів підключених пристроїв IoT. Використання застосунків Інтернету речей зростає у всіх частинах світу. Основними регіонами, що сприяють цьому, є західна Європа, Північна Америка та Китай. Цей стрибок в кількості свідчить про те, що Інтернет речей є одним з найважливіших майбутніх ринків, який може стати основою зростаючої цифрової економіки.

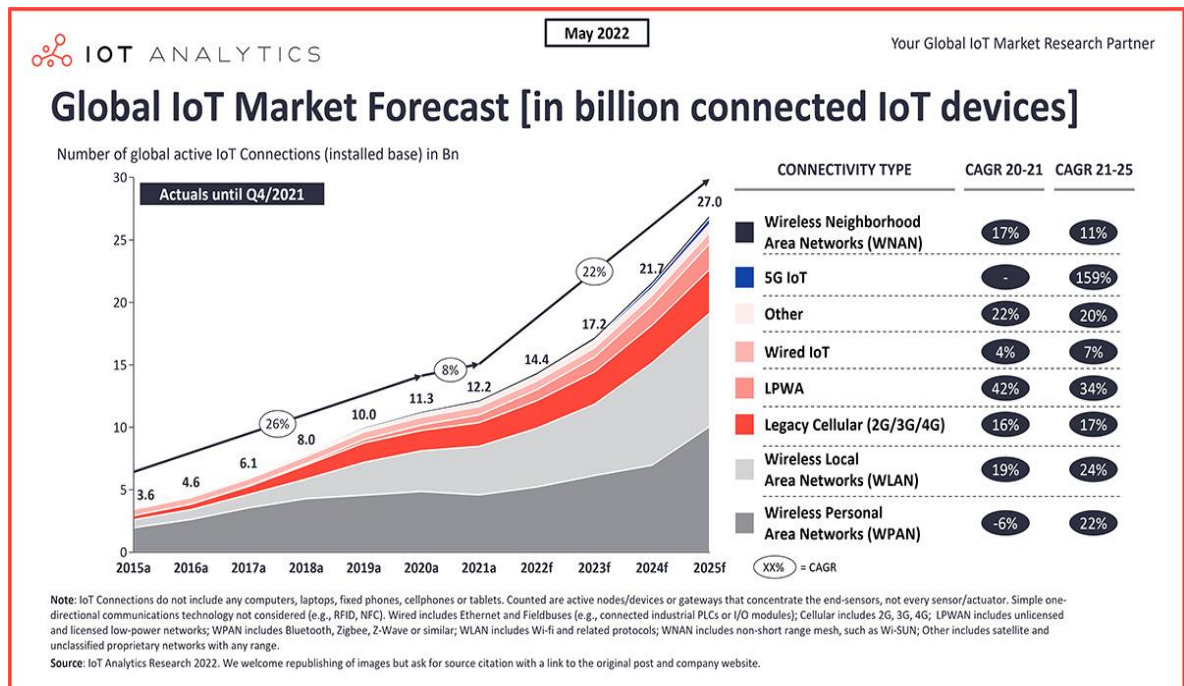


Рисунок 1.1 – Прогноз ринку IoT

Підключення машин-машина охоплює широкий спектр застосунків, таких як розумні міста, розумне середовище, розумні мережі, розумна роздрібна торгівля, розумне сільське господарство та інше. На рисунку 1.2 показана минула, поточна та майбутня архітектура Інтернету речей. У майбутньому очікується, що пристрої будуть не лише підключені до Інтернету та інших локальних пристроїв, але й безпосередньо взаємодіятимуть.

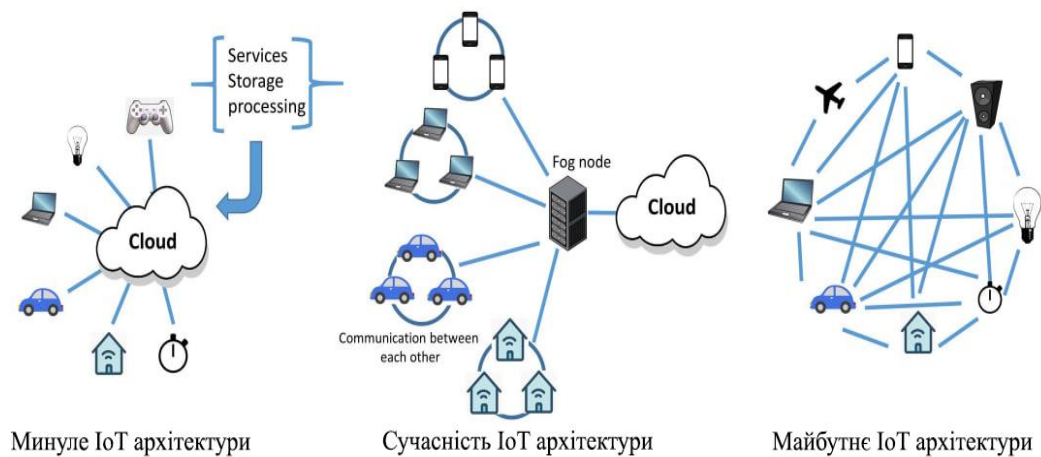


Рисунок 1.2 – минула, поточна та майбутня архітектура IoT

Однак разом із цим широким спектром застосувань Інтернету речей виникають проблеми безпеки та приватності. Відсутність довіри до екосистеми Інтернету речей та несумісність її компонентів можуть призвести до втрати потенціалу та недосягнення високого попиту на нові додатки.

Разом із загальними проблемами безпеки, з якими стикається Інтернет, мобільні мережі та бездротові датчики, Інтернет речей також має свої власні особливі виклики в галузі безпеки, такі як проблеми приватності, аутентифікації, управління та збереження інформації.

Всі ці проблеми і вразливості створюють потенціал для різних видів кіберзагроз. Існує багато прикладів атак на Інтернет речей, таких як атака Mirai, яка заражала мільйони пристроїв і запускала розподілену атаку зі збоєм обслуговування. Також існують приклади ботнет-атак, спрямованих на велику кількість пристроїв Інтернету речей.

Пристрої Інтернету речей, які мають обмежену потужність та меншу безпеку, можуть стати вразливими точками входу для зловмисників у домашні та корпоративні мережі, що може дати їм легкий доступ до даних користувача. Крім того, область застосування Інтернету речей розширюється й на людей, існують випадки вживання пристроїв Інтернету речей для моніторингу стану різних органів людини. Такі атаки поки що не стали реальністю, але можуть бути надзвичайно небезпечними, якщо пристрої Інтернету речей будуть скомпрометовані.

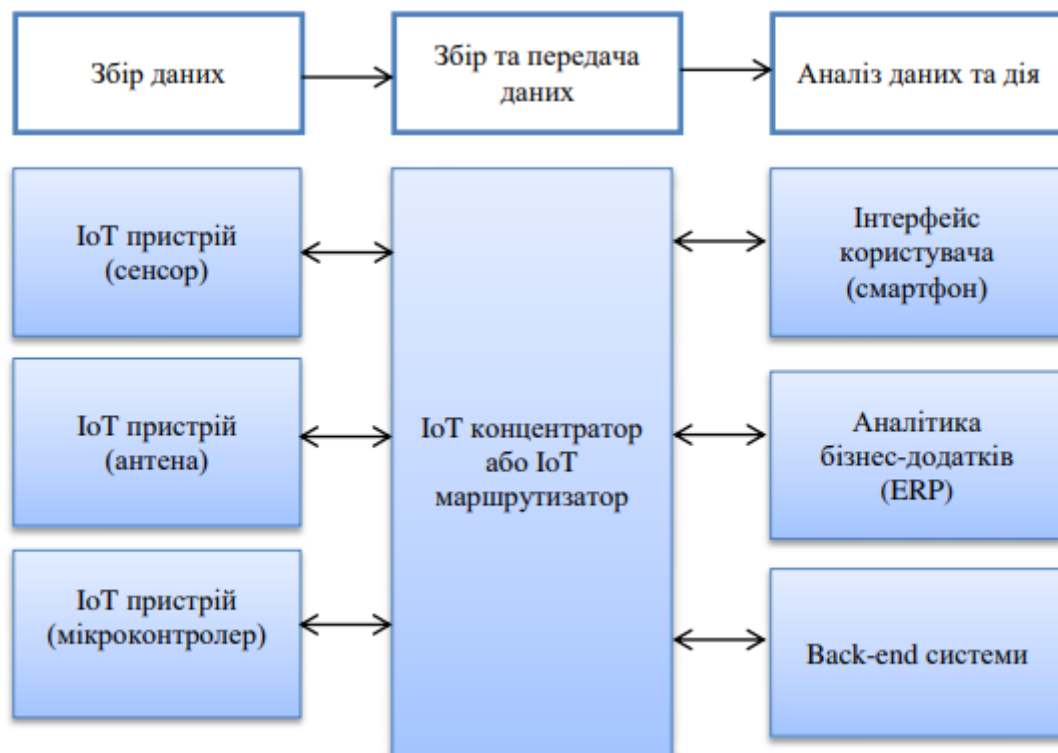


Рисунок 1.3 – приклад IoT-системи

Кіберфізичні системи (CPS) є ще одним напрямком, який виграє від зростання Інтернету речей. У CPS фізичні об'єкти в середовищі моніторяться, а дії вживаються на основі фізичних змін. Оскільки CPS охоплює активи важливого значення (наприклад, електричні мережі, транспортні системи), вразливості безпеки таких систем мають серйозні наслідки. Однак виклики щодо безпеки CPS мають свої унікальні характеристики і виходять за рамки цієї роботи.

У будь-якій екосистемі або середовищі Інтернету речей існують чотири важливі рівні. Перший рівень включає використання різноманітних датчиків та приводів для сприйняття даних або інформації для виконання різних функціональних завдань. На основі цього на другому рівні використовується комунікаційна мережа для передачі зібраних даних. Більшість додатків Інтернету речей, які розвиваються використовують третій рівень, відомий як проміжний рівень, який виступає мостом між мережею та рівнем додатків. Нарешті, на четвертому рівні існують різноманітні додатки на основі Інтернету речей, такі як розумні мережі, розумний транспорт, розумні фабрики і т.д. Усі ці чотири рівні мають свої власні проблеми безпеки. Крім цих рівнів, різноманітні шлюзи з'єднують ці рівні і допомагають у переміщенні даних, тож існують і певні загрози безпеці, специфічні для саме цих шлюзів.

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				12
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 1.4 – архітектура IoT

1.2 Критичні сфери застосування IoT

Безпека має вельми важливе значення для майже всіх застосувань Інтернету речей, які вже були розгорнуті або знаходяться в процесі розгортання. Застосування Інтернету речей швидко зростають і проникають у більшість існуючих галузей. Хоча оператори підтримують ці застосування Інтернету речей за допомогою наявних мережових технологій, деякі з них потребують більш жорсткої підтримки безпеки від використовуваних технологій. У цьому розділі розглядаються різні застосування Інтернету речей, які мають високий рівень критичності з погляду безпеки.

Розумні міста передбачають широке використання новітніх обчислювальних і комунікаційних ресурсів для підвищення загальної якості життя людей. Це охоплює розумні будинки, управління рухом транспорту, управління надзвичайними ситуаціями, комунальні послуги та інші аспекти. Існує активна тенденція до розвитку розумних міст, і уряди по всьому світу сприяють їхньому становленню,

надаючи різноманітні стимули. Незважаючи на те, що використання розумних додатків спрямоване на поліпшення якості життя громадян, воно несе загрозу приватності. Сервіси з використанням розумних карт можуть покласти під загрозу дані карток і покупкові звички громадян. Додатки для розумної мобільності можуть розкривати місцезнаходження користувачів. Існують додатки, які дозволяють батькам стежити за своїми дітьми. Проте, якщо такі додатки піддаються вторгненню, це може покласти під загрозу безпеку дитини.

Розумне довкілля включає різноманітні застосування Інтернету речей, такі як виявлення пожеж у лісах, контроль рівня снігу в гірських регіонах, запобігання зсувам ґрунту, раннє виявлення землетрусів, моніторинг забруднення навколишнього середовища тощо. Усі ці застосування Інтернету речей тісно пов'язані з життям людей та тварин у цих областях. Урядові агентства, що займаються такими сферами, також будуть залежати від інформації, наданої цими застосуваннями Інтернету речей. Порушення безпеки та вразливості у будь-якій зоні, пов'язаній з такими застосуваннями Інтернету речей, можуть мати серйозні наслідки. В цьому контексті як помилкові негативи, так і помилкові позитиви можуть призвести до катастрофічних результатів для таких застосувань Інтернету речей. Наприклад, якщо застосування неправильно починає виявляти землетруси, то це призведе до фінансових втрат для уряду та бізнесу. З іншого боку, якщо застосування не здатне передбачити землетрус, то це може призвести до втрат майна та життя. Тому застосування розумного довкілля повинні бути високо точними, а порушення безпеки та підробка даних повинні бути уникнуті.

Системи розумного вимірювання та розумні мережі електропостачання: Розумне вимірювання включає застосунки, пов'язані з різними вимірюваннями, моніторингом та управлінням. Найпоширенішим застосуванням розумного вимірювання є розумні мережі електропостачання, де вимірюється та контролюється споживання електроенергії. Розумне вимірювання також може використовуватися для вирішення проблеми крадіжки електроенергії. Іншими застосуваннями розумного вимірювання є моніторинг рівнів води, нафти та газу у резервуарах

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		14

і цистернах. Розумні лічильники також використовуються для моніторингу та оптимізації роботи сонячних електростанцій шляхом динамічної зміни кута сонячних панелей для отримання максимальної сонячної енергії. Також існують додатки Інтернету речей, які використовують розумні лічильники для вимірювання тиску в системах водопостачання або для вимірювання ваги вантажів. Однак, системи розумного вимірювання вразливі як до фізичних, так і до кібератак, в порівнянні з аналоговими лічильниками, які можуть бути підроблені лише фізичними атаками. Крім того, розумні лічильники або розширена лічильна інфраструктура (AMI) призначені для виконання функцій, що виходять за межі звичайного запису споживання енергії. У мережі розумного дому (HAN) всі електричні пристрої вдома підключені до розумних лічильників, і інформація, зібрана з цих пристроїв, може використовуватися для керування навантаженням та управління витратами. Намірене вторгнення в такі комунікаційні системи з боку споживача або ворожої сторони може змінити зібрану інформацію, що призведе до фінансових втрат для постачальників послуг або споживачів.

Безпека та надзвичайні ситуації: Безпека та надзвичайні ситуації є ще одним важливим напрямком, в якому впроваджуються різноманітні застосування Інтернету речей. Вони включають такі застосування, як обмеження доступу лише авторизованих осіб до обмежених зон, відеоспостереження, датчики руху і т. д. Іншим застосуванням в цій галузі є виявлення витоків небезпечних газів на промислових територіях або в околицях хімічних заводів. Рівні радіації також можуть бути виміряні в зонах навколо ядерних реакторів або базових станцій мобільного зв'язку, і можуть бути створені сповіщення, коли рівень радіації є високим. Існують різні будівлі, в яких зберігаються чутливі дані або цінні товари. Застосунки безпеки можуть бути використані для захисту чутливих даних та товарів. Застосування Інтернету речей, що виявляють різні рідини, також можуть бути використані для запобігання корозії та поломкам у таких чутливих будівлях. Порушення безпеки в таких застосунках можуть мати серйозні наслідки. Наприклад, злочинці можуть намага-

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		15

тися потрапити у заборонені зони, використовуючи вразливості в таких застосунках. Крім того, хибні сигнали про рівень радіації можуть мати серйозні негайні та віддалені наслідки.

Розумний роздріб: Застосування Інтернету речей широко використовуються в роздрібній торгівлі. Розроблено різні застосування для моніторингу умов зберігання товарів під час їх переміщення по ланцюгу постачання. Інтернет речей також використовується для контролю відстеження товарів на складах, щоб здійснювати оптимальне поповнення запасів. Також розробляються різні розумні додатки для покупців, які надають підтримку на основі їх вподобань, звичок, алергій на певні компоненти і т. д. Були розроблені механізми, які за допомогою технік доповненої реальності надають можливість офлайн-роздрібним торговцям отримати досвід онлайн-шопінгу. Різні компанії в роздрібній торгівлі стикаються з проблемами безпеки при впровадженні та використанні різноманітних застосувань Інтернету речей. До цих компаній належать Apple, Home Depot, JP Morgan Chase та Sony. Зловмисники можуть намагатися скомпрометувати застосування Інтернету речей, пов'язані з умовами зберігання товарів, і намагатися передавати користувачам невірну інформацію про продукти з метою збільшення продажів. Якщо в розумному роздрібі не реалізовані заходи безпеки, зловмисники можуть красти інформацію про дебетові та кредитні картки, номери телефонів, адреси електронної пошти тощо клієнтів, що може призвести до фінансових втрат для клієнтів та роздрібних торговців.

Автоматизація домашнього простору: Автоматизація домашнього простору є одним з найбільш широко використовуваних та розгорнутих застосувань Інтернету речей. Це включає застосування для віддаленого управління електричними приладами для енергозбереження, системи, встановлені на вікнах та дверях для виявлення зловмисників та інше. Моніторингові системи використовуються для відстеження споживання енергії та водопостачання, а користувачі отримують поради щодо економії коштів та ресурсів. Однак зловмисники можуть отримати несанкціонований доступ до пристроїв Інтернету речей в домі та намагатися завдати шкоди користувачам. Наприклад, кількість випадків крадіжок у домашніх приміщеннях

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		16

швидко зросла після впровадження різних систем автоматизації домашнього простору. Також було випадки, коли зловмисники намагалися аналізувати тип та обсяг інтернет-трафіку до/зі смарт-домів для оцінки поведінки та присутності мешканців.

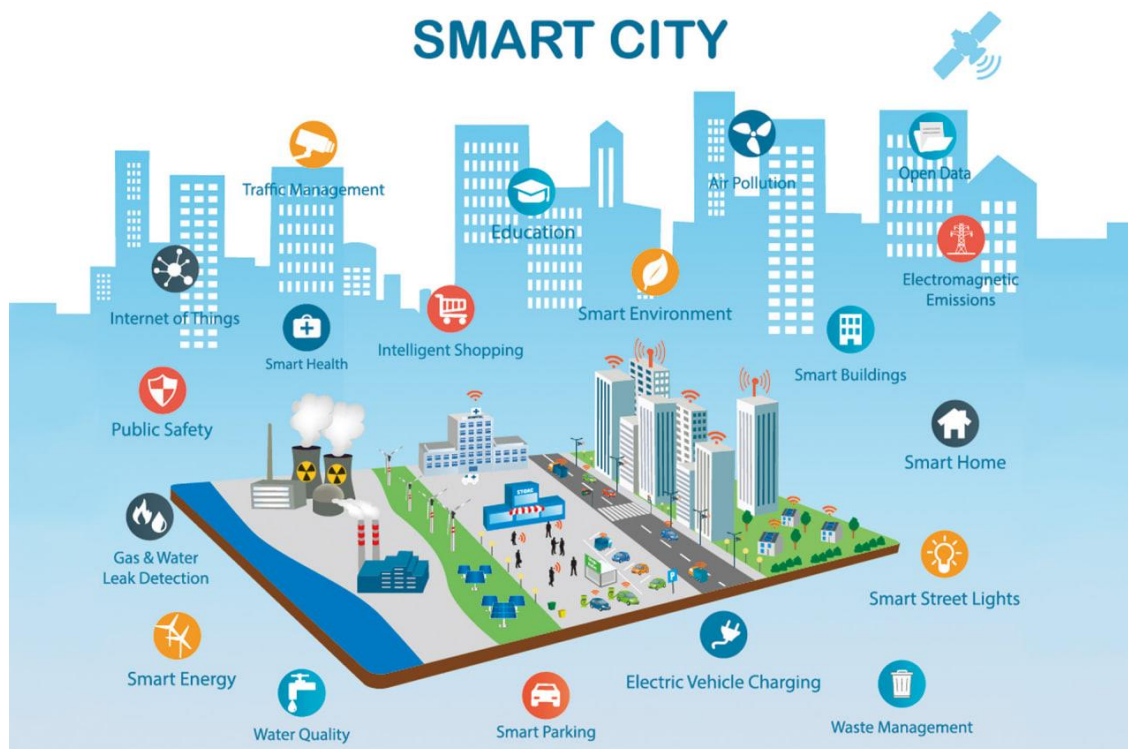


Рисунок 1.5 – Розумне місто та інтеграція IoT систем в різні сфери міського життя

Розумне сільське господарство та тваринництво: Розумне сільське господарство включає моніторинг вологості ґрунту, контроль мікроклімату, селективне поливання в сухих зонах, а також контроль вологості і температури. Використання таких передових функцій у сільському господарстві може допомогти досягти високих врожаїв та захистити фермерів від втрат коштів. Контроль рівнів температури та вологості у виробництві зерна та овочів може допомогти у запобіганні грибків та інших мікробних забруднень. Контроль кліматичних умов також може допомогти збільшити врожай та якість овочів і сільськогосподарських культур. Так само, як моніторинг врожаю, існують застосування Інтернету речей для моніторингу активності та стану здоров'я фермерських тварин шляхом встановлення датчиків на тварин. Якщо такі застосування піддаються компрометації, це може призвести до крадіжки тварин з ферми, а також до завдання шкоди врожаю.

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		17

1.3 Джерела загроз безпеці в IoT

Будь-яку IoT систему можна розділити на чотири рівні: рівень зчитування даних, мережний рівень, рівень проміжного програмного забезпечення, та рівень додатків. Кожен з цих рівнів використовує різноманітні технології, які викликають ряд проблем та загроз безпеці. У цьому розділі обговорюються різноманітні можливі загрози безпеці в системах IoT для цих чотирьох рівнів. Також в цьому розділі обговорюються особливі проблеми безпеки, пов'язані з шлюзами, які з'єднують ці рівні.

Проблеми безпеки на рівні зчитування даних: рівень зчитування даних в основному займається фізичними датчиками та виконавчими пристроями Інтернету речей (IoT). Датчики реєструють фізичні явища, що відбуваються навколо них. З використанням зібраних даних, виконавчі пристрої здійснюють певні дії в фізичному середовищі. Існує різноманітність датчиків для реєстрації різних видів даних, наприклад, ультразвукові датчики, камерні датчики, датчики виявлення диму, датчики температури та вологості тощо. Використовуються механічні, електричні, електронні або хімічні датчики для вимірювання фізичного середовища. В різних застосуваннях IoT використовуються різні технології рівня зчитування даних, такі як RFID, GPS, WSN, RSN тощо. Основні загрози безпеці, з якими можна стикнутися на рівні зчитування даних, наступні:

Захоплення вузла: системи Інтернету речей складаються з кількох вузлів з низьким рівнем споживання енергії, таких як датчики та виконавчі пристрої. Ці вузли вразливі до різних атак з боку злоумисників. Атакувачі можуть намагатися захопити або замінити вузол в системі IoT на злоумисний вузол. Новий вузол може видаватися частиною системи, але керується атакувачем. Це може призвести до компрометації безпеки всієї програми IoT.

Атака на впровадження злоумисного коду: Ця атака полягає в тому, що атакувач впроваджує злоумисний код у пам'ять вузла. Зазвичай прошивка або програмне забезпечення вузлів IoT оновлюється безпроводово, що дає можливість атакувачам впроваджувати злоумисний код. З використанням такого злоумисного коду

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		18

атакувачі можуть змусити вузли виконувати небажані функції або навіть намагатися отримати доступ до всієї системи IoT.

Атака внесення хибних даних: Після захоплення вузла атакувач може використовувати його для внесення помилкових даних в систему IoT. Це може призвести до отримання неправильних результатів та розхитування роботи програми IoT. Атакувач також може використовувати цей метод для проведення атаки DDoS.

Атаки з боку каналів бічного доступу: Окрім прямих атак на вузли, різні атаки з боку каналів бічного доступу можуть призвести до розкриття конфіденційної інформації. Мікроархітектура процесорів, електромагнітне випромінювання та їх споживання енергії розкривають чутливу інформацію перед атакувачами. Атаки з боку каналів бічного доступу можуть базуватися на споживанні енергії, атаках на основі лазерів, атаках з використанням часу або електромагнітних атак. Сучасні мікросхеми вживають різноманітні заходи захисту для запобігання таким атакам з боку каналів бічного доступу під час реалізації криптографічних модулів.

Прослуховування та перешкоджання: Програми IoT часто включають в себе різні вузли, розташовані у відкритих середовищах. У результаті цього такі програми IoT піддаються прослуховуванню. Атакувачі можуть прослуховувати та перехоплювати дані під час різних фаз, наприклад, передачі даних або аутентифікації.

Атаки з обмеженням сну: У таких типах атак атакувачі намагаються виснажити батарею пристроїв Інтернету речей з низьким рівнем споживання енергії. Це призводить до відмови в обслуговуванні вузлів у програмі IoT через розряд батареї. Це може бути досягнуто за допомогою виконання нескінченних циклів у пристроях краю за допомогою зловмисного коду або штучного збільшення споживання енергії пристроїв краю.

Атаки при завантаженні: Пристрої краю вразливі до різних атак під час процесу завантаження. Це стосується того, що вбудовані процеси безпеки не активуються в цей момент. Атакувачі можуть скористатися цією вразливістю та намагатися атакувати пристрої вузлів під час їх перезапуску. Оскільки пристрої краю, як правило, мають низьку потужність та періодично проходять через цикли сну та

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		19

пробудження, важливо забезпечити безпеку процесу завантаження в цих пристроях.

Проблеми на рівні мережі: основна функція рівня мережі полягає в передачі інформації зі слоя сприйняття до обчислювального пристрою для обробки. Основні проблеми безпеки, з якими стикаються на рівні мережі, такі:

Атака фішинг-сайтами: Існує можливість зустріти фішинг-сайти під час відвідування користувачами веб-сторінок в Інтернеті. Якщо обліковий запис і пароль користувача стають компрометованими, то всі присторої Інтернету речей, якими користується користувач, стають вразливими до кібератак. Рівень мережі в Інтернеті речей є дуже вразливим дотаких атак.

Атака на доступ: Атака на доступ також називається постійно присутньою загрозою (APT). Це тип атаки, в якому несанкціонована особа або противник отримує доступ до мережі Інтернету речей. Атакувач може залишатися в мережі непоміченим протягом тривалого часу. Метою цього типу атаки є крадіжка цінних даних або інформації, а не завдання шкоди мережі. Програми Інтернету речей постійно отримують та передають цінні дані і, отже, є дуже вразливими до таких атак

Атака DDoS/DoS: У цьому типі атак атакувач завалює цільові сервери великою кількістю небажаних запитів. Це призводить до паралізації цільового сервера і, отже, до відключення послуг для справжніх користувачів. Якщо атакувач використовує кілька джерел для завалювання цільового сервера, то така атака називається DDoS або розподілена атака відмовою в обслуговуванні. Такі атаки не є специфічними для програм Інтернету речей, але через гетерогенність та складність мереж Інтернету речей рівень мережі Інтернету речей вразливий до таких атак. Багато пристроїв Інтернету речей у програмах Інтернету речей не мають належної конфігурації, тому стають легкодоступними шлюзами для атакувачів для запуску атак DDoS на цільові сервери. Наприклад, атака ботнетом Mirai, яка була обговорена в Розділі I, використовувала цю вразливість та блокувала різні сервери, постійно поширюючи запити до слабо налаштованих пристроїв Інтернету речей.

Атаки на транзит даних: Програми Інтернету речей мають справу з багатою обробкою та обміном даними. Дані є цінними, тому завжди є об'єктом уваги хакерів

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		20

та інших противників. Дані, що зберігаються на локальних серверах або в хмарі, мають ризик безпеки, але дані, що перебувають у русі або пересуваються з одного місця в інше, є ще більш вразливими до кібератак. У програмах Інтернету речей відбувається багато руху даних між датчиками, виконавчими пристроями, хмарою тощо. У таких рухах даних використовуються різні технології з'єднання, тому програми Інтернету речей вразливі до витоку даних.

Атаки на маршрутизацію: У таких атаках зловмисні вузли в програмі Інтернету речей можуть спробувати перенаправити маршрутизаційні шляхи під час транзиту даних. Атаки залякування - це конкретний вид атак на маршрутизацію, при якому противник рекламує штучний найкоротший маршрут маршрутизації і повертає вузли для маршрутизації трафіку через нього. Атака через "черв'як-дірку" є ще одною атакою, яка може стати серйозною загрозою безпеці, якщо поєднана з іншими атаками "Черв'як-дірка" - це позаканальний зв'язок між двома вузлами для швидкого передавання пакетів. Атакувач може створити його між скомпрометованим вузлом і пристроєм в Інтернеті і спробувати обійти основні протоколи безпеки в системі Інтернету речей.

Безпекові проблеми на рівні шлюзів: шлюз є широким рівнем, який відіграє важливу роль у з'єднанні багатьох пристроїв, людей, речей та хмарових сервісів. Шлюзи також допомагають у наданні апаратних та програмних рішень для пристроїв Інтернету речей. Вони використовуються для розшифрування та шифрування даних Інтернету речей і перекладу протоколів для комунікації між різними рівнями. Сучасні системи Інтернету речей є гетерогенними і включають стеки LoraWan, ZigBee, Z-Wave та TCP/IP з багатьма шлюзами між ними. Нижче розглядаються деякі проблеми безпеки, пов'язані із шлюзами Інтернету речей.

Безпечна реєстрація: При встановленні нового пристрою або датчика в системі Інтернету речей має велике значення захист шифрувальних ключів. Шлюзи діють як посередники між новими пристроями та керуючими сервісами, і всі ключі проходять через шлюзи. Шлюзи піддаються атакам "чоловік-у-середині" та перехопленню для захоплення шифрувальних ключів, особливо під час процесу реєстрації.

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		21

Додаткові інтерфейси: Мінімізація площини атаки є важливою стратегією, яку слід враховувати при встановленні пристроїв Інтернету речей. Виробник шлюзів Інтернету речей має реалізовувати лише необхідні інтерфейси та протоколи. Деякі сервіси та функціональності слід обмежити для кінцевих користувачів, щоб уникнути використання та порушення конфіденційності інформації через задні двері.

Шифрування від кінця до кінця: Для забезпечення конфіденційності даних потрібне справжнє шифрування на рівні додатків. Додаток не повинен дозволяти розшифровувати зашифровані повідомлення нікому, крім унікального отримувача. Хоча протоколи Zigbee та Zwave підтримують шифрування, це не є шифруванням від кінця до кінця, оскільки для перекладу інформації з одного протоколу в інший потрібно розшифрувати та повторно зашифрувати повідомлення на рівні шлюзу. Це розшифрування на рівні шлюзу робить дані вразливими до порушень безпеки.

Оновлення прошивки: Більшість пристроїв Інтернету речей мають обмежені ресурси і, отже, не мають користувацького інтерфейсу або обчислювальної потужності для завантаження та встановлення оновлень прошивки. Зазвичай шлюзи використовуються для завантаження та застосування оновлень прошивки. Поточна та нова версії прошивки повинні бути записані, а валідність підписів повинна перевірятися для безпечних оновлень прошивки.

Безпекові проблеми на рівні додатків: рівень додатків безпосередньо працює з кінцевими користувачами і надає послуги. Додатки Інтернету речей, такі як розумний будинок, розумні лічильники, розумні міста, розумні мережі тощо, належать до цього рівня. На цьому рівні виникають специфічні проблеми безпеки, які відсутні на інших рівнях, такі як крадіжка даних та проблеми приватності. Проблеми безпеки на цьому рівні також специфічні для різних додатків. Багато додатків Інтернету речей також включають підрівень між мережевим рівнем та рівнем додатків, який зазвичай називається підтримуючим рівнем додатків або рівнем проміжного програмного забезпечення. Перераховані нижче основні проблеми безпеки, з якими зіштовхується рівень додатків.

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		22

Крадіжка даних: Додатки Інтернету речей мають справу з великою кількістю критичних та приватних даних. Дані, які перебувають у русі, вразливіші до атак, ніж дані, що спочивають, і в додатках Інтернету речей відбувається багато переміщення даних. Користувачі будуть схильні відмовитись від реєстрації своїх приватних даних у додатках Інтернету речей, якщо ці додатки вразливі до крадіжки даних. Для захисту додатків Інтернету речей від крадіжок даних використовуються такі техніки та протоколи, як шифрування даних, ізоляція даних, аутентифікація користувача і мережі, управління конфіденційністю тощо.

Атаки на контроль доступу: Контроль доступу є механізмом авторизації, який дозволяє доступ лише законним користувачам або процесам до даних або облікових записів. Атака на контроль доступу є критичною для додатків Інтернету речей, оскільки якщо доступ компрометований, то весь Інтернет речей стає вразливим. Для захисту додатків Інтернету речей від атак на контроль доступу використовуються різні техніки, такі як мультифакторна аутентифікація, різні рівні доступу, логування та аудит доступу, обмеження прав доступу тощо.

Несанкціоновані зміни: Додатки Інтернету речей можуть бути піддаються несанкціонованим змінам або модифікаціям. Атакувач може модифікувати програмне забезпечення додатка Інтернету речей, що може привести до зміни поведінки додатка або крадіжки даних. Для запобігання несанкціонованим змінам використовуються такі методи, як цифровий підпис програмного забезпечення, захист від модифікацій, механізми виявлення змін тощо.

Незахищені комунікації: Додатки Інтернету речей часто спілкуються з серверами та іншими пристроями через мережу. Незахищена комунікація може призвести до перехоплення або зміни даних, що передаються між додатками та серверами. Для забезпечення захищених комунікацій використовуються протоколи шифрування, тунелювання, контроль цілісності тощо.

Системи Інтернету речей (IoT) відкривають безліч перспективних можливостей у різних сферах життя. Інноваційні технології та зростаюча взаємодія між фізичними та цифровими пристроями приводять до з'явлення нових інтелектуаль-

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		23

них систем. Одним з перспективних напрямків є розумне будівництво, де застосування IoT дозволяє оптимізувати енергоефективність, безпеку та зручність в управлінні будівлями. Також, сфера здоров'я та медицини отримує значний потенціал завдяки IoT, де моніторинг здоров'я, електронні медичні картки та підключені медичні пристрої можуть покращити діагностику, лікування та пацієнтський догляд. В сільському господарстві та промисловості IoT може забезпечити ефективне управління ресурсами, моніторинг умов вирощування рослин та виробничих процесів. Більш того, в містах концепція "розумне місто" широко використовує IoT для оптимізації управління транспортом, енергетикою, відходами та інфраструктурою, що сприяє покращенню якості життя мешканців. Усі ці перспективи демонструють, що системи Інтернету речей мають значний потенціал для створення ефективних та зручних рішень у багатьох галузях і можуть перетворити спосіб, яким ми взаємодіємо з навколишнім середовищем.

Але це також приводить до проблеми безпеки на різних рівнях і всі вимагають комплексного підходу та використання різних технологій і методів для їх вирішення. Організації, розробники, системні адміністратори та спеціалісти з кібербезпеки повинні докладати зусиль для забезпечення безпеки на кожному рівні систем Інтернету речей, починаючи з апаратного забезпечення та мережі Інтернету речей і закінчуючи додатками та послугами, що надаються користувачам.

1.4 Висновки до розділу 1

В першому розділі розглядалась актуальна проблема захисту в контексті швидкого розвитку Інтернету речей (IoT) та його впливу на наше життя. IoT-системи суттєво змінили і продовжують змінювати технологічний пейзаж, а також мають вплив на інші сфери нашого життя.

За допомогою IoT-систем ми отримуємо нові можливості в галузях як технологій, так і повсякденного життя. Вони розширюють можливості моніторингу, автоматизації та збільшують нашу зв'язаність з навколишнім середовищем. Однак, разом з цим розвитком, з'являється все більше кібер загроз, які можуть серйозно підірвати безпеку IoT-систем.

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		24

Кібер загрози стають все небезпечнішими і складнішими, оскільки зловмисники постійно вдосконалюють свої методи атак та використовують розширені можливості IoT-систем для здійснення своїх намірів. Велика кількість пристроїв, підключених до IoT-мережі, створює нові вразливості, що можуть бути використані для зламу та несанкціонованого доступу. Тому надзвичайно важливо бути захищеним від цих загроз.

Розуміння ризиків та використання відповідних методів та технологій захисту є важливими факторами для забезпечення безпеки IoT-систем. Правильна архітектура та реалізація підсистеми захисту, такої як VPN-тунель, внесе суттєвий внесок у створення надійної мережної інфраструктури IoT-системи.

Загалом, розвиток IoT-системи відкриває безліч нових можливостей, проте разом з цими можливостями приходять і загрози. Важливо розуміти ці ризики та вживати заходів для їхнього управління та забезпечення безпеки. З розвитком Інтернету речей (IoT), наш світ стає все більш зв'язаним та інтегрованим. IoT-системи проникають у різні сфери нашого життя, включаючи домашнє господарство, медицину, промисловість, транспорт та багато іншого. Вони пропонують нам безліч переваг, забезпечуючи зручність, ефективність та автоматизацію процесів.

Проте, з поширенням IoT-систем виникає ряд проблем, пов'язаних з безпекою. Зловмисники можуть використовувати різні методи та техніки для атак на ці системи. Від перехоплення даних до зламу пристроїв та маніпуляцій з ними, кібер загрози стають все більш складними та суттєвими.

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				25
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 2 ВИБІР ТИПУ ІОТ-СИСТЕМИ ТА ПРОЕКТУВАННЯ ЇЇ ПІДСИСТЕМИ ЗАХИСТУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ

2.1 Вибір обладнання

Для реалізації підсистеми захисту мережної інфраструктури ІоТ-системи було вирішено використовувати мережеве обладнання компанії Cisco Systems, inc.

При виборі моделі маршрутизатора важливо врахувати його можливості в маршрутизації пакетів складних глобальних мереж та ІоТ-систем. Маршрутизатор повинен відповідати певним вимогам: бути сучасним, забезпечити максимально надійну роботу та працювати на необхідній швидкості для передачі та обробки даних, тому в мережі використовуватиметься маршрутизатор Cisco 7204VXR.

Маршрутизатори серії 7200 забезпечують високу надійність, стійкість до відмов, підтримку широкого спектру середовищ передачі даних. За рахунок модульності їх конструкції замовник може підібрати конфігурацію, що відповідає його запитам, що дозволяє досягти оптимального поєднання функціональності та вартості мережі. Для забезпечення відмовостійкості системи Cisco 7200 передбачена можливість підключення двох джерел живлення, а також можливість заміни інтерфейсних модулів без припинення функціонування пристрою. Все це особливо актуально для ІоТ-систем.

Багатофункціональні платформи Cisco 7200 є ефективною з точки зору вартості системою, що поєднує в собі можливості підтримки наступних технологій:

- Інтерфейси глобальних та локальних мереж високої щільності
- Пакетна маршрутизація поверх мереж SONET/SDH
- Пряме підключення до глобальних мереж АТМ
- Структуровані сполуки Е3 або Е1 високої густини
- Пряме з'єднання з ІВМ мейнфреймами
- Підключення цифрових АТС (РВХ) на основі Е1, підключення джерел відеосигналів

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		26

Cisco 7200 забезпечує широкі функціональні можливості за високої продуктивності. Користувач може скористатися перевагами високопродуктивної комутації мережного рівня та додатковими сервісами, включаючи безпеку, якість сервісу (Quality of Service) та додаткові можливості керування трафіком.

Основні можливості

- Підтримка всіх функцій Cisco IOSTM
- Підтримка наступних інтерфейсів ЛОМ: Ethernet, Fast Ethernet, 100VG-AnyLAN, Token Ring, FDDI
- Інтерфейси глобальних мереж підтримуються ISDN PRI/BRI, HSSI, T3/E3, ATM
- Підтримуються цифрові голосові інтерфейси E1
- Можливість передачі голосу (телефонії) і факсів через мережі TCP/IP, забезпечуючи з'єднання телефонів, передачу факсів у часі й у режимі їх маршрутизації через загальну мережу IP. Цифрові голосові модулі підтримують стандарти ITU G.729, G.726, G.711 та G.723.1 для забезпечення якості голосу та факсів, і дозволяють обробляти до 120 голосових з'єднань.
- Підтримка функції Tandem Switching для передачі голосу через протоколи IP та Frame Relay
- Подвійне (резервоване) внутрішнє джерело живлення (Redundant Power Supply - RPS) забезпечує рівномірне навантаження по живленню і подвоює час на працювання на відмову (Mean Time Between Failure - MTBF)
- Повне віддалене та локальне керування за допомогою інтерфейсу командного рядка, протоколу SNMP або графічного інтерфейсу користувача CiscoView
- Модульний дизайн забезпечує легкість упровадження майбутніх технологій.

Варіанти програмного забезпечення

- Повний набір мережевих протоколів (Enterprise Feature Set)
- Шифрування на мережному рівні за допомогою стандартної технології IPSec (Plus Encryption Feature Set)
- Міжмережевий екран (IOS Firewall Feature Set)

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		27

Cisco серії 7200VXR – ефективна за вартістю платформа, яка надає:

- високу щільність інтерфейсів LAN та WAN
- агрегацію користувацьких сервісів (у тому числі PPP, RFC1483 termination та тунелі L2TP)
- термінацію цифрового TDM транку T1/E1 для голосу, відео та даних
- високу щільність портів Multichannel T3/E3 та T1/E1
- підтримку технологій ATM, SDH, Packet over SONET (POS) та DPT
- Direct ATM Circuit Emulation Standard для голосу, відео та даних

Cisco 7200VXR має резервування живлення та можливість гарячої заміни порт-адаптерів, зовнішній Flash-диск підвищує надійність, зберігаючи резервні копії програмного забезпечення та файлів конфігурації.

Пристрої моніторингу стану системи мають рівні ескалації — оператор може вчасно запобігти серйозним неполадкам. Для зручності обслуговування та розширюваності всі компоненти Cisco 7200VXR замінюються.

Всі ці фактори роблять з Cisco 7200VXR одним із найкращих варіантів для IoT-систем.

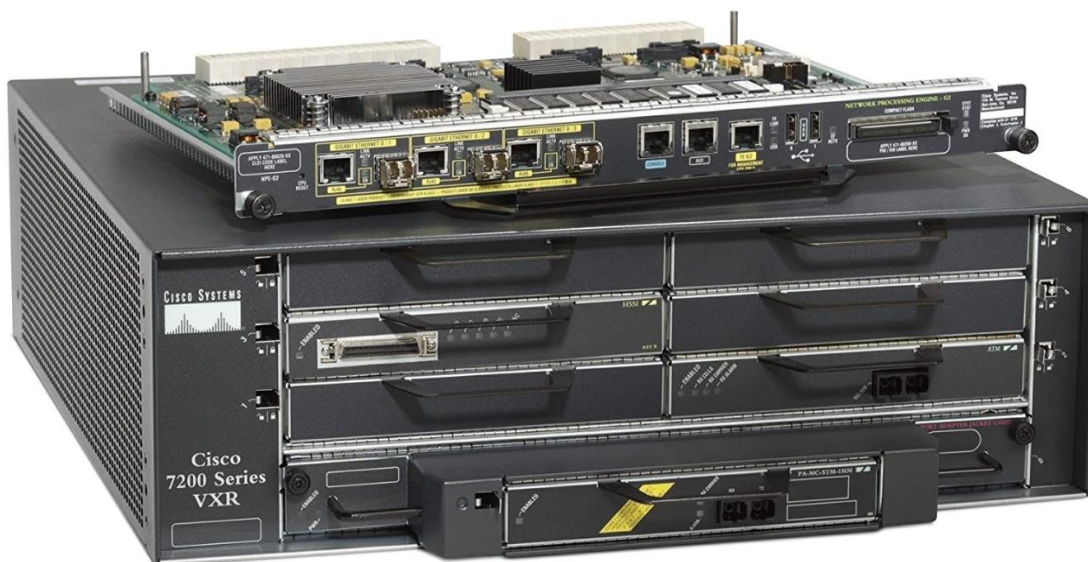


Рисунок 2.1 – Маршрутизатор Cisco 7204VXR

При виборі моделі мережного фаєрволу для проєкту підсистеми захисту мережної інфраструктури IoT-системи важливо враховувати безпеку та сумісність з IoT-системою. Безпека є найкритичнішим фактором та саме тому має бути забез-

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		28

печена надійність захисту мережі від вторгнень та небажаного доступу. Також важливо, щоб обрана модель мережного фаєрволу була сумісна з IoT-системою, щоб забезпечити оптимальну інтеграцію та функціональність.

Cisco ASA 5505 є прекрасним вибором для проекту підсистеми захисту мережної інфраструктури IoT-системи з кількох причин. Ось кілька ключових характеристик, які роблять його підходящим для цього проекту:

Мережевий захист: Cisco ASA 5505 надає потужні механізми захисту мережі, включаючи функціонал мережевого екрану (firewall), виявлення та запобігання вторгнень (IDS/IPS), фільтрацію трафіку і VPN (віртуальну приватну мережу). Ці функції допоможуть утримати зловмисників подалі від мережної інфраструктури IoT-системи та захистити її від небажаного доступу.

Масштабованість: ASA 5505 може бути легко масштабований для використання в маленьких і середніх організаціях, які вимагають захисту своєї мережі IoT-системи. Він має достатньо потужності для обробки великого обсягу трафіку та одночасного керування багатьма підключеними пристроями.

Простота у використанні: ASA 5505 має дружній інтерфейс користувача, що спрощує його налаштування та керування. Це важливо для проекту з підсистемою захисту мережної інфраструктури IoT-системи, оскільки можливість швидкого налаштування і управління є ключовою вимогою для ефективного захисту.

Висока надійність: ASA 5505 є надійним мережевим пристроєм з високою доступністю, що забезпечує мінімальний вплив на роботу мережі IoT-системи. Він має функції резервування та відновлення, які допомагають уникнути відмов в роботі та забезпечити неперервну роботу системи.

Інтеграція з екосистемою Cisco: ASA 5505 підтримує інтеграцію з іншими продуктами Cisco, такими як системи керування мережею (Cisco Network Management) та інші мережеві пристрої Cisco. Це дозволяє забезпечити єдиний інфраструктурний стек для мережної інфраструктури IoT-системи, спрощуючи управління та розвиток.

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		29

Узагалі, Cisco ASA 5505 має всі необхідні характеристики, щоб забезпечити захист мережної інфраструктури IoT-системи. Він надійний, масштабований, простий у використанні та інтегрується з екосистемою Cisco. Вибір ASA 5505 для проєкту підсистеми захисту мережної інфраструктури IoT-системи допоможе забезпечити ефективний та надійний захист мережі.

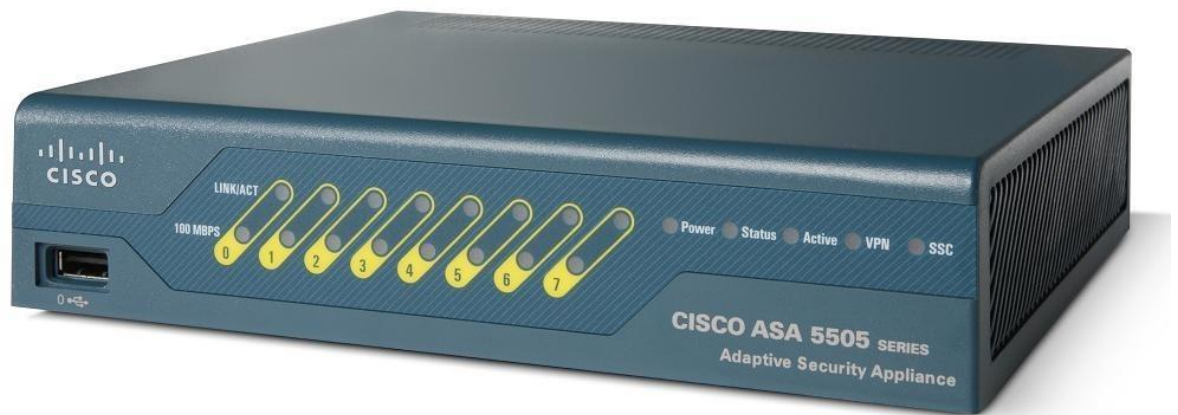


Рисунок 2.2 – Мережевий фаєрвол Cisco ASA 5505

Що до точки доступу Cisco Catalyst 9100L є прекрасним вибором для проєкту підсистеми захисту мережної інфраструктури IoT-системи з багатьох причин.

Cisco Catalyst 9100L має вбудовані функції безпеки, такі як шифрування WPA3 і додаткові функції безпеки Cisco. Це дозволяє забезпечити захищене підключення для розумних пристроїв в мережі IoT. Вона допомагає захищати важливі дані та запобігає несанкціонованому доступу до мережі.

Ця модель підтримує технологію Cisco TrustSec, яка забезпечує аутентифікацію та авторизацію на рівні мережевого доступу. Це дозволяє забезпечити контроль доступу до мережі IoT та захистити її від потенційних загроз.

Cisco Catalyst 9100L підтримує інтеграцію з різноманітними сторонніми рішеннями безпеки, такими як системи моніторингу та розпізнавання загроз. Це дозволяє створити комплексну систему захисту мережної інфраструктури IoT-системи та виявляти потенційні загрози.

Ця точка доступу також є частиною екосистеми Cisco DNA Center, що забезпечує централізоване управління і моніторинг мережі. Це дозволяє зручно

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		30

налаштовувати, керувати та відстежувати роботу точок доступу в мережі IoT, а також швидко реагувати на потенційні проблеми безпеки.

Вона володіє стабільністю та високою продуктивністю, що є важливим для підсистеми захисту мережної інфраструктури IoT-системи. Вона забезпечує надійне та швидке безпроводове підключення для всіх розумних пристроїв, які використовуються в системі.

Загалом, Cisco Catalyst 9100L має необхідні характеристики, функції безпеки та інтеграцію з системами управління, щоб бути прекрасним вибором для підсистеми захисту мережної інфраструктури IoT-системи. Вона допоможе забезпечити безпечну та надійну роботу всіх підключених пристроїв і захистити мережу від потенційних загроз.



Рисунок 2.3 – точка доступу Cisco Catalyst 9100L

2.2 Вибір модельного прикладу IoT-системи

В першому розділі було розкрито, що IoT системи можуть бути застосовані в різних галузях, включаючи такі, як розумне тваринництво, медицина, промисловість, енергетика та інші. Кожна модель IoT системи має свої особливості і переваги, що робить їх привабливими для кіберзлочинців і справжнім випробовуванням для спеціалістів з кібербезпеки.

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		31

Але для модельного прикладу IoT-системи було вибрано розумний будинок, тому що це системи, які з одного боку мають мати високий рівень безпеки, а з іншого мають бути не дуже дорогими та неважкими в обслуговуванні. Вони потребують простої, але безпечної підсистеми захисту мережної інфраструктури Інтернету речей.

У сучасному світі, де технології розвиваються з кожним днем, розумні будинки стають все більш популярними. Ці будинки обладнані різноманітними підсистемами, які забезпечують автоматизацію та комфорт в повсякденному житті. Однак, залучення Інтернету речей (IoT) в такі системи створює нові виклики, зокрема у сфері безпеки та захисту мережної інфраструктури.

Розумний будинок, який підключений до Інтернету, може бути під загрозою на мережовому рівні. Основними кіберзагрозами, з якими може зіштовхнутися розумний будинок, є наступні:

Атаки DDoS (розподілені атаки з відмовою в обслуговуванні): Кіберзлочинці можуть спрямовувати велику кількість трафіку на мережу розумного будинку, призводячи до перевантаження мережевих пристроїв і припинення їх нормальної роботи. Це може призвести до відмови в обслуговуванні всіх підключених до мережі пристроїв та заборони доступу до ресурсів.

Розумний будинок зазвичай використовує фаєрволи для контролю доступу та фільтрації трафіку. Кіберзлочинці можуть спробувати обійти фаєрвол або скомпрометувати його, отримати несанкціонований доступ до мережі і зловживати ним.

Перехоплення трафіку: Зловмисники можуть намагатися перехопити мережевий трафік, що йде до та від розумного будинку. Це може дозволити їм отримати доступ до чутливої інформації, яка передається через мережу, такої як паролі, особисті дані або відеозаписи з камер спостереження.

Вторгнення в мережу: Кіберзлочинці можуть намагатися проникнути в мережу розумного будинку, зламавши аутентифікаційні дані або використовуючи вразливості мережевих пристроїв. Це може дозволити їм отримати контроль над пристроями, включеними до мережі, і здійснювати небажані дії або отримувати нелегальний доступ до конфіденційної інформації.

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		32

Мережеві вразливості: Розумні пристрої та мережеві пристрої в межах розумного будинку можуть мати вразливості в програмному забезпеченні, які можуть бути використані зловмисниками для зламу або контролю пристроїв. Недостатнє оновлення програмного забезпечення або відсутність заходів безпеки можуть зробити мережу вразливою до таких атак.

Фішинг та соціальний інжиніринг: Зловмисники можуть намагатися отримати доступ до розумного будинку, використовуючи методи соціального інжинірингу або фішингу. Шляхом відправки фальшивих повідомлень або введенням користувачів в оману, зловмисники можуть отримати доступ до облікових записів та проникнути в мережу.

2.3 Загальний опис розробленої мережі та топології

Розроблена топологія мережі враховує не лише аспекти безпеки, але й витратоефективність, забезпечуючи оптимальне поєднання захисту та економічної ефективності в контексті створення захищеної IoT мережі.

У розробленій топології для створення захищеної мережі Інтернету речей (IoT) було враховано безпеку, витратоефективність, а також легкість утримання та конфігурації для домовласника. Основний акцент був зроблений на захисті від потенційних загроз та зловмисних атак на мережу IoT. Шляхом використання захисних механізмів, таких як фаєрволи, VPN та протоколи шифрування, було створено надійну і безпечну інфраструктуру для забезпечення конфіденційності, цілісності та доступності даних.

Мережа для IoT-системи поділена на три зони: зону з IoT пристроями, зону мережевої інфраструктури та зону звичайного користування Інтернетом. Це розділення на зони дозволяє створити контрольоване середовище, де кожна зона має свої особливості та рівень доступу. Зона з IoT пристроями призначена для підключення й керування різними пристроями, такими як датчики, актуатори та інші "розумні" пристрої. Зона мережевої інфраструктури містить необхідні компоненти, такі як сервери IoT та інші мережеві пристрої, для забезпечення безперебійної роботи системи. Зона звичайного користування Інтернетом призначена

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		33

для підключення до мережі звичайних пристроїв користувача, наприклад, комп'ютерів та смартфонів.

Зона з мережевою інфраструктурою та доступом в Інтернет захищена фаєрволом під назвою ASA-MANAGEMENT. Цей фаєрвол відповідає за контроль доступу до мережі та фільтрацію трафіку, що надходить та виходить з мережі. Він перевіряє пакети даних на відповідність правилам безпеки та блокує небажані або потенційно шкідливі з'єднання. ASA-MANAGEMENT забезпечує захист мережевої інфраструктури від атак, включаючи DDoS атаки та спроби несанкціонованого доступу до системи.

Зона з IoT пристроями захищена фаєрволом з назвою ASA-HOME, який виконує аналогічні функції контролю доступу та фільтрації трафіку. ASA-HOME забезпечує моніторинг та захист IoT пристроїв від можливих атак, зокрема використання вразливостей цих пристроїв для зловмисних цілей. Встановлення фаєрвола ASA-HOME значно зменшує ризик компрометації пристроїв IoT та можливих наслідків, що з ним пов'язані, таких як несанкціоноване керування пристроями або незаконний доступ до збережених даних.

Між цими двома фаєрволами встановлений ikev2 IPsec site-to-site VPN з шифруванням aes-256 та хешуванням sha-256. Це забезпечує безпечний тунельний канал для передачі даних між зонами з мережевою інфраструктурою та IoT пристроями. Шифрування aes-256 забезпечує високий рівень конфіденційності та захисту даних від несанкціонованого доступу. Хешування sha-256 забезпечує цілісність даних, дозволяючи виявляти будь-які зміни в переданих даних під час транзиту. Встановлення VPN забезпечує безпеку та захист інформації, яка передається між різними зонами мережі IoT, знижуючи ризик несанкціонованого доступу до даних та покращуючи загальний рівень безпеки системи.

Ці дві зони, з мережевою інфраструктурою та з IoT пристроями, добре ізолювані від Інтернету, що додає додатковий рівень захисту. Проте, в разі потреби можна налаштувати VPN тунель, щоб забезпечити безпечне з'єднання до мережі Інтернету з цих зон. Це дозволяє домовласнику використовувати звичайні сервіси та доступ до Інтернету за необхідності, забезпечуючи при цьому захист мережі IoT.

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		34

Також було налаштовано протокол віддаленого доступу SSH та локальну автентифікацію. Це дозволяє домовласнику забезпечити контроль та безпеку доступу до мережі. Протокол SSH забезпечує шифрування та автентифікацію при підключенні до мережевих пристроїв, запобігаючи несанкціонованому доступу. Локальна автентифікація дозволяє контролювати права доступу користувачів та забезпечувати безпеку на рівні мережевих пристроїв.

В зоні з IoT пристроями було налаштовано протокол DHCP для автоматичного призначення IP-адрес та автентифікацію з використанням WPA2-PSK і надійної кодової фрази. Це забезпечує безпечний і контрольований доступ пристроїв до мережі. Автентифікація WPA2-PSK використовує сильне шифрування та персональний пароль, що робить мережу IoT недосяжною для несанкціонованих пристроїв або користувачів. Надійна кодова фраза забезпечує безпеку пароля та утримує пристрої IoT в безпечному стані, запобігаючи можливим атакам на пароль.

Для симуляції мережі Інтернет був налаштований протокол BGP (Border Gateway Protocol) на трьох маршрутизаторах, включаючи WAN маршрутизатор мережі.

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		35

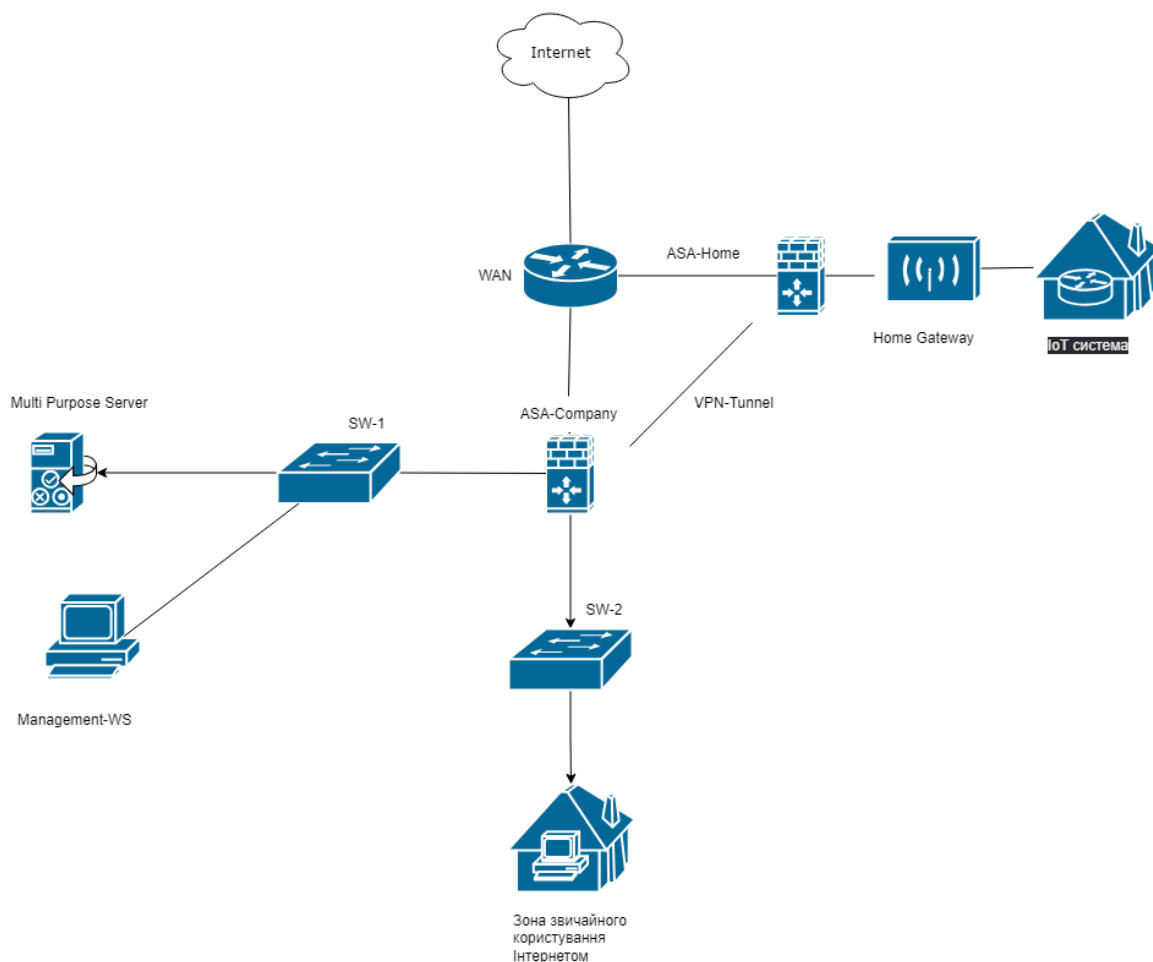


Рисунок 2.4 – Топологія мережі

Таблиця 2.1 – Параметри адресації мережі

Підмережа/ Пристрій	Інтерфейс/ Мережний адаптер/ Шлюз	ІР-адреса	Маска підмережі	Префікс
Підмережа Management	—	192.168.10.0	255.255.255.192	/24
Підмережа out- side	—	209.165.201.224	255.255.255. 248	/29
Підмережа HOME-Internet	—	192.168.11.0	255.255.255.0	/24
Підмережа Home1	—	192.168.33.0	255.255.255.0	/24
Підмережа out- side2	—	209.165.200.224	255.255.255.248	/29
Підмережа WAN-Internet	—	10.191.17.0	255.255.255.252	/30
Підмережа Inter- net- Remote	—	11.191.17.0	255.255.255.252	/30
Підмережа Re- mote	—	192.191.17.0	255.255.255.0	/24

В цілому, розроблена топологія створює захищену IoT мережу, де безпека та ефективність є основними пріоритетами. Застосування захисних механізмів, фаєрволів, VPN тунелів та протоколів шифрування забезпечує високий рівень безпеки та захисту даних в мережі. Такі заходи допомагають уникнути можливих загроз і зловмисних атак, забезпечуючи домовласнику спокій та контроль над Інтернетом речей в їх домі.

Але для запобігання цим кіберзагрозам в розумному будинку на мережевому рівні не достатньо, тільки одноразової конфігурації, рекомендується використовувати сильні паролі, регулярно оновлювати програмне забезпечення мережевих пристроїв, використовувати безпечні протоколи шифрування, налаштовувати нові фаєрволи та VPN-тунелі для контролю доступу та шифрування трафіку, а також бути обережними під час взаємодії з невідомими повідомленнями та посиланнями. Так що по при простоті конфігурування та захищеності користувачам та людям, які обслуговують мережу, потрібно бути відповідальними та обережними.

2.4 Висновки до розділу 2

В другому розділі було проведено дослідження та аналіз обладнання для побудови IoT-системи в розумному будинку. Зокрема, були розглянуті та обрані такі моделі обладнання: Cisco 7204VXR, ASA 5505 та точка доступу Cisco Catalyst 9100L.

Вибір обладнання Cisco 7204VXR зумовлений його потужними характеристиками, які включають високу продуктивність, можливість масштабування та підтримку різноманітних модулів, що забезпечують гнучкість та розширені можливості для мережі IoT. ASA 5505 обрано через його здатність до виконання функцій мережевого екрану та VPN-з'єднань, що забезпечує необхідний рівень безпеки для IoT-системи. Точка доступу Cisco Catalyst 9100L була обрана через свою високу швидкість передачі даних, підтримку стандарту Wi-Fi 6 та здатність працювати в умовах високої щільності підключених пристроїв.

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		37

Оскільки обрано модельний приклад IoT-системи - розумний будинок, було враховано вимоги до безпеки та ефективності. Розумні будинки потребують надійної мережевої інфраструктури, яка забезпечує високий рівень захисту від зовнішніх загроз, а також має бути економічно ефективною та простою в обслуговуванні.

У рамках дослідження була розроблена топологія мережі для IoT-системи в розумному будинку. Вирішено побудувати ikev2 IPsec site-to-site VPN між двома фаєрволами. Це дозволить забезпечити безпечний обмін даними між різними пристроями та системами в мережі IoT, а також захистити їх від несанкціонованого доступу та зловмисних атак.

Загальною метою вибору обладнання та розроблення мережевої топології є створення надійної та безпечної мережі для розумного будинку, яка забезпечує ефективне функціонування IoT-системи. Обране обладнання Cisco 7204VXR, ASA 5505 та точка доступу Cisco Catalyst 9100L, разом із застосуванням ikev2 IPsec site-to-site VPN, відповідають вимогам безпеки, ефективності та економічної доцільності для реалізації IoT-системи в розумному будинку.

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				38
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 3 НАЛАШТУВАННЯ ПРОЄКТУ ПІДСИСТЕМИ ЗАХИСТУ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ ІОТ-СИСТЕМИ НА ПРИКЛАДІ РОЗУМНОГО БУДИНКУ

3.1 Налаштування Мережевих екранів

Перш за все потрібно налаштувати зовнішній та внутрішній інтерфейс.

Сценарій налагодження виглядає так:

```
interface gigabitEthernet0/0
    nameif outside2
    no shut
    security-level 0
    ip address 209.165.200.226
```

Ця частина налаштовує інтерфейс "outside2" з адресою 209.165.200.226. Інтерфейс має найнижчий рівень безпеки 0, який і має мати зовнішня сторона мережі.

```
interface gigabitEthernet0/1
    nameif dmz
    security-level 50
    ip address 192.168.11.1
    no shut.
```

Ця частина налаштовує інтерфейс демілітаризованої зони (DMZ) з адресою 192.168.11.1. Інтерфейс має середній рівень безпеки (security-level 50) .

```
interface gigabitEthernet0/1
    nameif inside
    security-level 100
    ip address 192.168.10.1
    no shut
```

Ця частина налаштовує інтерфейс "inside" з адресою 192.168.10.1. Інтерфейс має найвищий рівень безпеки 100 і використовується для внутрішніх мереж.

```
Route outside 0.0.0.0 0.0.0.0 209.165.200.225
```

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		39

Ця команда встановлює статичний маршрут для всього трафіку (0.0.0.0/0) через зовнішній інтерфейс ASA5505 з використанням IP-адреси 209.165.200.225 як наступного хопу. Це використовується для вказання шлюзу за замовчуванням, до якого мережевий пристрій буде надсилати пакети, якщо не має більш конкретних маршрутів для цільової мережі.

Тепер потрібно налаштувати Ipsec ikev2 site-to-site VPN між двома мережевими екранами.

```
access-list 33_to_center extended permit ip 192.168.33.0 255.255.255.0
192.168.10.0 255.255.255.0
```

ASA-management:

```
access-list center_to_33 extended permit ip 192.168.10.0 255.255.255.0
192.168.33.0 255.255.255.0
```

home:

```
object-group network obj-local
```

```
network-object 192.168.33.0 255.255.255.0
```

```
object-group network obj-remote
```

```
network-object 192.168.10.0 255.255.255.0
```

```
nat (inside,outside) source static obj-local obj-local destination static obj-remote
obj-remote no-proxy-arp route-lookup
```

ASA-management:

```
object-group network obj-local
```

```
network-object 192.168.10.0 255.255.255.0
```

```
object-group network obj-remote
```

```
network-object 192.168.33.0 255.255.255.0
```

```
nat (inside,outside2) source static obj-local obj-local destination static obj-remote
obj-remote no-proxy-arp route-lookup
```

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		40

home:

crypto ikev2 policy 1

encryption aes-256

integrity sha256

group 14

prf sha256

lifetime seconds 43200

ASA-management:

crypto ikev2 policy 1

encryption aes-256

integrity sha256

group 14

prf sha256

lifetime seconds 43200

home:

crypto ipsec ikev2 ipsec-proposal AES

protocol esp encryption aes-256

protocol esp integrity sha-256

ASA-management:

crypto ipsec ikev2 ipsec-proposal AES

protocol esp encryption aes-256

protocol esp integrity sha-256

home:

crypto map outside_map 1 match address 33_to_center

crypto map outside_map 1 set peer 209.165.200.226

crypto map outside_map 1 set ikev2 ipsec-proposal AES

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		41

crypto map outside_map interface outside

ASA-management:

crypto map outside_map 1 match address center_to_33
crypto map outside_map 1 set peer 209.165.201.226
crypto map outside_map 1 set ikev2 ipsec-proposal AES
crypto map outside_map interface outside2

home:

tunnel-group 209.165.201.226 type ipsec-l2l
tunnel-group 209.165.201.226 general-attributes
default-group-policy GroupPolicy_209.165.201.226
tunnel-group 209.165.201.226 ipsec-attributes
ikev2 remote-authentication pre-shared-key 1WWARgNQUn
ikev2 local-authentication pre-shared-key 1WWARgNQUn

ASA-management:

tunnel-group 209.165.200.226 type ipsec-l2l
tunnel-group 209.165.200.226 general-attributes
default-group-policy GroupPolicy_209.165.200.226
tunnel-group 209.165.200.226 ipsec-attributes
ikev2 remote-authentication pre-shared-key 1WWARgNQUn
ikev2 local-authentication pre-shared-key 1WWARgNQUn

Home:

crypto ikev2 enable outside
ASA-management:
crypto ikev2 enable outside

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		42

Ці налаштування були зроблені для створення IPsec IKEv2 site-to-site VPN (віртуальної приватної мережі між двома мережами), щоб забезпечити шифрування та захист трафіку, що переміщується між IoT системою і зоною, де знаходиться мережава інфраструктура.

Далі був налаштований статичний NAT для зони з доступом інтернет:

```
object network DMZ-SERVER
```

```
host 192.168.11.3
```

```
nat (dmz,outside) static 209.165.200.227
```

```
access-list outside extendet permit icmp any host 192.168.2.3 ip any  
209.165.200.227
```

```
access-group outside-dmz in interface outside2
```

Після цього було налаштовано локальну AAA автентифікацію та віддалений доступ для зони з мережною інфраструктурою за допомогою безпечного протоколу SSH на ASA-MANAGEMENT:

```
enable password MoNOtERmArity
```

```
username admin password istoRYaNtienth privilege 15
```

```
crypto key generate rsa modulus 2048
```

```
ssh 192.168.10.0 255.255.255.0 inside
```

Крім налаштувань, що були описані раніше, було налаштовувані всі пристрої в локальних мережах і в симуляції Інтернету.

Нажаль у емуляторів є свої обмеження тому симуляція IoT-системи була реалізована в cisco packet tracer.

Проект повторює відповідний проект в GNS3.

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		43

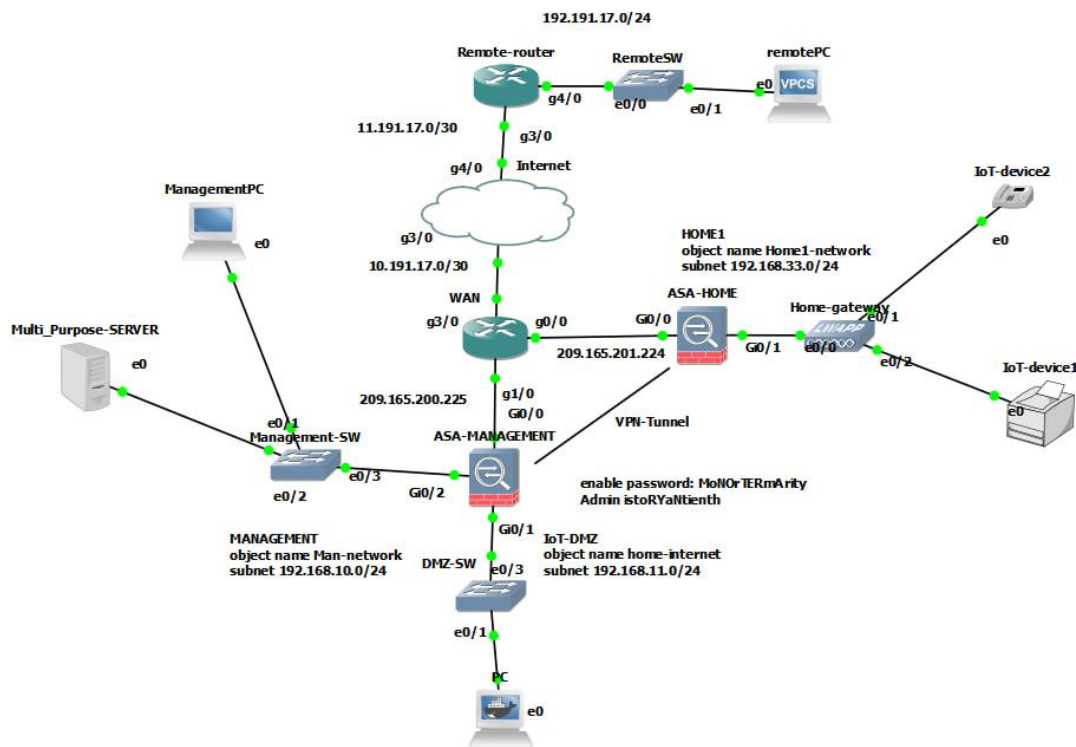


Рисунок 3.3 – Проект підсистеми захисту мережної інфраструктури IoT-системи

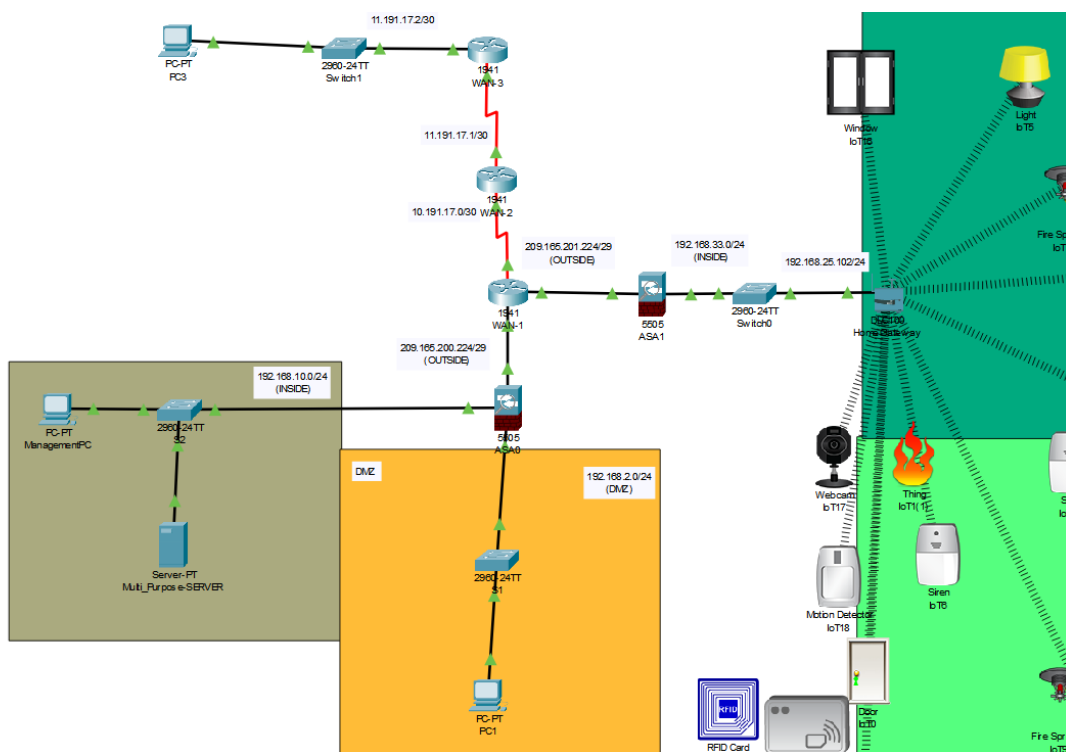


Рисунок 3.4 – Проект підсистеми захисту мережної інфраструктури IoT-системи

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				44
Змн.	Арк.	№ докум.	Підпис	Дата		

Перш за все була налаштована точка доступу (access point). Точка доступу є центральним пристроєм, який забезпечує бездротове з'єднання між пристроями IoT та мережею.

При налаштуванні точки доступу для підсистеми захисту мережної інфраструктури IoT-системи, були враховані наступні аспекти:

Аутентифікація: Точка доступу була налаштована з вимогою аутентифікації пристроїв перед підключенням до мережі. Це дозволяє перевірити легітимність пристроїв та забезпечити доступ тільки авторизованим користувачам.

Шифрування даних: Точка доступу була налаштована для використання шифрування даних, що передаються по бездротовій мережі. Це забезпечує конфіденційність і захист від перехоплення чутливої інформації.

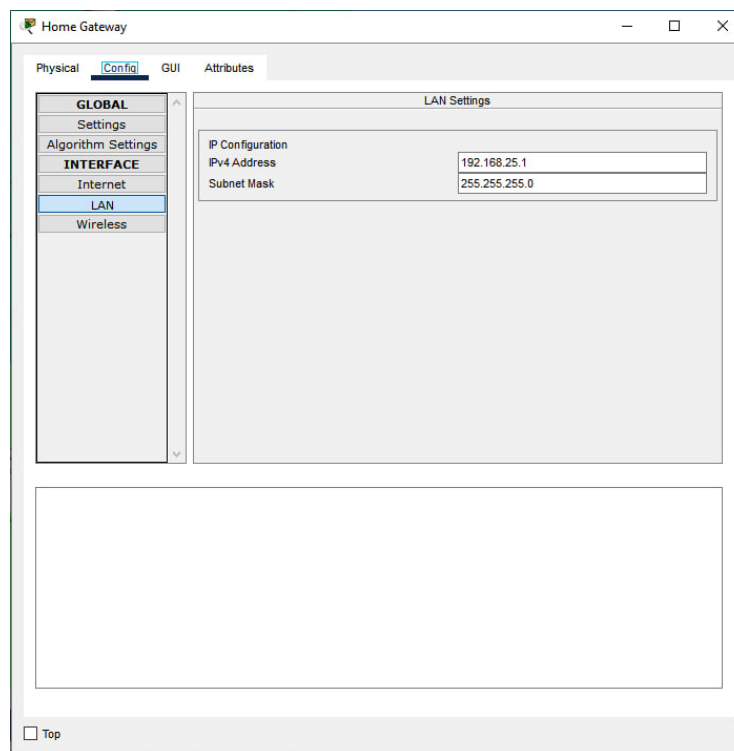


Рисунок 3.5 – Налаштування точки доступу для LAN IoT-системи

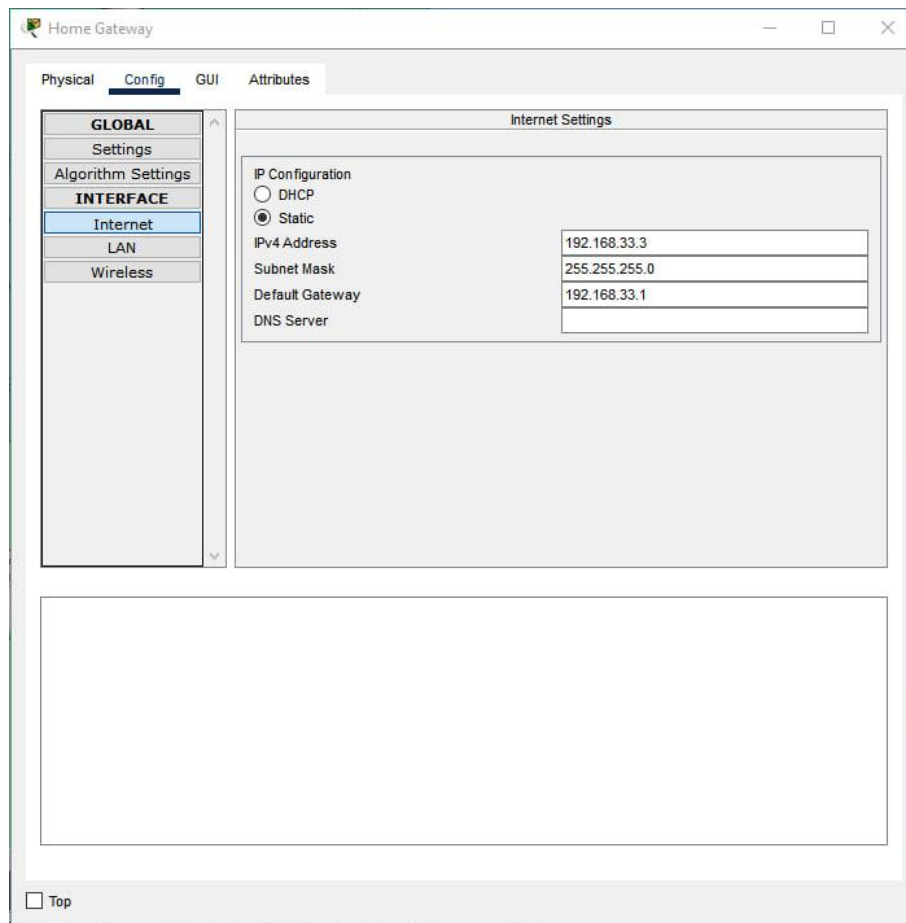


Рисунок 3.6 – Налаштування точки доступу для підключення до зовнішнього інтерфейсу

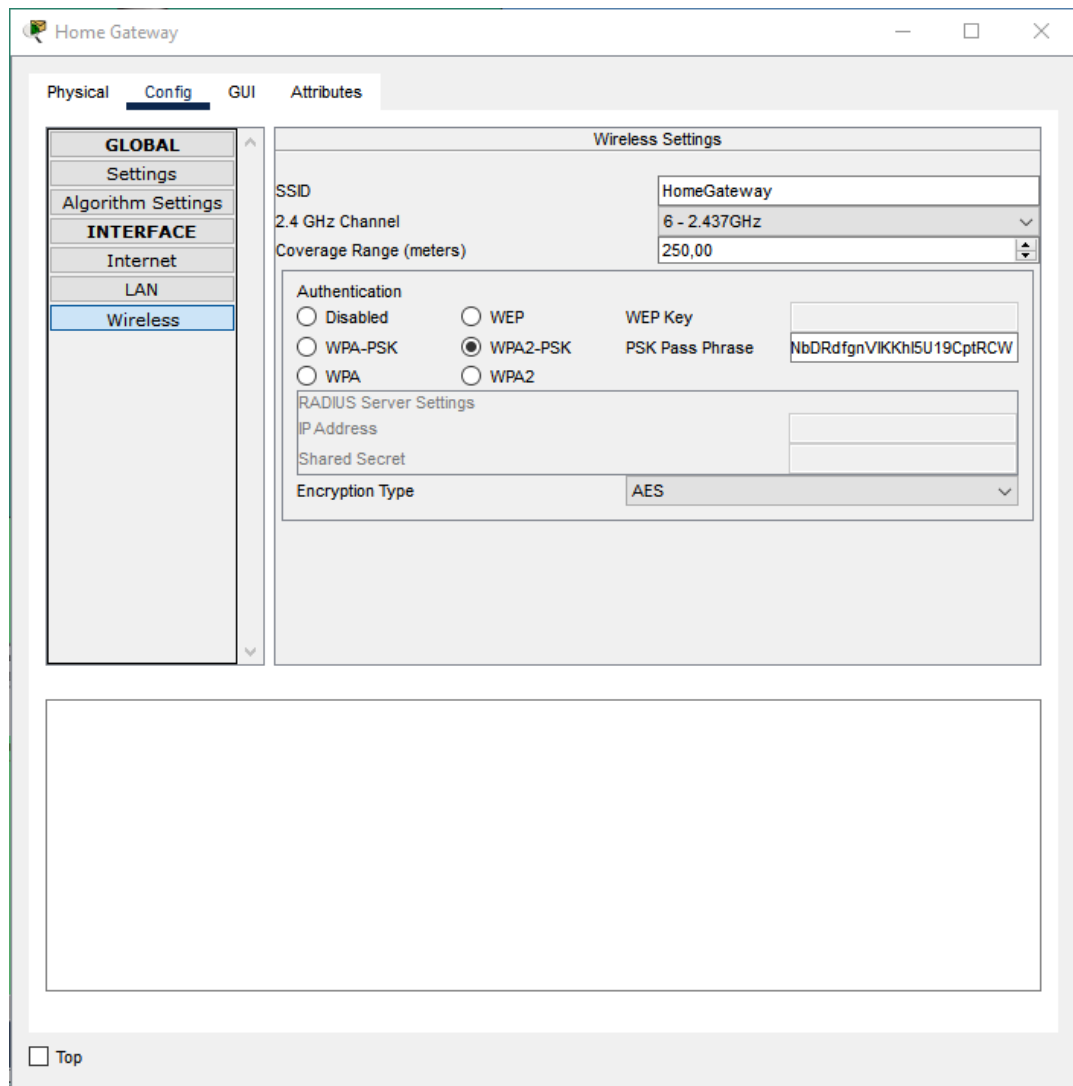


Рисунок 3.7 – Налаштування точки доступу для підключення безпроводних підключень

На елементах IoT-системи налаштовано WPA2-PSK (Wi-Fi Protected Access - Pre-Shared Key) з парольною фразою "O6Nh8I1fNbDRdfgnVIKKhI5U19CptRCW". Це єдиний ключ, який використовується для аутентифікації та шифрування з'єднання Wi-Fi між пристроями IoT та мережею.

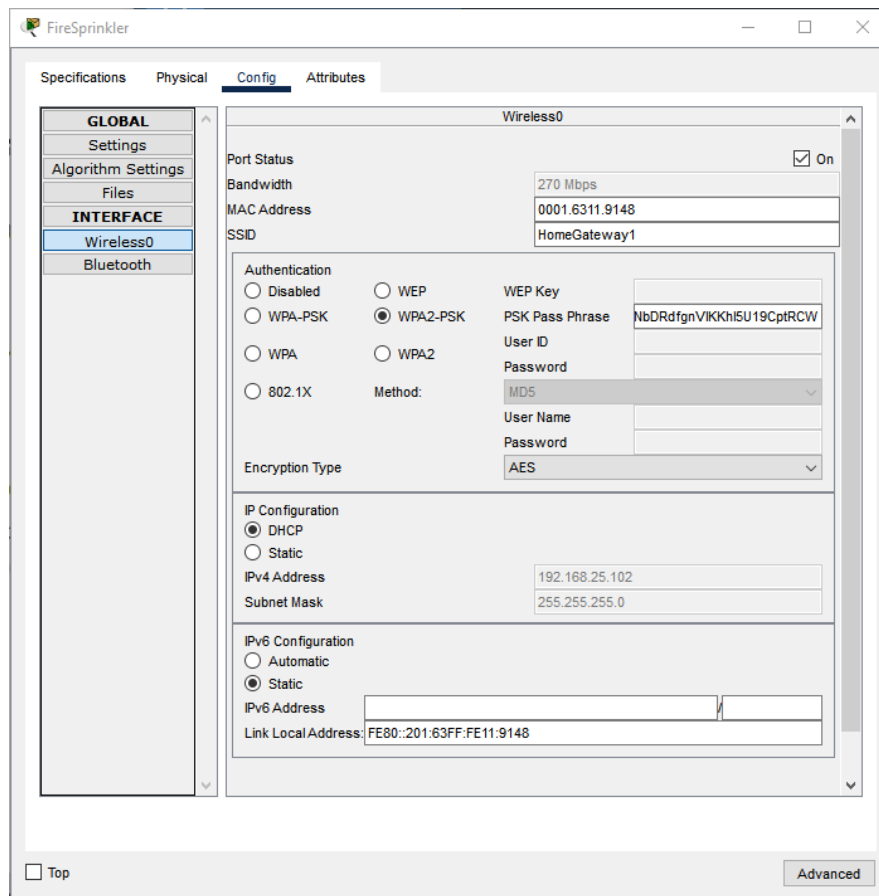


Рисунок 3.8 – Налаштування одного з елементів IoT-системи

3.2 Перевірка працездатності

Найважливіші налаштування були зроблені для створення IPsec IKEv2 site-to-site VPN (віртуальної приватної мережі між двома мережами), щоб забезпечити шифрування та захист трафіку, що переміщується між IoT системою і зоною, де знаходиться мережева інфраструктура.

Для перевірки працездатності проекту підсистеми захисту мережної інфраструктури IoT-системи перш за все потрібно перевірити VPN тунель, який зв'язує між собою дві головні частини IoT-системи всередині мережі.

Тож спробуємо отримати доступ до мережі IoT-системи.

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		48

```

Multi_Purpose-SERVER - PuTTY
host (192.168.10.1) not reachable

VPCS> ping 192.168.33.3
host (192.168.10.1) not reachable

VPCS> ping 192.168.33.3
192.168.33.3 icmp_seq=1 timeout
84 bytes from 192.168.33.3 icmp_seq=2 ttl=64 time=29.420 ms
84 bytes from 192.168.33.3 icmp_seq=3 ttl=64 time=22.284 ms
84 bytes from 192.168.33.3 icmp_seq=4 ttl=64 time=16.871 ms
84 bytes from 192.168.33.3 icmp_seq=5 ttl=64 time=20.968 ms

VPCS> ping 192.168.33.3
192.168.33.3 icmp_seq=1 timeout
192.168.33.3 icmp_seq=2 timeout
192.168.33.3 icmp_seq=3 timeout
84 bytes from 192.168.33.3 icmp_seq=4 ttl=64 time=20.121 ms
84 bytes from 192.168.33.3 icmp_seq=5 ttl=64 time=23.042 ms

VPCS> ping 192.168.33.3
84 bytes from 192.168.33.3 icmp_seq=1 ttl=64 time=21.400 ms
84 bytes from 192.168.33.3 icmp_seq=2 ttl=64 time=17.915 ms
84 bytes from 192.168.33.3 icmp_seq=3 ttl=64 time=21.889 ms
84 bytes from 192.168.33.3 icmp_seq=4 ttl=64 time=20.090 ms
84 bytes from 192.168.33.3 icmp_seq=5 ttl=64 time=17.506 ms

VPCS>

```

Рисунок 3.9 – Зв’язок між IoT-приладом та IoT-сервером

```

QEMU (ASA-MANAGEMENT) - TightVNC Viewer
Active Tunnels: 1
Previous Tunnels: 1
In Octets: 37806
In Packets: 455
In Drop Packets: 0
In Drop Fragments: 0
In Notifys: 11
In P2 Exchange: 451
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In IPSEC Delete: 0
In IKE Delete: 1
Out Octets: 37804
Out Packets: 455
Out Drop Packets: 0
Out Drop Fragments: 0
Out Notifys: 12
Out P2 Exchange: 451
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out IPSEC Delete: 0
Out IKE Delete: 0
SAs Locally Initiated: 2
SAs Locally Initiated Failed: 0
<--- More --->_

```

Рисунок 3.10– Статистика VPNa

Тепер потрібно перевірити чи важливі мережі ізольовані від інтернет підключення і чи доступний хост з зони для доступу в інтернет.

```

remotePC - PuTTY

PC1> ping 209.165.200.227
84 bytes from 209.165.200.227 icmp_seq=1 ttl=255 time=3.147 ms
84 bytes from 209.165.200.227 icmp_seq=2 ttl=255 time=3.556 ms
84 bytes from 209.165.200.227 icmp_seq=3 ttl=255 time=11.677 ms
84 bytes from 209.165.200.227 icmp_seq=4 ttl=255 time=7.614 ms
84 bytes from 209.165.200.227 icmp_seq=5 ttl=255 time=6.895 ms

PC1> ping 192.168.10.3
*209.165.200.227 icmp_seq=1 ttl=255 time=11.421 ms (ICMP type:3, code:1, Destination host unreachable)
*209.165.200.227 icmp_seq=2 ttl=255 time=8.198 ms (ICMP type:3, code:1, Destination host unreachable)
*209.165.200.227 icmp_seq=3 ttl=255 time=7.707 ms (ICMP type:3, code:1, Destination host unreachable)
*209.165.200.227 icmp_seq=4 ttl=255 time=10.255 ms (ICMP type:3, code:1, Destination host unreachable)
*209.165.200.227 icmp_seq=5 ttl=255 time=6.588 ms (ICMP type:3, code:1, Destination host unreachable)

PC1> ping 192.168.33.3
*209.165.200.227 icmp_seq=1 ttl=255 time=3.470 ms (ICMP type:3, code:1, Destination host unreachable)
*209.165.200.227 icmp_seq=2 ttl=255 time=3.055 ms (ICMP type:3, code:1, Destination host unreachable)
*209.165.200.227 icmp_seq=3 ttl=255 time=4.419 ms (ICMP type:3, code:1, Destination host unreachable)
*209.165.200.227 icmp_seq=4 ttl=255 time=12.468 ms (ICMP type:3, code:1, Destination host unreachable)
*209.165.200.227 icmp_seq=5 ttl=255 time=9.329 ms (ICMP type:3, code:1, Destination host unreachable)

PC1>
PC1>
PC1>
PC1>
PC1>
PC1>
PC1>
PC1>
PC1>

```

Рисунок 3.11– Безуспішні спроби пропінгувати захищені мережі та успішні для хоста

Після цього перевіряєм чи наявне підключення IoT пристроїв до IoT-сервера в середовищі Packet tracer

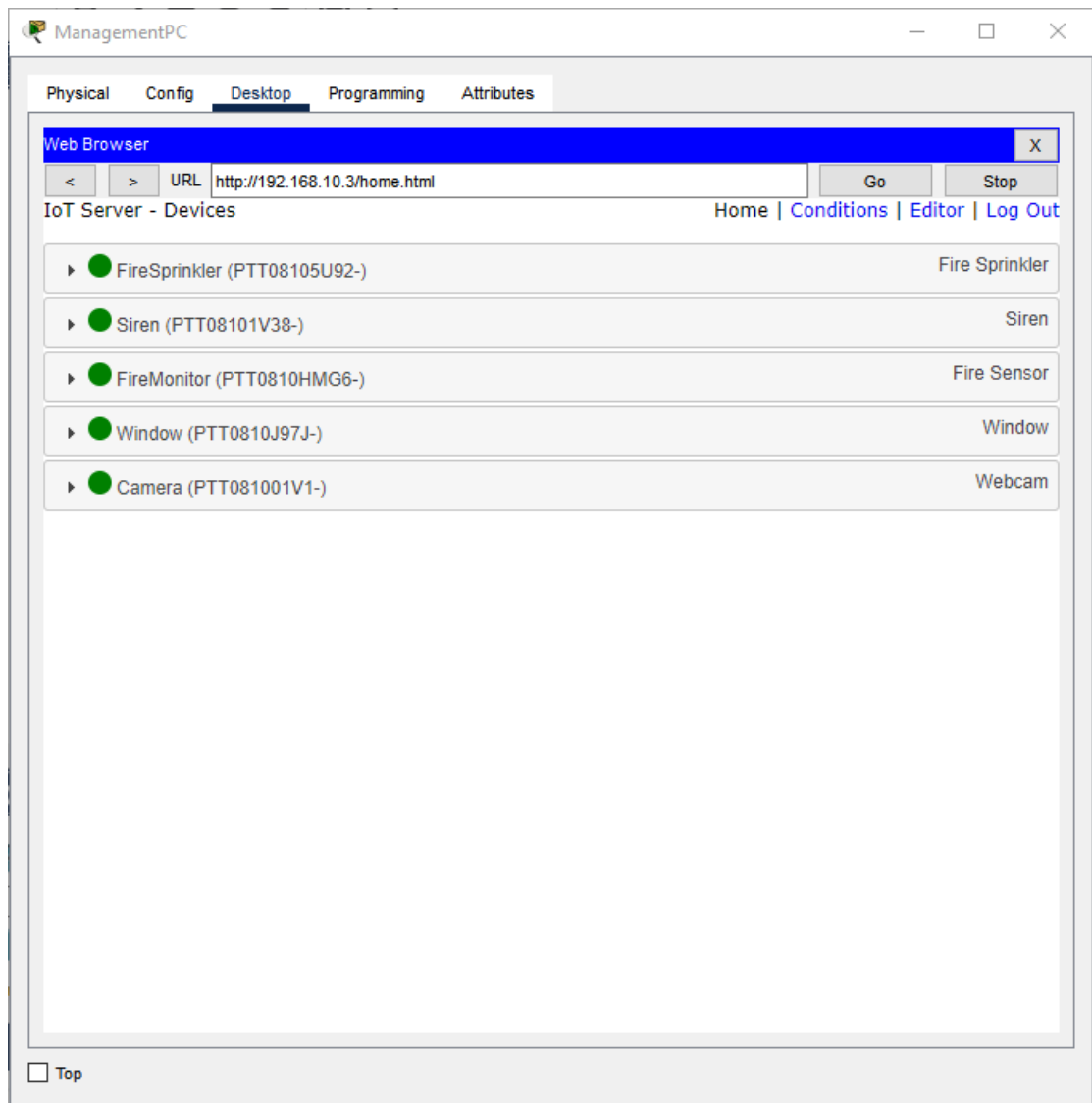


Рисунок 3.12 – Успішне підключення IoT-пристроїв після Аутентифікації
За допомогою WPA2-PSK

3.3 Висновки до розділу 3

У третьому розділі кваліфікаційної роботи проведено перевірку працездатності та було проведено налаштування мережевих екранів для реалізації IoT-системи. Була виконана налаштування локальної AAA автентифікації на ASA-MANAGEMENT, що забезпечує автентифікацію та авторизацію. Також було успішно налаштовано ikev2 IPsec site-to-site VPN між двома фаєрволами, що забезпечує безпечний та зашифрований обмін даними між IoT-системою та мережевою інфраструктурою.

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				51
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі, система IoT була налаштована, включаючи налаштування WPA2-PSK на елементах IoT-системи. Це забезпечує захищене бездротове з'єднання між пристроями IoT, що є важливим аспектом забезпечення безпеки та приватності в IoT-системі. Також було проведено налаштування точки доступу (access point), яка виступає центральним пристроєм для бездротового з'єднання між пристроями IoT та мережею.

У результаті проведених налаштувань та перевірок, було підтверджено працездатність всієї системи. Усі компоненти мережі, включаючи мережеві екрани, VPN-з'єднання, систему IoT та точку доступу, успішно працювали відповідно до очікувань та вимог проекту. Це свідчить про успішну реалізацію обраної моделі IoT-системи в розумному будинку та демонструє ефективність використання обраного обладнання та налаштувань для забезпечення безпеки та надійності мережевої інфраструктури.

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				52
Змн.	Арк.	№ докум.	Підпис	Дата		

ВИСНОВКИ

У кваліфікаційній роботі був розроблений проект підсистеми захисту мережної інфраструктури IoT-системи на основі моделі розумного будинку. Ця підсистема складається з трьох зон: мережної інфраструктури, IoT-системи та ізольованої зони для виходу в Інтернет.

Основною метою проекту було забезпечити високий рівень безпеки, одночасно зберігаючи економічну доцільність та легкість обслуговування підсистеми. Для досягнення цих цілей було вибрано обладнання Cisco 7204VXR, ASA 5505 та точку доступу Cisco Catalyst 9100L, які відповідають вимогам безпеки, ефективності та економічної доцільності.

З метою забезпечення безпечного та захищеного обміну даними між мережевою інфраструктурою та IoT-системою, було успішно налаштовано ikev2 IPsec site-to-site VPN. Цей механізм забезпечує шифрування та захист даних під час їх передачі між цими зонами, створюючи захищений тунель для безпечного обміну інформацією.

Окрім того, IoT-система була налаштована з використанням автентифікації по WPA2-PSK, яка є широко використовуваним протоколом забезпечення безпеки в бездротових мережах. З правильною парольною фразою, цей метод автентифікації є надійним і забезпечує безпеку з'єднання між пристроями IoT та мережею.

В результаті реалізації проекту підсистеми захисту, досягнуто високого рівня безпеки мережної інфраструктури IoT-системи в розумному будинку. При цьому, було збережено економічну доцільність та легкість обслуговування підсистеми, що є важливими аспектами для успішної реалізації проектів IoT-систем в розумних будинках.

Загалом, розроблений проект підсистеми захисту відповідає вимогам безпеки та надає надійний захист мережної інфраструктури IoT-системи. Цей проект демонструє успішну інтеграцію обладнання Cisco 7204VXR, ASA 5505 та точки доступу Cisco Catalyst 9100L в модель розумного будинку. Враховуючи важливість безпеки та ефективного використання ресурсів, підсистема захисту є економічно доцільною

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				
Змн.	Арк.	№ докум.	Підпис	Дата		53

та легко обслуговується, що є ключовими факторами для успішної реалізації IoT-систем в розумних будинках.

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				54
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кулаков Ю.О., Луцький Г.М. Комп'ютерні мережі. Підручник / За ред. Ю.С. Ковтанюка. – К.: Юніор, 2003. – 400 с.
2. A1tzori L. Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm / L. Atzori, A. Lera, G. Morabito. // Ad Hoc Networks. – 2017. – №56. – С. 121–140.
3. Rouse M. Internet of things (IoT) / Margaret Rouse. – New York, 2019. – 624 с.
4. Challenges when Realizing a Fully Distributed Internet-of-Things – How we Created the SensibleThings Platform / S.Forsström, V. Kardeby, P. Österberg, U. Jennehag. // The Ninth International Conference on Digital Telecommunications. – 2014. – С. 13–18.
5. Eui-Nam H. Fog Computing and Smart Gateway Based Communication for Cloud of Things / H. Eui-Nam, M. Aazam. // International Conference on Future Internet of Things and Cloud. – 2014. – С. 25–62.
6. MediaSense – an Internet of Things Platform for Scalable and Decentralized Context Sharing and Control / [S. Forsström, V. Kardeby, J. Walters та ін.]. // The Seventh International Conference on Digital Telecommunications. – 2012. – С. 27– 32.
7. Наукове дослідження Інтернету речей Hewlett Packard Enterprise [Електронний ресурс] – Режим доступу до ресурсу: https://www.network-cultures.org/uploads/notebook2_theinternetofthings.pdf.
8. Створення інформаційної системимоніторингу забруднення атмосферногоповітря міста на основі технології «інтернет речей» / [В. Б. Мокін, Б. Ю. 89 Собко, М. В. Дратований та ін.]. // вінницький національний технічний університет. – 2017. – №3. – с. 49–57.
9. Xiang Y. Low-rate DDoS attacks detection and traceback by using new information metrics / Y. Xiang, K. Li, W. Zhou. // IEEE Transactions on Information Forensics and Security. – 2011. – С. 426–437.

		Савченко І.В			<i>ККІКБ.КР.Б – 125 – 15 – ПЗ</i>	Арк.
		Бродський Ю. Б				55
Змн.	Арк.	№ докум.	Підпис	Дата		

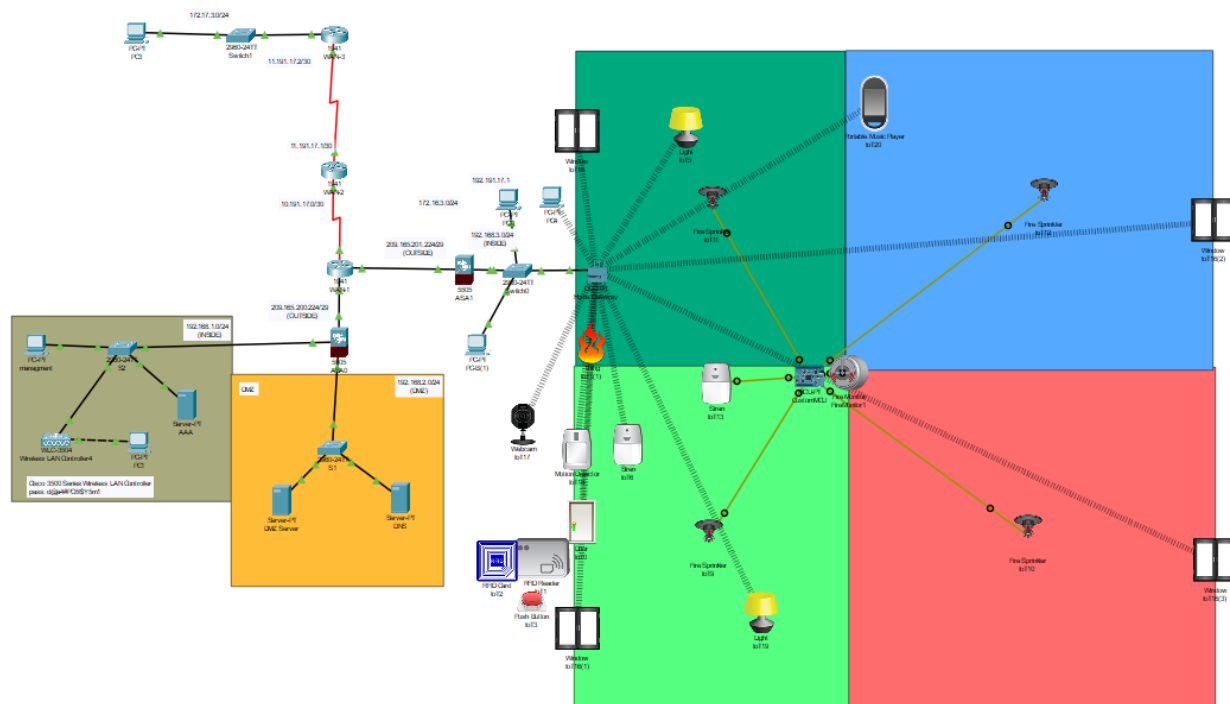
10.Coetzee and J. Eksteen. The Internet of Things-promise for the future? An introduction. ISTAfrica Conference Proceesing. – 2011. – С. 1-9.

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				56
Змн.	Арк.	№ докум.	Підпис	Дата		

ДОДАТКИ

		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				57
Змн.	Арк.	№ докум.	Підпис	Дата		

Детальна схема побудованої мережі в cisco Packet Tracer



		Савченко І.В			ККІКБ.КР.Б – 125 – 15 – ПЗ	Арк.
		Бродський Ю. Б				58
Змн.	Арк.	№ докум.	Підпис	Дата		