ДВНЗ «Донецький національний технічний університет»

Факультет комп'ютерно-інформаційних технологій та автоматизації

(повне найменування інституту, назва факультету)

Кафедра автоматики та телекомунікацій

(повна назва кафедри)

«До захисту допущено»
В.о. завідувача кафедри автоматики та телекомунікацій
_____ Валерій ПОЦЕПАЄВ
(підпис) (ім'я та прізвище)
«___» _____ 2024 р.

Випускна кваліфікаційна робота

бакалавра

(освітньо-кваліфікаційний рівень)

на тему «Розробка системи захисту від кіберзагроз для телекомунікаційної інфраструктури IoT-мережі»

Виконав студентка 4 курсу, групи ТКР-20

(шифр групи)

спеціальності 172 Телекомунікації та радіотехніка

(шифр і назва спеціальності)

Каптан Дар'я Миколаївна _____

(Прізвище, Ім'я та По-батькові) (підпис)

Керівник ст. викл. кафедри АТ _____ Гліб СТУПАК

(посада, науковий ступінь, вчене звання, прізвище та ім'я) (підпис)

Рецензент к.т.н., доц., доц. кафедри ЕТКІ _____ Ганна ШЕЇНА

(посада, науковий ступінь, вчене звання, прізвище та ім'я) (підпис)

Нормоконтроль:

Дар'я ЖУКОВСЬКА

17.06.2024 р.

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

Студент _____

(підпис)

Луцьк – 2024 р.

ДВНЗ «Донецький національний технічний університет»
Факультет комп'ютерно-інформаційних технологій та автоматизації
(повне найменування інституту, назва факультету)
Кафедра автоматики та телекомунікацій
(повна назва кафедри)

Захист відбувся _____

(дата)

з оцінкою_____

Секретар ЕК _____

(підпис)

Випускна кваліфікаційна робота

бакалавра

Тема: «Розробка системи захисту від кіберзагроз для телекомунікаційної інфраструктури IoT-мережі»

Виконавець, студент
гр. ТКР – 20 _____ Дар'я КАПТАН
(підпис, дата, Ім'я ПРІЗВИЩЕ)
Керівник _____ Гліб СТУПАК
(підпис, дата, Ім'я ПРІЗВИЩЕ)
Консультанти: _____ Дар'я ЖУКОВСЬКА
(підпис, дата, Ім'я ПРІЗВИЩЕ)
_____ Ганна ТЕЛИЧКО
(підпис, дата, Ім'я ПРІЗВИЩЕ)

Нормоконтроль _____ Дар'я ЖУКОВСЬКА
(підпис, дата, Ім'я ПРІЗВИЩЕ)

Луцьк – 2024 р.

Державний вищий навчальний заклад
"Донецький національний технічний університет"

Інститут, факультет Комп'ютерно-інформаційних технологій та автоматизації
Кафедра Автоматика та телекомунікації
Освітньо-кваліфікаційний рівень бакалавр
Галузі знань 17 Електроніка та телекомунікації
(шифр і назва)
Спеціальність 172 Телекомунікації та радіотехніка
(шифр і назва)

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри АТ
Валерій ПОЦЕПАЄВ
«____» _____2024 року

З А В Д А Н Н Я
НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Каптан Дар'я Миколаївна
(прізвище, ім'я, по батькові)
1. Тема проекту (роботи) «Розробка системи захисту від кіберзагроз для телекомунікаційної інфраструктури IoT-мережі»
керівник проекту (роботи) Ступак Гліб Володимирович
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від 25.04.2024 року № 164
2. Строк подання студентом проекту (роботи)_____

3. Вихідні дані до проекту (роботи)_____
Технічна документація та матеріали з переддипломної практики

4.Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
1) Основні існуючи кіберзагрози для телекомунікаційної інфраструкрути IoT-мереж. Найбільш ефективні методи і засоби захисту; 2) Аналіз прототипу IoT-мережі з врахуванням вимог кібербезпеки; 3) Розробка та налаштування моделі захищеної IoT-мережі; 4) Охорона праці.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Топологія IoT-мережі, модель мережі з елементами захисту.

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Ступак Г.В., ст. викл. каф. АТ		
2	Теличко Г.О., доц. каф. АТ		
3	Жуковська Д.О., асист. каф. АТ		
нормоконтроль	Жуковська Д.О., асист. каф. АТ	-	17.06.2024 р.

7. Дата видачі завдання: 25.04.2024

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Аналіз завдання	27.04	
2	Аналіз об’єкту	28.04	
3	Аналіз предметної області	29.04	
4	Визначення ключових трендів	30.04	
5	Аналіз існуючих загроз та вразливостей	07.05	
6	Розробка концепції системи захисту	17.05	
7	Проектування архітектури безпечної мережі	21.05	
8	Вибір та налаштування засобів безпеки	27.05	
9	Реалізація системи захисту	30.05	
10	Тестування	05.06	
11	Охорона праці	12.06	
12	Оформлення	17.06	

Студент _____ **Дар’я КАПТАН**
(підпис) (прізвище та ініціали)

Керівник роботи _____ **Гліб СТУПАК**
(підпис) (прізвище та ініціали)

ЛИСТ ЗАУВАЖЕНЬ

Посада, Ім’я та ПРІЗВИЩЕ	Суть зауваження, оцінка та підпис

АНОТАЦІЯ

Каптан Д.М. Розробка системи захисту від кіберзагроз для телекомунікаційної інфраструктури IoT-мережі / Випускна кваліфікаційна робота на здобуття освітнього ступеня «бакалавр» зі спеціальності 172 Телекомунікації та радіотехніка. – ДВНЗ «ДонНТУ», Луцьк, 2024.

Пояснювальна записка: 85 стор., 41 рис., 15 посиланнь.

У дипломній роботі представлено процес розробки системи захисту від кіберзагроз для телекомунікаційної інфраструктури IoT-мережі. Розроблена система підвищує рівень безпеки та надійності мережевих з'єднань. Вона забезпечує захист даних від несанкціонованого доступу та зменшує ризик кіберінцидентів, що дозволяє безпечно експлуатувати IoT-мережу у складних умовах сучасного кіберпростору.

В процесі виконання роботи, було проведено оцінку ризиків та вразливостей мережевих компонентів. Визначено потенційні кіберзагрози, які можуть вплинути на телекомунікаційну інфраструктуру IoT-мережі.

Ключові слова: ІНТЕРНЕТ РЕЧЕЙ, КІБЕРБЕЗПЕКА, ХМАРНІ СЕРВІСИ, ТЕЛЕКОМУНІКАЦІЙНА ІНФРАСТРУКТУРА, ІОТ-ПРИСТРОЇ, ШИФРУВАННЯ ДАНИХ, АУТЕНТИФІКАЦІЯ, КОНТРОЛЬ ДОСТУПУ, СЕГМЕНТАЦІЯ МЕРЕЖІ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

M2M - Machine-to-Machine

IIoT - Industrial Internet of Things

ПЛК - програмовані логічні контролери

IoT - Internet of Things

AI - Artificial intelligence

NLP - Natural language processing

DVR - Digital Video Recorder

NVR - Network Video Recorder

ПЗ - програмне забезпечення

IT - Information Technology

USB - Universal Serial Bus

DDoS - Distributed Denial of Service attack

NFC - Near Field Communication

2FA - Two-Factor Authentication

MFA - multi-factor authentication

AES - Advanced Encryption Standard

WPS - Wi-Fi Protected Setup

WPA2 - Wi-Fi Protected Access 2

GPS - Global Positioning System

RTK - Real-Time Kinematic

DGNSS - Differential Global Navigation Satellite System

DGPS - Differential Global Positioning System

JTAG - Joint Test Action Group

SSH - Secure Shell

DNS - Domain Name System

CSP - Content Security Policy

LAN - Local Area Network

VPN - Virtual Private Network

DoS - Denial of Service

API - Application Programming Interface

MITM - Man in the middle

IDS - Intrusion Detection System

IPS - Intrusion Prevention System

VLAN - Virtual Local Area Network

ПК - Персональний комп'ютер

IPv4 - Internet Protocol version 4

ISP - Internet Service Provider

DHCP - Dynamic Host Configuration Protocol

ACL - Access Control List

SIEM - Security information and event management

SSID - Service Set Identifier

HTTP - HyperText Transfer Protocol

HTTPS - Hyper Text Transfer Protocol Secure

URL - Uniform Resource Locator

ВСТУП

Хоча Інтернет речей може здатися новим явищем, його походження сягає XIX століття. У 1832 році барон Шиллінг створив перший електромагнітний телеграф, що дозволяв здійснювати пряму комунікацію між двома машинами за допомогою передачі електричних сигналів. Ця міжмашинна взаємодія (M2M) лягла в основу подальшого розвитку технологій.

IoT має широкі можливості, від спрощення повсякденного життя користувачів до перетворення різних галузей, у тому числі виробництва. Можна припустити, що розвиток промислового Інтернету речей (IIoT) почався у 1992 році, коли програмовані логічні контролери (ПЛК) отримали здатність до підключення. З того часу вони відіграють важливу роль у розробці та використанні автоматизованих ліній зборки та промислових роботів на заводах.[4]

Сучасний світ вже важко уявити без цього, повсякденне життя охоплено низкою технологічних процесів. За допомогою IoT пристроїв ми можемо здійснювати моніторинг, управління та взаємодію з навколишнім середовищем, збільшуючи ефективність, зручність та безпеку нашого життя і бізнесу. Проте разом з неймовірними можливостями виникають і нові виклики, пов'язані з безпекою, конфіденційністю та захистом даних.

Всі знають наскільки важливо зберігати конфіденційну інформацію, але чи точно знають як це роботи? Багато речей залежить безпосередньо від користувача, його відповідальності, розуміння та готовності забезпечити захист для себе. Багато залежить і від виробників, зокрема фізична захищеність пристрою та можливість його цифрового захисту, але якщо не користуватися певними правилами та можливостями захисту, то нараженя на небезпеку стає надто вірогідною подією. В нашому часі хакери можуть скористатися будь якими пристроями з вашої системи, для досягнення своєї мети, тому дуже важливо знати можливі ризики та вміти їх запобігати.

Мета роботи: розробка системи захисту від кіберзагроз для

телекомунікаційної інфраструктури IoT-мережі з метою підвищення безпеки та надійності мережевих підключень і захисту даних.

Об'єкт дослідження: телекомунікаційна інфраструктура IoT-мережі, що включає мережеві пристрої, сервіси, і кінцеві IoT-пристрої.

Предмет дослідження: методи та засоби захисту від кіберзагроз, зокрема технології шифрування, аутентифікації, контролю доступу та безпечної веб-комунікації.

Завдання:

1. Проаналізувати можливі кіберзагрози для телекомунікаційної інфраструктури IoT-мережі.

2. Визначити вразливості мережевих компонентів.

3. Розробити стратегію захисту мережі, включаючи використання сучасних технологій безпеки.

4. Реалізувати безпечну архітектуру мережі з урахуванням сегментації та захисту хмарних сервісів.

5. Провести тестування розробленої системи.

Актуальність роботи: зростом кількості IoT-пристроїв та їх інтеграції у телекомунікаційні мережі зростає і ризик кіберзагроз, що можуть завдати значної шкоди інфраструктурі та конфіденційності даних. Розробка ефективних засобів захисту є критично важливою для забезпечення безпеки та надійності таких мереж у сучасному кіберпросторі. Дана робота спрямована на вирішення актуальних проблем безпеки в IoT-мережах, що робить її значущою для наукової та практичної спільноти.

Методи дослідження:

Аналіз літератури та нормативних документів. Це дозволило скласти уявлення про загрози та вразливості, які можуть впливати на IoT-мережі, а також про існуючі підходи до їх захисту.

Створення моделі IoT-мережі. За допомогою цього методу, можна виявити потенційні вразливості ще на етапі проектування та оцінити, як різні заходи безпеки впливатимуть на загальну стійкість мережі.

Експериментальне впровадження мережі. Це дозволило побачити, як система захисту працює в умовах, наближених до реальних, та допомогло виявити та виправити можливі недоліки.

Результат:

Визначено та класифіковано основні кіберзагрози, що можуть вплинути на телекомунікаційну інфраструктуру IoT-мережі. Було проведено оцінку вразливості мережевих компонентів, таких як пристрої, протоколи зв'язку та програмне забезпечення.

Розроблено стратегію, що включає використання сучасних методів шифрування даних, аутентифікації користувачів та контролю доступу. Впроваджено багаторівневу модель безпеки, яка враховує фізичну, мережеву та прикладну безпеку.

Реалізовано архітектуру сегментації мережі для ізоляції критичних компонентів, а також безпечну взаємодію хмарних сервісів з внутрішньою мережею складу, що дозволяє використовувати віддалені сервіси без ризику компрометації даних.

Структура та обсяг роботи – 85 сторінок, 41 рисунок, 15 використаних джерел.

1 АНАЛІЗ КІБЕРЗАГРОЗ ДЛЯ ІОТ-СИСТЕМ.

1.1 Загальна характеристика IoT-мереж та систем.

Інтернет речей (IoT) описує мережу фізичних об'єктів - "речей", оснащених датчиками, програмним забезпеченням та іншими технологіями для підключення та обміну даними з іншими пристроями та системами через Інтернет. Ці пристрої можуть бути як звичайними предметами побуту, так і складними промисловими інструментами. Експерти очікують, що кількість активних пристроїв буде налічувати близько 22 мільярдів до 2025 року.[1]

Протягом останніх років IoT став однією з ключових технологій XXI століття. Тепер, коли ми можемо підключати предмети побуту - кухонне обладнання, автомобілі, термостати, радіоняні - до Інтернету за допомогою вбудованих пристроїв, відбувається безперешкодна комунікація між людьми, процесами та об'єктами.

Завдяки доступним обчислюваним ресурсам, хмарним технологіям, великим даним, аналітиці та мобільним технологіям фізичні об'єкти можуть обмінюватися даними та збирати їх, при цьому втручання людини мінімальне. У цьому гіперпов'язаному світі цифрові системи можуть реєструвати, відстежувати та регулювати кожну взаємодію між підключеними об’єктами. Фізичний світ зустрічається з цифровим - і вони співпрацюють.

Хоча ідея IoT існує вже давно, останні досягнення в різних технологіях зробили її практичною:

1. Доступність недорогих сенсорних технологій. Доступні та надійні датчики роблять IoT доступним для більшої кількості виробників.

2. Зв'язок. Багато мережевих протоколів спростили підключення датчиків до хмари та інших "речей" для більш ефективної передачі даних.

3. Платформи хмарних обчислень. Збільшення доступності хмарних платформ дозволяє як підприємствам, так і споживачам отримувати доступ до

інфраструктури, необхідної для масштабування, без необхідності фактичного управління цим.

4. Машинне навчання та аналітика. Завдяки досягненням у сфері машинного навчання та аналітики, а також доступу до різноманітних та великих обсягів даних, що зберігаються в хмарі, компанії можуть збирати інформацію швидше та простіше. Поява цих супутніх технологій продовжує розширювати межі, і дані, що виробляються Інтернетом речей, також живлять ці технології.

5. Голосовий штучний інтелект (AI). Досягнення у сфері нейронних мереж внесли обробку природної мови (NLP) до пристроїв IoT (таких як цифрові особисті помічники Alexa, Cortana та Siri) і зробили їх привабливими, доступними та придатними для домашнього використання.

Промисловий Інтернет речей (IIoT) використовується для застосування технології Інтернету речей в промисловому середовищі, особливо щодо контролю і вимірювань, а також управління датчиками та пристроями, які використовують хмарні технології. Останнім часом галузі використовують міжмашинну комунікацію (M2M), щоб забезпечити бездротову автоматизацію та контроль. Проте з появою хмарних і супутніх технологій (таких як аналітика та машинне навчання) галузі можуть досягти нового рівня автоматизації та створити нові джерела доходів і бізнес-моделі. IIoT іноді називають четвертою промисловою революцією або Індустрією 4.0. Нижче наведено деякі загальні області використання IIoT:

1.Розумне виробництво;

2.Підключені активи та передбачуване обслуговування;

3.Розумні електромережі;

4.Розумні міста;

5.Підключена логістика;

6.Розумні цифрові ланцюги постачання.

Організації, які найбільше виграють від IoT, це ті, які можуть інтегрувати датчикові пристрої у свої бізнес-процеси.

Виробництво:

Виробники можуть здобути конкурентну перевагу, використовуючи моніторинг виробничих ліній для передбачуваного технічного обслуговування обладнання за умови виявлення датчиками майбутньої несправності. Це дозволяє знижувати витрати на експлуатацію, забезпечувати кращу доступність обладнання та покращувати управління активами.

Автомобільна промисловість:

Використання IoT в автомобільній галузі може значно підвищити безпеку водіїв та забезпечити прогнозоване технічне обслуговування для автомобілів на дорозі за допомогою реальних часових сповіщень про можливі відмови обладнання.

Транспорт та логістика:

Застосування в транспорті та логістиці дозволяє ефективне управління транспортними засобами та вантажами з використанням даних від датчиків. Це дозволяє оптимізувати маршрутизацію та знижувати затримки.

Інші галузі, такі як роздрібна торгівля, охорона здоров'я та загальна безпека праці, також можуть виграти від використання технологій для вдосконалення своїх процесів та підвищення рівня захисту.

До основних характеристик мереж та систем Інтернету речей відносяться наступні:

Можливість підключення: пристрої можуть підключатися до Інтернету, забезпечуючи обмін даними між пристроями, користувачами та хмарними сервісами.

Датчики та виконавчі механізми: зазвичай прилади оснащені різними типами датчиків (температури, вологості, руху тощо), які збирають дані з навколишнього середовища, а також виконавчими механізмами, які можуть виконувати певні дії на основі зібраних даних.

Зв'язок: IoT можуть використовувати різні технології зв'язку, такі як Wi-Fi, Bluetooth, Zigbee, LoRaWAN тощо, для передачі даних.

Хмарне зберігання та обробка даних: зібрані дані можуть бути збережені та оброблені у хмарних сервісах для аналізу, використання та подальшого

управління.

Масштабованість: системи IoT повинні мати здатність масштабуватися, щоб враховувати зростання кількості підключених пристроїв і обсягу оброблюваних даних.

Безпека: спираючись на попередній фактор, безпека є критичною характеристикою мереж та систем Інтернету речей. Забезпечення конфіденційності, цілісності та доступності даних є важливою задачею.[1]

Отже, основною характеристикою мереж та систем є їхня здатність до підключення, збору, передачі, аналізу та управління даними з різних пристроїв для досягнення певних цілей у різних сферах.

1.2 Типи загроз, які впливають на безпеку IoT

З розвитком технологій зростає онлайн-вразливість пристроїв та мереж Інтернету. Безпека IoT передбачає захист пристроїв та мереж, до яких вони підключені, від онлайн-загроз і вторгнень.

Взагалі безпека Інтернету речей - це широкий термін, що охоплює стратегії, інструменти, процедури, системи та методи, які використовуються для захисту всіх складових. Для забезпечення доступності, цілісності та конфіденційності екосистеми необхідно захищати фізичні компоненти, додатки, дані та мережеві з'єднання.[3]

Впровадження IoT пристроїв ставить перед користувачем та IT-командою завдання забезпечення безпеки. Комплексний підхід може допомогти ефективно вирішувати проблеми.

В середньому, щотижня 54% організацій стикаються з спробами кібератак, спрямованими на пристрої Інтернету речей. Найбільш піддаються атакам пристрої в європейських організаціях, за якими слідують організації з Азіатсько-Тихоокеанського регіону та Латинської Америки. Сучасні технології стали неодмінною частиною нашого повсякденного життя. Одним з факторів, які сприяли зростанню кібератак, є швидка цифрова трансформація.

Атаковані пристрої різноманітні: маршрутизатори, IP-камери, DVR (цифрові відеореєстратори), NVR (мережеві відеореєстратори), принтери та багато іншого. Динаміки та IP-камери, стають все більш поширеними в середовищах віддаленої роботи та навчання, що надає кіберзлочинцям безліч потенційних точок входу.

Надійна стратегія безпеки охоплює всі аспекти захисту, такі як підсилення компонентів, оновлення вбудованого програмного забезпечення, відстеження, контроль доступу, виявлення загроз та усунення вразливостей.

Проблеми безпеки часто виникають через те, що пристрої Інтернету речей не розробляються з урахуванням безпеки як головного пріоритету, більшість розробників систем більше зосереджуються на функціональності пристроїв. Це може мати серйозні наслідки для користувачів і призвести до потенційних витоків даних. Нижче наведений список проблем безпеки, пов'язаних із згаданими вище пристроями, які можуть піддатися ризику. [5]

Відсутність фізичної безпеки.

Недостатня фізична безпека на пристроях є легкою мішенню для зловмисників. Протягом тривалого часу пристрої IoT, розміщені у віддалених районах, стають доступними за допомогою фізичних змін. Хакери можуть легко скористатися проблемами безпеки на пристроях з недостатньою або взагалі відсутньою фізичною безпекою.

Наприклад, пристрої Інтернету речей можуть бути інфіковані шкідливим ПЗ через USB-накопичувачі. Основна відповідальність виробників полягає в наданні пріоритету фізичній безпеці. Проте створення безпечних і захищених передавачів та датчиків за доступною ціною може виявитися складною задачею для розробників.

Відсутність видимості.

Для IT-команди є складним завданням забезпечити видимість всіх пристроїв в мережі, оскільки багато з них не зареєстровані в інвентарних записах IT. Наприклад, кавоварки, системи вентиляції та кондиціювання повітря, не мають значення для відстеження IT-командами.

Служби безпеки не зможуть запобігти взломам, якщо вони не зможуть бачити, що підключено до мережі. Відсутність видимості пристроїв ускладнює можливість точного обліку того, що потрібно захищати та контролювати.

Конфіденційність даних.

В Інтернеті речей серйозною проблемою є конфіденційність даних. Інформація користувачів передається через багато пристроїв, наприклад, дані пацієнтів з медичного обладнання та особиста інформація з розумних іграшок та носимих пристроїв.

Наприклад, хакер або кіберзловмисник може зібрати корпоративні дані та розголосити, продати або використовувати їх для вимагання викупу у власника.

Ботнет та DDoS-атаки.

Ботнети та DDoS-атаки є одними з найбільш поширених загроз для пристроїв IoT. Ботнети представляють собою мережі взламаних пристроїв, які керуються кіберзлочинцями. Ці ботнети можуть бути використані для запуску розподілених атак типу «відмова у обслуговуванні» (DDoS), які перевантажують цільовий сервер або веб-сайт великими обсягами трафіку, що призводить до його недоступності.

Програми-вимагачі.

У цій проблемі безпеки Інтернету речей атаки програм-вимагачів шифрують та блокують доступ до конфіденційних файлів. Хакер вимагає викуп за ключ розшифрування для розблокування файлів.

Пристрої Інтернету речей зі слабкою безпекою також можуть стати об'єктами, але випадки атак програм-вимагачів на IoT наразі не спостерігаються.

Шпигунство та прослуховування.

Пристрої з вбудованими мікрофонами та камерами можуть бути взламані для слідкування за окремими людьми чи організаціями. Це може призвести до порушення конфіденційності та розголошення приватних розмов чи інтелектуальної власності.

Атаки «людина посередині».

Під час цих атак кіберзлочинці перехоплюють і змінюють зв'язок між

пристроями Інтернету речей та пов'язаними з ними серверами або мережами. Це може призвести до маніпулювання даними, несанкціонованого доступу або прослуховування повідомлень.

Медичні гаджети, розумний дім та інші інтелектуальні пристрої можуть бути у небезпеці у майбутньому через їх зростаючу цінність для власників та залежність від цих пристроїв як від критично важливих систем.[6]

Звісно теоретично легко обговорювати можливі загрози, тому розглянемо чотири реальні приклади взлому Інтернету речей.

1. Незахищена мережа університету: У звіті Verizon Data Breach Digest за 2017 рік описується приклад університету, чиє мережа була завалена запитами DNS для ресторанів морепродуктів. Зловмисники використовували 5000 пристроїв Інтернету речей, таких як торгові автомати та системи освітлення, для атаки на університетську мережу через слабкі паролі.

2. Взлом IoT-камер: Деякі камери безпеки IoT, зокрема NeoCoolCam, виявились з важливими проблемами безпеки, що дозволяє їх взламувати. Використовуючи ці камери, зловмисники можуть незаконно спостерігати або навіть проникнути в мережу.

3. Ботнет Mirai: Це зловмисна програма, яка заражає мережеві пристрої, які працюють на Linux, шукаючи вразливі пристрої IoT в Інтернеті. Вона використовує фабричні імена користувачів та паролі, що встановлені за замовчуванням, для доступу до пристроїв.

4. Взлом автомобіля Jeep: Дослідники Чарлі Міллер і Кріс Валасек змогли використати вразливості в системі розваг автомобіля Jeep Cherokee, щоб віддалено керувати автомобілем. Це включало можливість впливати на рульове керування та гальма, що створювало серйозну загрозу безпеці.[7]

1.3 Інструменти, технології, методи для підвищення рівня безпеки IoT мереж.

Найкращі практики забезпечення безпеки Інтернету речей включають в

себе наступне:

Використання надійних протоколів аутентифікації та шифрування: Застосування надійних методів аутентифікації користувачів та шифрування даних є важливими для запобігання несанкціонованому доступу та збереження конфіденційності інформації. Адміністраторам важливо розуміти широкий спектр протоколів, які використовуються в їх системах Інтернету речей, оскільки це дозволить їм ефективно зменшити ризики та запобігти загрозам безпеки. Ці протоколи можуть варіюватися від стандартних і широко відомих, таких як Bluetooth та Near Field Communication (NFC), до менш відомих, таких як nRF24, nRFxx, 443МГц, LoRA та LoRaWAN, а також оптичних та інфрачервоний зв'язок. Це допоможе забезпечувати сумісність та інтеграцію різних протоколів в межах системи IoT.

1. Протоколи аутентифікації розуміють під собою використання надійних протоколів, таких як двофакторна аутентифікація (2FA) або багатофакторна аутентифікація (MFA), дозволяє впевнитися у легальності доступу до системи. Прикладом може бути введення пароля та отримання коду підтвердження на мобільний телефон.

2. Шифрування є процесом кодування даних, який робить їх доступними лише авторизованим користувачам, є ключовим для забезпечення безпеки в IoT. Широко використовується стандарт шифрування AES, який забезпечує надійний рівень захисту. Використовуйте надійні та унікальні паролі для всіх облікових записів. Надійні паролі допомагають у запобіганні багатьох кібератак. Менеджери паролів можуть допомогти користувачам створювати унікальні та надійні паролі, які користувачі можуть зберігати в самому додатку або програмному забезпеченні.

Контроль доступу: Встановлення правильного контролю доступу до пристроїв і мережі зберігає дані в безпеці та допомагає уникнути їх несанкціонованого використання . Загалом, це визначення того, хто або що має право доступу до конкретних ресурсів. Це може бути реалізовано через управління обліковими записами користувачів та наділення їх відповідними

правами доступу. Програмні рішення, такі як AWS IoT Core від Amazon, забезпечують ці функції.

Надайте перевагу безпеці Wi-Fi. Деякі способи, якими користувачі можуть це зробити, включають увімкнення брандмауера роутера, вимкнення WPS та ввімкнення протоколу безпеки WPA2, а також використання надійного пароля для доступу до Wi-Fi. Забезпечення безпеки налаштувань роутера також є важливою частиною цього кроку.

Забезпечте збіг IoT-хмар та використовуйте хмарні рішення. Інтернет речей та хмара стають все більш інтегрованими. Важливо враховувати вплив кожної технології на безпеку іншої. Хмарні рішення також можна розглядати як додаткові засоби безпеки та можливості обробки даних на периферійних пристроях Інтернету речей.

Регулярне оновлення програмного забезпечення: оновлення ПЗ є критично важливим для забезпечення безпеки пристроїв. Своєчасне оновлення дозволяє виправляти виявлені вразливості та запобігати потенційним атакам. Однією з ключових рекомендацій є постійне відстеження та впровадження оновлень для всіх пристроїв та програмного забезпечення.

Особливу увагу варто приділяти бібліотекам та пакетам, які використовуються в розробці програмного забезпечення. Оскільки більшість оновлень спрямовані на усунення відомих шляхів проникнення, що знаходять зловмисники, своєчасне застосування цих оновлень значно знижує ризик компрометації.

Загалом, регулярне оновлення ПЗ є фундаментальною практикою для підтримання безпеки IoT-систем, що допомагає мінімізувати ризики та захищати дані від потенційних загроз.

Існують інструменти автоматичного оновлення залежностей, такі як Dependabot або Renovate. Вони спрощують процес підтримки актуальності кодової бази. Ці інструменти автоматизують завдання перевірки та застосування оновлень до залежностей. Вони усувають необхідність ручних перевірок з боку розробників. Ці інструменти гарантують, що кодова база буде оновлена до

останніх безпечних версій.[11]

Моніторинг уразливостей та аудити безпеки: Проведення регулярних моніторингів уразливостей системи та аудитів безпеки допомагає вчасно виявляти потенційні загрози та запобігати їхньому використанню зловмисниками. Аудит безпеки відіграє ключову роль у забезпеченні надійності та цілісності додатків Інтернету речей. Вони включають в себе:

1. Ретельне тестування, аналіз та оцінку заходів безпеки,

2. Виявлення потенційних вразливостей (наприклад, потенційних точок входу для шкідливих атак).

Вони також повідомлять вас про слабкі механізми аутентифікації чи недостатні протоколи шифрування. Проводячи аудит безпеки, організації можуть виявити та усунути слабкі місця безпеки.

Огляд коду - важка практика для забезпечення безпеки. В ньому бере участь людина, яка відрізняється від розробника, що написав код. Така особа переглядає код з іншої точки зору, що дозволяє їй виявити потенційні проблеми безпеки та кодування, які могли бути пропущені автором.

Завдяки перевірці коду розробники можуть скористатися новими поглядами та досвідом. Інтегруючи регулярну перевірку коду в процес розробки, організації можуть підвищити безпеку.

Юридичний аудит включає перевірку політики на відповідність певним законам та правилам. Оцінюючи вимоги, юристи виявляють прогалини в заходах безпеки. Вони можуть рекомендувати необхідні дії та забезпечувати відповідність правових рамок. Це дозволить знизити юридичні та нормативні ризики.

Політика конфіденційності також є важливою складовою, яка описує, як ви збираєте, зберігаєте та передаєте дані своїх користувачів. Юристи також допомагають у впровадженні механізмів захисту даних та механізмів згоди.

Створення культури безпеки: важливо розвивати усвідомленість про безпеку серед користувачів та персоналу, щоб уникнути простих помилок та захистити систему від внутрішніх загроз.

Забезпечення безпеки важкого використання GPS є важливим аспектом для деяких пристроїв та застосунків Інтернету речей, оскільки це може створювати потенційні проблеми з захищеностю. Особливу увагу слід приділяти випадкам, коли сигнали GPS можуть бути перешкоджені або навіть підроблені, особливо якщо вони використовуються для систем позиціонування у виробництві, моніторингу та інших функцій. Якщо ці системи є важливими для компанії, у ній також повинні існувати засоби моніторингу сигналів GPS. Ще одним варіантом може бути використання компанією інших систем позиціонування, таких як Real-Time Kinematic (RTK) або Differential GNSS (DGNSS або DGPS).[8]

Також не слід забувати, що з моменту створення будь-який фізичний пристрій може підлягати несанкціонованому втручанню способом, не передбаченим виробником чи продавцем.

Пристрої Інтернету речей є особливою ціллю, оскільки вони мають багато функцій, які можуть бути цікавими для інших:

1.Можуть знаходитися в приватних, віддалених або необслуговуваних місцях, тому доступ не обмежений як фізично, так і за часом.

2.Деякі пристрої IoT можуть мати невеликий розмір, тому їх легко приховати в разі крадіжки.

3. З характеру та місцезнаходження пристрою часто стає зрозуміло, що якщо він буде скомпрометований, то його використають для атаки на конкретну ціль. Як тільки один пристрій опиниться в руках зловмисника, багато подібних пристроїв також будуть взламані, що в подальшому призведе до можливої розподіленої атаки типу "відмова в обслуговуванні" на бажаний об’єкт. Такий алгоритм дій, спрямований на пристрої IoT, може надати хакеру подальший доступ до мережі.

4. Деякі пристрої можуть використовуватися протягом багатьох років. Технології розвиваються, тож з часом може стати легше взламати пристрій, створений на базі застарілих технологій.

Щоб скомпрометувати пристрій, що знаходиться безпосередньо перед

злодієм, він скоріш за все виконає наступні дії:

1.Фізичне відкриття пристрою для доступу до його складових частин. Це може включати розбірку корпусу або видалення захисних панелей для доступу до компонентів пристрою.

2.Підключення до фізичного порту пристрою. Це може бути використання різних кабелів або адаптерів для підключення до портів, які можуть надати доступ безпосередеьо до системи або даних пристрою.

3.Використання безконтактної технології для виявлення активності пристрою. Наприклад, це може включати використання приладів для виявлення електромагнітного випромінювання, високо- або низькочастотних звуків, коливань напруги живлення тощо.[9]

Ключем до досягнення будь-якої з цих цілей є доступ до пристрою. Чим більше захисних заходів використовується для забезпечення безпеки пристрою, тим більше часу і зусиль потрібно для його компрометації.

Як вже раніше згадувалось, про майбутню безпеку мають піклуватися не лише безпосередні користувачі, але й виробники пристроїв, розглянемо способи забезпечення захищеності пристроїв з точки зору виробництва, та що варто зробити, якщо постачальники все ж таки знехтували цими заходами.

Першим кроком у захисті пристрою перед запуском у виробництво є видалення всіх фізичних, радіо- або оптичних портів, які використовувалися для розробки. Звичайно, для підключення виробничого пристрою до локальної мережі або знову до хмари потрібен принаймні один порт, але всі інші порти, які вже не потрібні, повинні бути видалені, включаючи будь-які відповідні доріжки на печатній платі, які з'єднують порт зі схемою.

Аналогічно, ідеально видалити всі тестові точки, включаючи контакти та доріжки, або, принаймні, ефективно заборонити доступ до тестування, наприклад, спалюючи вбудовані запобіжники для JTAG.

Якщо виробничому пристрою необхідно мати який-небудь порт адміністрування, це стане основною ціллю зловмисників. Тому логічний доступ до цього порту повинен бути дуже жорстко заблокований. Отже, на ньому

повинен працювати єдиний сервіс, необхідний для адміністрування, всі інші сервіси повинні бути вимкнені і не відповідати на запити інструментів сканування тощо. Сервіс адміністрування повинен використовувати безпечний протокол, такий як SSH; використання небезпечного протоколу, такого як Telnet, на адміністративному порту фактично залишає пристрій широко відкритим. Управління обліковими даними для доступу до цього порту повинно бути безпечним та ефективно управленим, щоб гарантувати, що доступ не може бути несанкціонованим.

Чіпи, які керують критично важливими функціями, іноді можуть бути видалини зловмисниками з печатних плат, щоб вони могли підключити їх до випробувального обладнання для аналізу. Щоб запобігти цьому, чіпи ключів можна приклеїти епоксидною смолою до печатної плати або інших елементів, щоб чіп руйнувався під час його видалення. Крім того, вся схема може бути вбудована в блок смоли, що зробить її абсолютно недоступною для всіх, крім самих рішучих.

Звичайно, останньою лінією захисту є сам корпус пристрою. Це може забезпечити фізичний захист внутрішніх частин, стати частиною монтажного вузла та допомогти захиститися від виявлення випромінювання. Один з варіантів — зробити пристрій постійно відключеним, якщо корпус відкритий.

Завжди існує ризик того, що пристрій може бути підроблений десь у ланцюжку постачання, наприклад, на складі або під час транспортування. Для візуальної індекації будь-якої спроби втручання у продукт можна використовувати упаковку або пломби, що захищають від несанкціонованого доступу.[9]

Не слід забувати що є спеціальні пристрої Інтернету Речей, такі як датчики або камери відеоспостереження, які допомагають у підвищенні безпеки, але їх також слід в свою чергу захищати та налаштовувати відповідно. Доцільно створювати своєрідні «обманки», які будуть відволікати зловмисника, концентруючи увагу на собі, поєднувати системи захисту та інше.

Ще одна корисна порада буде розглянути можливість отримання реально-

часових повідомлень про небезпеку та виявляти здатність до передбачення в управлінні кібербезпекою майбутніх загроз, для забезпечення фізичної безпеки пристроїв Інтернету речей

Висновки до розділу 1

В наші часи, де технології постійно розвиваються та вдосконалюються, Інтернет речей грає важливу роль у перетворенні нашого оточення та взаємодії з ним. Від побутових пристроїв до великих промислових систем, IoT надає безліч можливостей для управління. Для максимального використання потенціалу мережі необхідно розробляти та впроваджувати найкращі практики забезпечення безпеки, бо це є дуже важливим аспектом. Оскільки все більше пристроїв стають підключеними до Інтернету, ризики стати жертвою кіберзлочинності зростають. Тож інтегрування заходів безпеки є ключовим правилом.

Це означає розробку та впровадження надійних механізмів аутентифікації та авторизації, використання шифрування для захисту конфіденційності даних, а також регулярне оновлення програмного забезпечення для усунення виявлених уразливостей. Крім того, важливо проводити аудит безпеки та моніторинг мережі для виявлення та запобігання потенційним загрозам.

Зокрема, слід приділяти увагу захисту від атак типу DDoS, використанню надійних паролів та безпеці Wi-Fi мереж. Також важливо бути готовим до можливих атак на системи з використанням GPS та вміти вчасно реагувати на них.

Однак зусилля забезпечення безпеки не повинні обмежуватися лише технічними заходами. Важливо також мати відповідні юридичні та організаційні політики, які регулюють збір, зберігання та обробку даних, а також реагування на можливі інциденти безпеки.

У висновках необхідно підкреслити важливість фізичного захисту в контексті Інтернету речей. Фізичний захист пристроїв є одним з головних

елементів загальної стратегії безпеки, оскільки він забезпечує захист від прямого доступу до обладнання та його компонентів.

Приділяти увагу слід обмеженням доступу до пристроїв та їх з'єднань. Це може включати в себе видалення непотрібних портів та тестових точок з плат, а також застосування захисних кожухів або блокувань для запобігання фізичному втручанню.

Не слід забувати про фізичний захист у контексті розміщення пристроїв. Наприклад, для пристроїв, що встановлюються в публічних місцях або віддалених локаціях, важливо забезпечити їх захист від несанкціонованого доступу та втручання.

Фізичний захист також включає заходи для запобігання від крадіжок та втрати пристроїв. Це може включати в себе застосування систем відстеження, використання безпекових кріплень та неможливості відкриття корпусу без авторизованого доступу.

Загалом, фізичний захист є невід'ємною складовою стратегії безпеки Інтернету речей і варто надавати йому належну увагу при розробці та впровадженні IoT-систем.

Тільки комплексний підхід до забезпечення безпеки в умовах IoT дозволить максимально використати потенціал цієї технології та забезпечити надійність та конфіденційність інформації в цифровому світі. Це дозволить забезпечити безпеку та прозорість в світі, де IoT стає все більш важливим елементом нашого повсякденного життя.

2 АНАЛІЗ ЦІЛІСНОСТІ (БЕЗПЕЧНОСТІ) IOT МЕРЕЖІ

2.1 Опис існуючої IoT-мережі компанії

Наша мережа представляє собою схему IoT-мережі, що включає декілька сегментів і різні пристрої, які підключені до Інтернету та один до одного. Топологія наведена нижче на Рис.2.1.

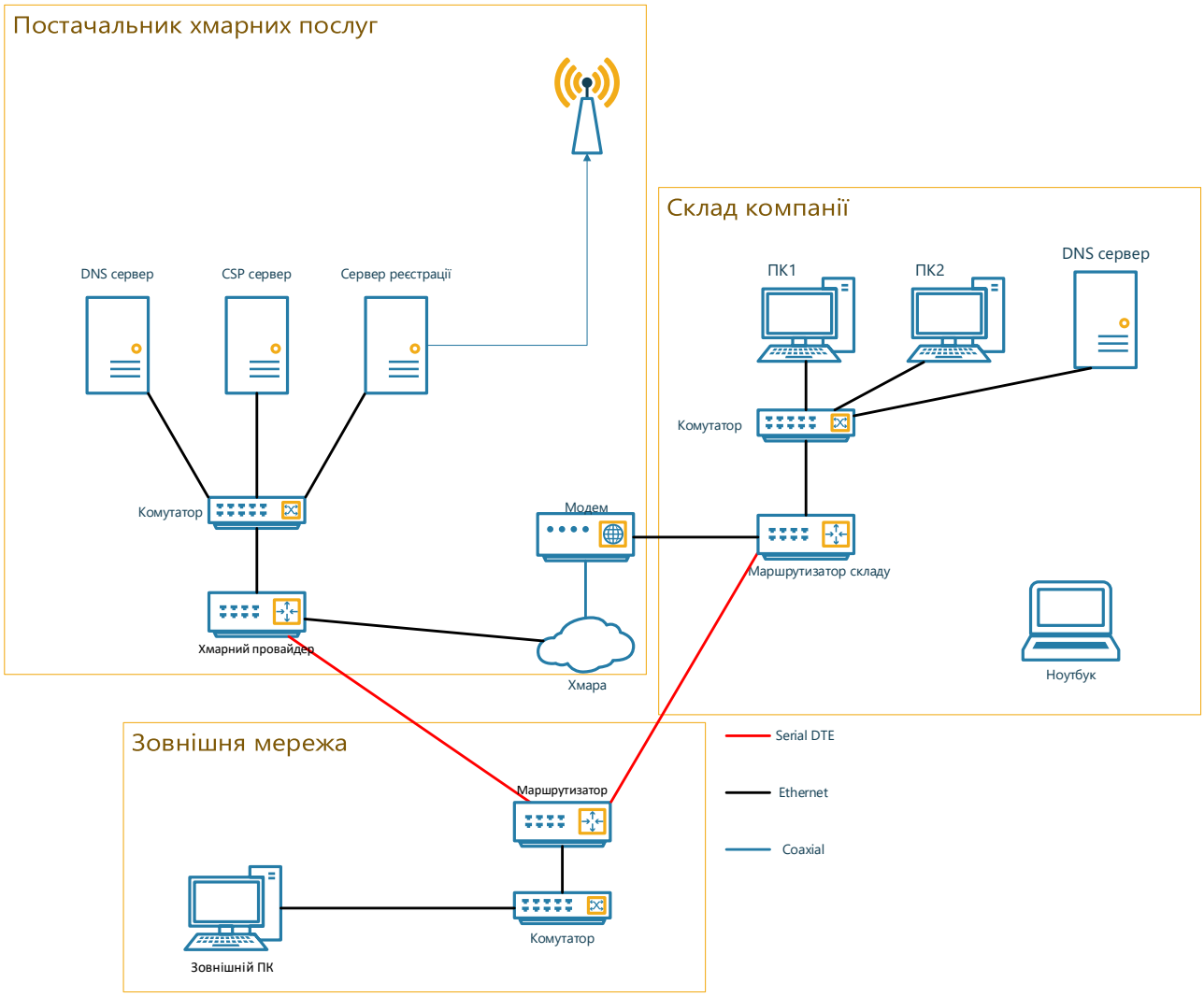

Рисунок 2.1 – Топологія IoT-мережі

Ця IoT-мережа складається з трьох основних секцій: постачальник хмарних послуг, склад компанії та зовнішня мережа. Давайте розглянемо кожну з них окремо.

Перший сектор-постачальник хмарних послуг.

У цій секції знаходяться наступні компоненти:

-DNS сервер підключений до комутатора.

-CSP сервер підключений до комутатора.

-Сервер реєстрації підключений до комутатора.

-Комутатор, який з'єднує всі сервери та підключений до хмарного провайдера.

Другий сектор-склад компанії.

У цій секції знаходяться наступні компоненти:

-ПК1 підключений до комутатора.

-ПК2 підключений до комутатора.

-DNS сервер підключений до комутатора.

-Комутатор, що з'єднує всі вищезгадані пристрої та підключений до маршрутизатора складу.

-Маршрутизатор складу, який з'єднує комутатор складу з хмарним провайдером через хмару за допомогою модема.

Третій сектор-зовнішня мережа.

У цій секції знаходяться наступні компоненти:

-Зовнішній ПК, підключений до комутатора.

-Комутатор, що з'єднує зовнішній ПК з маршрутизатором.

-Маршрутизатор, що з'єднує комутатор із хмарним провайдером через послідовне з'єднання (Serial DTE).

Все сектори мають з’єднання між собою.

Типи з'єднань у мережі:

-Ethernet з'єднання (позначене чорними лініями) використовується для з'єднання серверів, ПК та інших пристроїв із комутаторами та маршрутизаторами.

-Serial DTE з'єднання (позначене червоними лініями) використовується для з'єднання маршрутизаторів між собою.

-Коаксіальне з'єднання (позначене синіми лініями) використовується для

зв'язку з модемом.

Все це між собою з’єднує хмарний провайдер.

Цей вузол з'єднує постачальника хмарних послуг, склад компанії та зовнішню мережу через хмару. Хмарний провайдер забезпечує взаємодію між різними секціями мережі.

На основі наданої схеми, давайте розглянемо детальніше кожний компонент системи.

Сектор постачальника хмарних послуг:

1.DNS сервер

Призначення: DNS (Domain Name System) сервер відповідає за перетворення доменних імен на IP-адреси, що дозволяє користувачам вводити легкозапам'ятовувані доменні імена замість числових IP-адрес.

Функції:

-Розв'язання імен: Перетворює доменні імена на IP-адреси.

-Кешування DNS-записів: Зберігає результати попередніх запитів для прискорення доступу.

-Маршрутизація запитів: Передає запити до інших DNS серверів, якщо сам не може надати відповіді.

2.CSP сервер

Призначення: CSP (Cloud Service Provider) сервери надають обчислювальні ресурси, зберігання даних та інші сервіси через Інтернет.

Функції:

-Хостинг веб-додатків: Забезпечує роботу вебсайтів та додатків.

-Зберігання даних: надає простір для зберігання файлів та баз даних.

-Обробка даних: виконує обчислювальні завдання за запитами користувачів.

-Масштабування ресурсів: автоматично збільшує або зменшує кількість ресурсів відповідно до потреб клієнтів.

3.Сервер реєстрації

Призначення: сервер реєстрації використовується для управління

обліковими записами користувачів та пристроїв, забезпечуючи автентифікацію та авторизацію доступу.

Функції:

-Реєстрація нових користувачів та пристроїв: Створює нові облікові записи.

-Управління обліковими записами: оновлює, видаляє та зберігає інформацію про користувачів.

-Автентифікація користувачів: перевіряє особу користувача перед наданням доступу до ресурсів.

4.Комутатор

Призначення: комутатор (Switch) використовується для з'єднання різних пристроїв у локальній мережі (LAN) і управління потоком даних між ними.

Функції:

-Перемикання пакетів даних: Передає дані між різними пристроями в мережі.

-Зменшення колізій у мережі: забезпечує ефективну передачу даних, мінімізуючи конфлікти.

-Підвищення пропускної здатності мережі: оптимізує використання мережевих ресурсів.

5.Хмарний провайдер

Призначення: забезпечує з'єднання між внутрішніми серверами та зовнішньою мережею (Інтернетом).

Функції:

-Маршрутизація трафіку: Перенаправляє трафік між внутрішніми серверами та Інтернетом.

-Забезпечення безпеки: Фільтрує трафік для захисту від зовнішніх загроз.

Склад компанії

1.ПК1 та ПК2

Призначення: Робочі комп'ютери, що використовуються співробітниками для виконання щоденних завдань.

Функції:

-Виконання офісних завдань: Робота з документами, електронною поштою та іншими офісними програмами.

-Доступ до корпоративних ресурсів: Підключення до внутрішніх серверів та баз даних.

-Використання мережевих сервісів: Доступ до Інтернету та інших мережевих ресурсів.

2.DNS сервер

Призначення: Виконує ті ж функції, що й DNS сервер у постачальника хмарних послуг, але використовується для внутрішніх потреб компанії.

Функції:

-Розв'язання імен у локальній мережі: Перетворює доменні імена внутрішніх ресурсів на IP-адреси.

-Кешування локальних DNS-записів: Зберігає результати попередніх запитів для швидшого доступу до внутрішніх ресурсів.

-Маршрутизація запитів до зовнішніх DNS серверів: Передає запити до зовнішніх DNS серверів, якщо запитуваний ресурс не знаходиться у внутрішній мережі.

3.Комутатор

Призначення: З'єднує всі пристрої на складі, забезпечуючи локальну мережу.

Функції:

-Перемикання пакетів даних: Оптимізує маршрутизацію даних між пристроями всередині локальної мережі.

-Управління трафіком: Забезпечує ефективне використання мережевих ресурсів, мінімізуючи затримки та колізії.

-Забезпечення ефективної роботи мережі: Допомагає утримувати стабільне та швидке з'єднання між усіма пристроями в мережі.

4.Маршрутизатор складу

Призначення: Забезпечує з'єднання локальної мережі складу з зовнішньою

мережею через хмарного провайдера.

Функції:

-Маршрутизація пакетів даних: Направляє трафік між локальною мережею складу та зовнішньою мережею.

-Управління трафіком: Оптимізує потоки даних для забезпечення максимальної продуктивності.

-Забезпечення безпеки: Фільтрує трафік для захисту від зовнішніх загроз та несанкціонованого доступу.

5.Модем

Призначення: Забезпечує з'єднання з Інтернетом через хмару.

Функції:

-Модуляція і демодуляція сигналу: Перетворює цифрові сигнали з комп'ютера на аналогові для передавання через телефонні або кабельні лінії, та навпаки.

6.Ноутбук

Призначення: Мобільний пристрій для доступу до мережевих ресурсів.

Функції:

-Виконання офісних завдань: Робота з документами, презентаціями, електронною поштою тощо.

-Доступ до корпоративних ресурсів: Підключення до внутрішніх серверів та баз даних, використання корпоративних додатків.

-Використання мережевих сервісів: Доступ до Інтернету, корпоративних VPN, внутрішніх та зовнішніх ресурсів.

Зовнішня мережа

1.Зовнішній ПК

Призначення: Комп'ютер, що знаходиться поза межами корпоративної мережі, але може підключатися до неї через Інтернет.

Функції:

-Доступ до зовнішніх ресурсів: Використовується для доступу до Інтернету та інших зовнішніх сервісів.

-Віддалена робота: Може підключатися до корпоративної мережі через VPN для виконання робочих завдань.

-Обмін даними: Може обмінюватися даними з іншими комп'ютерами та серверами через Інтернет.

2.Маршрутизатор

Призначення: Забезпечує з'єднання між зовнішніми комп'ютерами та Інтернетом.

Функції:

-Маршрутизація трафіку: Направляє дані між зовнішніми комп'ютерами та Інтернетом.

-Управління з'єднаннями: Контролює розподіл мережевих ресурсів та забезпечує якість обслуговування для різних типів трафіку.

-Забезпечення безпеки: Може мати вбудовані функції фільтрації та захисту від атак.

3.Комутатор

Призначення: З'єднує пристрої у локальній мережі (LAN), забезпечуючи комунікацію між ними.

Функції:

-Перемикання пакетів даних: Передає дані між пристроями в локальній мережі.

-Зменшення колізій: Оптимізує передачу даних, зменшуючи кількість конфліктів у мережі.

-Підвищення продуктивності мережі: Забезпечує високу швидкість передачі даних між пристроями.

Взаємодія між всіма компонентами в системі наступна:

Постачальник хмарних послуг надає різні сервіси, такі як DNS, CSP та сервер реєстрації, для забезпечення функціонування корпоративної мережі та доступу до зовнішніх ресурсів.

Склад компанії використовує внутрішній DNS сервер для обробки локальних запитів та забезпечує з'єднання з Інтернетом через модем і хмару.

Зовнішня мережа забезпечує доступ до Інтернету для зовнішніх ПК та їх взаємодію з корпоративними ресурсами через VPN.

Комутатори і маршрутизатори у всіх частинах мережі забезпечують ефективну передачу даних, управління трафіком та безпеку.

Ця система забезпечує надійний зв'язок між внутрішньою мережею компанії, хмарними сервісами та зовнішніми ресурсами, забезпечуючи при цьому безпеку даних та ефективне управління ресурсами.

Таким чином, ця IoT-мережа є складною системою, яка поєднує різні компоненти через різні типи з'єднань для забезпечення ефективної роботи та взаємодії між різними частинами мережі.

2.2 Аналіз ризиків безпеки для IoT-мережі

Аналіз безпеки для поданої IoT-мережі включає в себе ідентифікацію можливих ризиків, вразливостей та загроз для кожного сегменту мережі.

1.Постачальник хмарних послуг:

DNS сервер, CSP сервер, Сервер реєстрації: можливі ризики включають атаки типу "відмова в обслуговуванні" (DoS), крадіжку даних, зловмисне програмне забезпечення, несанкціонований доступ, а також уразливості в програмному забезпеченні серверів.

Комутатор: Вразливість до фізичних атак, несанкціонований доступ до управління комутатором, злом через незахищені порти.

Хмарний провайдер: Ризики пов’язані з безпекою хмарної інфраструктури, включаючи викрадення даних, атаки на інтерфейси API, внутрішні загрози (недобросовісні працівники), злом хмарної платформи.

2.Склад компанії:

ПК1, ПК2, DNS сервер: Небезпека від фішинг-атак, вірусів, шпигунських програм, несанкціонованого доступу до конфіденційної інформації, а також атаки на операційну систему та прикладне програмне забезпечення.

Комутатор: Вразливість до фізичних атак, перехоплення даних,

несанкціоноване підключення та управління.

Маршрутизатор складу: Можливість віддаленого злому, атаки на прошивку, неправильна конфігурація безпеки, перехоплення даних, несанкціоноване управління.

Модем: Ризики несанкціонованого доступу, злом через відкриті порти, атаки на конфігурацію.

Ноутбук: Загрози пов’язані з фізичною крадіжкою, фішинг-атаки, віруси та інше шкідливе ПЗ, незахищені бездротові підключення.

3.Зовнішня мережа:

Зовнішній ПК: Вразливий до віддалених атак, шкідливого ПЗ, крадіжки даних, фішинг-атак, несанкціонованого доступу до внутрішніх мереж.

Комутатор: Ризики фізичних атак, несанкціонованого доступу, перехоплення даних.

4.Загальні ризики для всієї мережі:

Відсутність шифрування: Перехоплення даних під час їх передачі через незашифровані канали зв’язку.

Мережеві атаки: Атаки типу «людина посередині» (MITM), DDoS-атаки, мережеве сканування, злом маршрутизаторів і комутаторів.

Відсутність актуальних оновлень ПЗ: Вразливості через застарілі версії програмного забезпечення.

Неправильне налаштування: Неправильні конфігурації безпеки на мережевих пристроях та серверах.

Внутрішні загрози: Недобросовісні працівники або зловмисники, що мають фізичний доступ до мережевих пристроїв.

Кожен з цих ризиків може призвести до серйозних наслідків, таких як втрата даних, фінансові втрати, порушення норм безпеки та конфіденційності, а також зниження репутації компанії.

2.3 Рекомендації для підвищення рівня безпеки IoT-мережі

Для підвищення рівня безпеки наведеної IoT-мережі, можна застосувати такі рекомендації:

1. Постачальник хмарних послуг:

DNS сервер, CSP сервер, Сервер реєстрації:

Оновлення та патчі: регулярне оновлення програмного забезпечення та операційні системи є дуже важливим моментом безпеки.

Моніторинг та логування: впровадження системи моніторингу та ведення логів для відстеження аномальної активності.

Файрволи та IDS/IPS: використання мережеві файрволи та системи виявлення/запобігання вторгнень (IDS/IPS) для захисту від мережевих атак.

Шифрування: використання шифрування для передачі даних між серверами та зовнішніми клієнтами.

Комутатор:

Контроль доступу: обмеження фізичного доступ до комутатора та налаштування аутентифікації для управління.

Сегментація мережі: використання VLAN для розділення трафіку і зниження ризику перехоплення даних.

Хмарний провайдер:

Безпечні API: Забезпечення використання безпечних API та обмеження доступу до них.

Моніторинг та аудит: використання інструментів моніторингу для відстеження активності у хмарній інфраструктурі.

2. Склад компанії:

ПК1, ПК2, DNS сервер:

Антивірус та антивірусні програми: встановлення і регулярне оновлення антивірусного програмного забезпечення.

Безпечна конфігурація: важливо переконатися, що всі пристрої налаштовані згідно з найкращими практиками безпеки.

Регулярне резервне копіювання: потрібно запровадити регулярні резервні копії важливих даних, аби не втратити їх.

Комутатор:

Контроль доступу: використання аутентифікації для доступу до комутатора та введення логування.

Маршрутизатор складу:

Оновлення прошивки: регулярне оновлення прошивки маршрутизатора.

Безпечне налаштування: вимкнення невикористовуваних сервіси та закривання невикористовуваних портів.

Використання VPN: використання VPN для захисту трафіку між складом та хмарою.

Модем:

Захист конфігурації: захист конфігурації модема паролями та регулярне їх змінення.

Моніторинг: використання інструментів моніторингу для відстеження активності модема.

Ноутбук:

Шифрування даних: використання шифрування дисків для захисту даних на ноутбуці.

Безпечне підключення: важливо перекотись, що ноутбук підключається до мережі через захищені канали (VPN).

3. Зовнішня мережа:

Зовнішній ПК:

Антивірус та безпека: потрібно встановлювати антивірусне програмне забезпечення та налаштувати регулярне оновлення.

Обмеження доступу: обмежити доступ до внутрішніх ресурсів компанії через зовнішній ПК.

Маршрутизатор:

Оновлення прошивки: регулярно оновлювати прошивку маршрутизатора.

Налаштування безпеки: потрібно переконатись, що маршрутизатор

налаштований відповідно до кращих практик безпеки, включаючи використання складних паролів, вимкнення незахищених сервісів, та закриття невикористовуваних портів.

VPN: налаштування VPN для захищеного з'єднання з зовнішніми користувачами.

Моніторинг трафіку: використання системи моніторингу трафіку для виявлення підозрілої активності та потенційних загроз.

Файрвол: впровадження файрвол для контролю вхідного та вихідного трафіку.

Комутатор:

Фізична безпека: захист комутатора від несанкціонованого фізичного доступу.

Безпека портів: налаштування безпеку портів (наприклад, Port Security) для запобігання несанкціонованого підключення.

4. Загальні рекомендації:

Шифрування: використання шифрування для всіх критичних з'єднань і даних.

Мережеві політики безпеки: впровадження та дотримання політик безпеки мережі, включаючи управління доступом, аудит та реагування на інциденти.

Навчання персоналу: регулярне навчання працівників щодо кібербезпеки, включаючи розпізнавання фішинг-атак та дотримання кращих практик безпеки.

Аудити безпеки: проводження регулярних аудитів безпеки для виявлення та усунення вразливостей у мережі.

Багатофакторна аутентифікація (MFA): використання MFA для доступу до критичних систем і даних.

Застосування цих рекомендацій допоможе значно підвищити рівень безпеки IoT-мережі та зменшити ризики кібератак і витоку даних.

Висновки до розділу 2

Після ретельного аналізу структури та потенційних загроз Інтернету речей (IoT) стає очевидним, що безпека цього типу мережі вимагає комплексного підходу та надзвичайної уважності до деталей. Наведена IoT-мережа складається з трьох основних секцій: постачальника хмарних послуг, складу компанії та зовнішньої мережі, кожна з яких має свої особливості та потенційні загрози.

У секції постачальника хмарних послуг, основними загрозами є атаки на DNS сервер, крадіжка конфіденційної інформації через CSP сервер та можливість злому сервера реєстрації. Недостатня безпека на цьому рівні може призвести до серйозних проблем з безпекою всієї мережі.

У складі компанії, варто враховувати загрози від зловмисних програм, фішингу, атак типу DoS та несанкціонованого доступу до пристроїв. Недбалість у забезпеченні безпеки на цьому рівні може призвести до проникнення зловмисників у внутрішні мережеві ресурси та крадіжки конфіденційної інформації.

На зовнішній мережі загрози можуть бути пов'язані з зловмисними програмами, атаками на підключеність та недостатньою фізичною безпекою пристроїв. Зловмисники можуть використовувати цей шлях для проникнення у мережу та отримання доступу до конфіденційної інформації.

Для запобігання цим загрозам та мінімізації можливих наслідків в разі кібератаки необхідно вжити ряд заходів безпеки. Зокрема, рекомендації включають оновлення програмного забезпечення, впровадження політик безпеки, встановлення моніторингу та застосування шифрування. Такі заходи можуть стати важливими стратегіями для захисту мережі від потенційних загроз.

Безпека IoT-мережі є невід'ємною частиною її успішного функціонування. Лише комплексний підхід до захисту, систематичне впровадження рекомендацій та постійний моніторинг можуть забезпечити надійність та захищеність цієї мережі в сучасному кіберпросторі. Недбалість у забезпеченні безпеки може призвести до серйозних проблем, включаючи втрату конфіденційності,

порушення норм безпеки та фінансові втрати.

Отже, ретельний аналіз загроз та застосування відповідних заходів безпеки є вирішально важливими для забезпечення стійкості та надійності IoT-мережі. Надійний захист мережі вимагає поєднання технологічних рішень, які міцно вбудовуються в архітектуру мережі, з ефективними політиками та процедурами безпеки, які дотримуються на всіх рівнях організації. Досягнення цієї мети вимагає співпраці між IT-фахівцями, кібербезпековими експертами та керівництвом компанії.

3 ПОБУДОВА ЗАХИЩЕНОЇ IoT МЕРЕЖІ

3.1 Розробка моделі мережі в середовищі PT

Першим кроком буде встановлення базової інфраструктури

Додавання пристроїв:

Згідно Рис.2.1. додаємо три маршрутизатори (1941), три комутатори (2960-24TT), кабельний модем (Cable Modem-PT), хмару (Cloud-PT), три сервери (Server-PT) для CSP DNS, CSP, та реєстрації у секторі постачальника хмарних послуг, та сервер (Server-PT) для DNS у складі компанії. Також маємо додати два ПК (PC-PT) для офісу складу, ноутбук (Laptop-PT), зовнішній ПК (PC-PT External). Всі обранні компоненти проілюстровані на Рис.3.1.

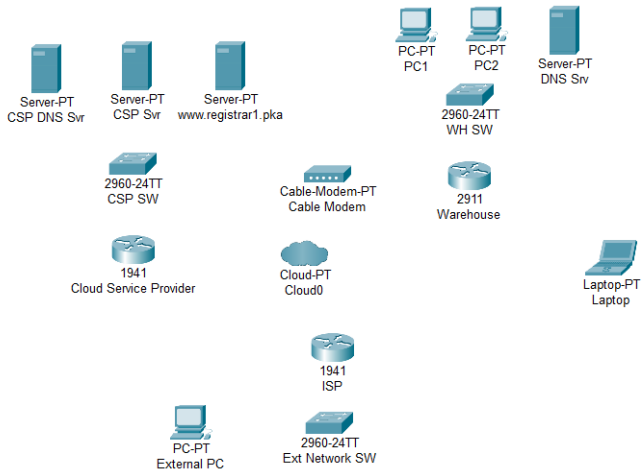

Рисунок 3.1 – Встановлення базової інфраструктури

Задля забезпечення фізичної безпеки пристроїв в офісі нашої компанії, додамо датчики, камери, світильники, контролери і т.д. для IoT частини мережі, Нам знадобиться ще один комутатор(2960-24TT), шлюз(DLC100), сервер SBC (SBC-PT SBC), він же центральний контролер, що під'єднується до інших пристроїв і управляє ними, направлене світло (Light), руху(Motion Detector), спотикання(Trip Sensor), веб-камеру(Webcam) та перемикач(Rocker Switch).

Доданні пристрої зображенні на Рис.3.2.

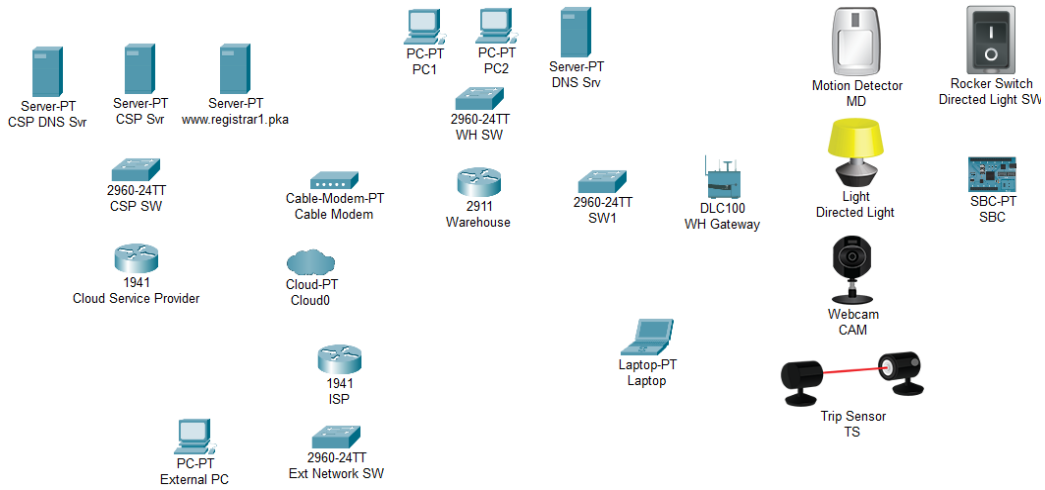

Рисунок 3.2 – Модель IoT мережі з урахуванням елементів для фізичного захисту офісу складу

З'єднання пристроїв:

Використовуємо Ethernet кабелі для з'єднання серверів, комутаторів та ПК, coaxial кабель для з'єднання кабельного модему з хмарою, серійні з'єднання (Serial DTE) для з'єднання маршрутизаторів, та IoT Custom Cable, для підключення контролеру до камери, направленого світла та перемикача направленого світла. (Рис.3.3)

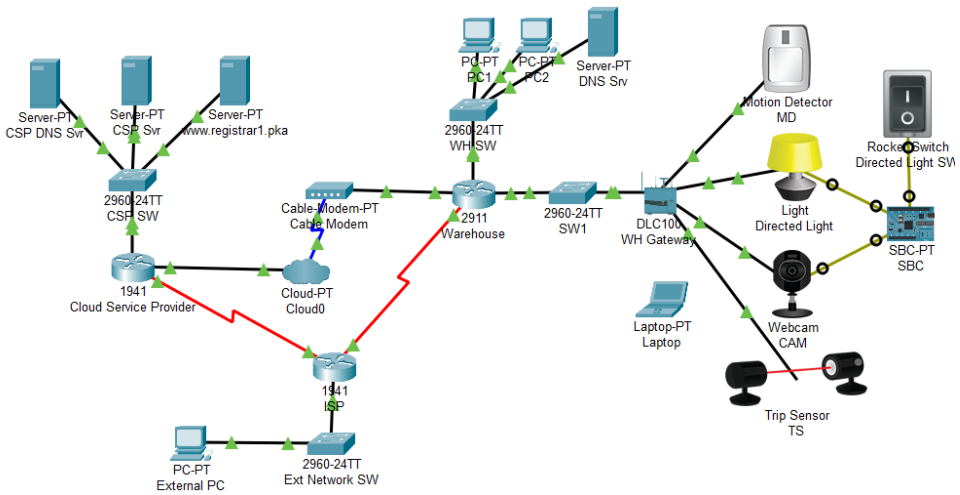

Рисунок 3.3 – Модель IoT мережі з з’днаними елементами мережі

Наступним кроком налаштуємо IP адреса.

IP-адрес на маршрутизаторах та серверах:

Встановимо IP-адреси для CSP DNS сервера, CSP сервера та реєстраційного сервера: 209.165.201.1, 209.165.201.3, 209.165.201.5, відповідно. Для ПК будуть наступні адреси:

PC1- 172.18.1.2

PC2- 172.18.1.3

External PC- 198.51.100.2

Для цього натискаємо на сервер, переходимо на вкладку Config , далі FastEthernet0, обираємо статичну адресу IPv4, та вносимо її.(Рис.3.4.)

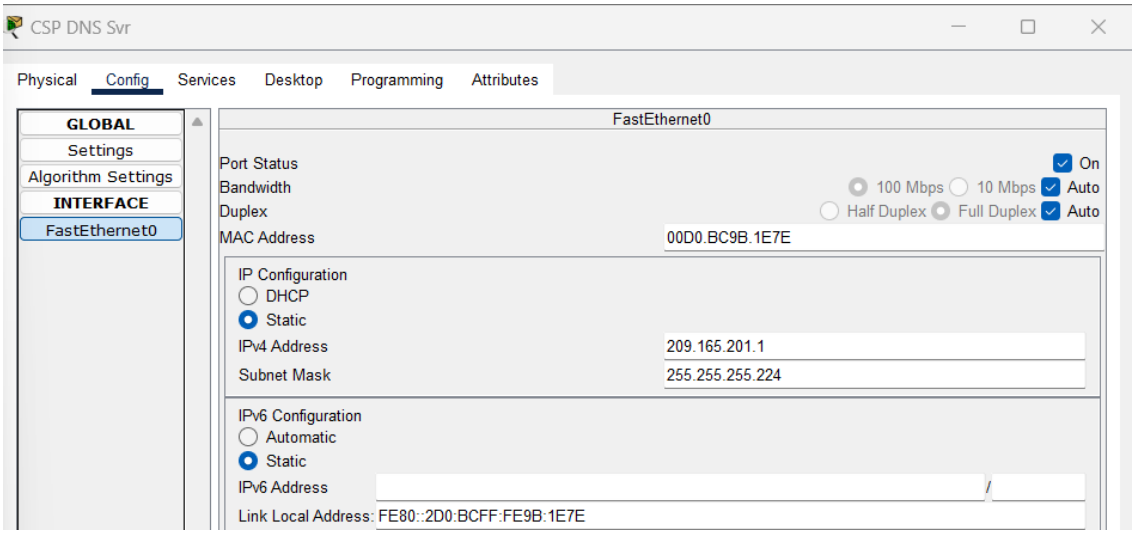

Рисунок 3.4 – Налаштування IP адреси серверу

Такі самі дії проводи і з іншими серверами та персональними комп’ютерами.

Переходимо до налаштування маршрутизації.

Маршрутизатор Cloud Service Provider (CSP):

Для налаштування інтерфейсів G0/0 та G0/1 ми натискаємо на наш маршрутизатор, на вкладці Config обираємо GigabitEthernet0/0 та вказуємо наступні дані:

IPv4 Address - 209.165.201.30

Subnet Mask - 255.255.255.224.

Процес налаштування приведений на Рис.3.5.

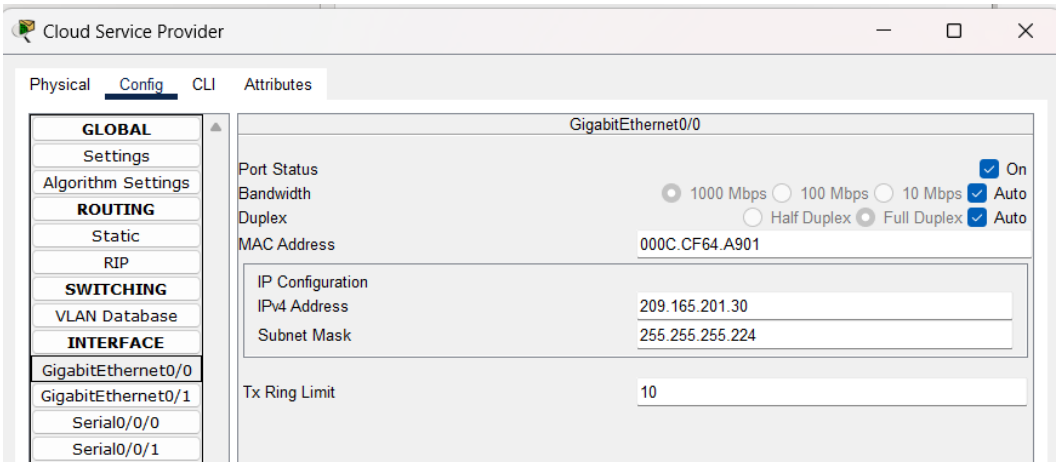

Рисунок 3.5 – Налаштування інтерфейсів маршрутизації

Для інтерфейсу G0/1 вказуємо дані:

IPv4 Address - 209.165.200.225

Subnet Mask - 255.255.255.252

Маршрутизатор на складі:

Для налаштування інтерфейсів G0/0, G0/1 та G0/2 маршрутизатору складу, використовуємо таку ж інструкцію, як для маршрутизатору CSP:

Для інтерфейсу G0/0:

IPv4 Address - 209.165.200.226

Subnet Mask - 255.255.255.252

Для інтерфейсу G0/1:

IPv4 Address - 172.18.1.254

Subnet Mask - 255.255.255.0

Для інтерфейсу G0/2:

IPv4 Address - 10.10.10.254

Subnet Mask - 255.255.255.0

ISP маршрутизатор:

Для ISP маршрутизатора треба налаштувати інтерфейси G0/0, S0/0/0 та S0/0/1:

Для інтерфейсу G0/0:

IPv4 Address - 198.51.100.254

Subnet Mask - 255.255.255.0

Для інтерфейсу S0/0/0:

IPv4 Address - 192.0.2.5

Subnet Mask - 255.255.255.252

Для інтерфейсу S0/0/1:

IPv4 Address - 192.0.2.1

Subnet Mask - 255.255.255.252

Налаштування маршрутизації:

Для маршрутизатора Cloud Service Provider (CSP) додамо статичний маршрут для мережі складу (10.10.10.0/24) через хмару. Для цього, натискаємо на маршрутизатор CSP та обираємо вкладинку CLI. В командному рядку набираємо наступну команду та натискаємо Enter (Рис. 3.6):

ip route 10.10.10.0 255.255.255.0 192.0.2.1.

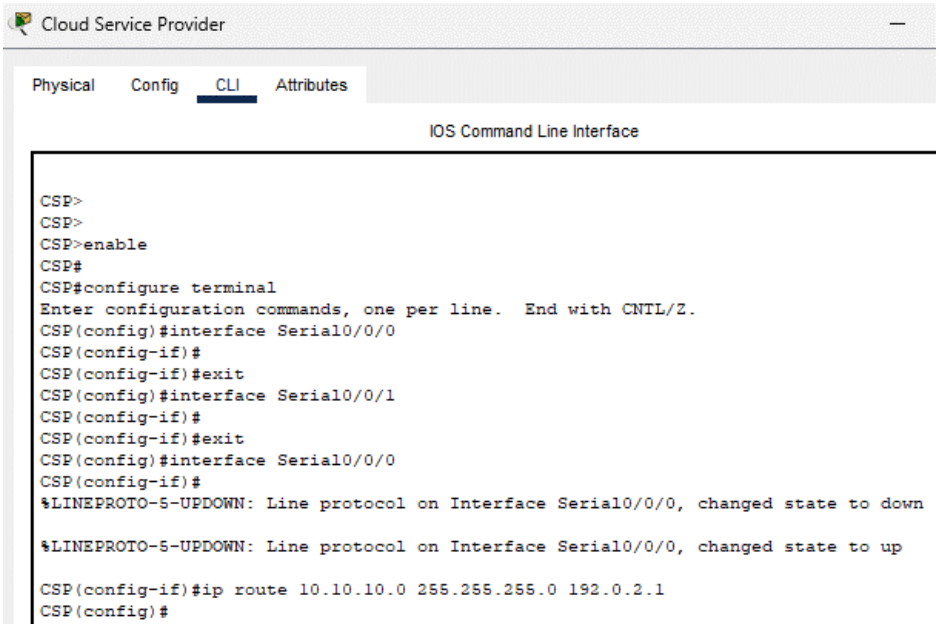

Рисунок 3.6 – додавання статичного маршруту для мережі складу (10.10.10.0/24) через хмару

Щоб зміни було збережено, необхідно виконати команду (Рис. 3.7):

do wr

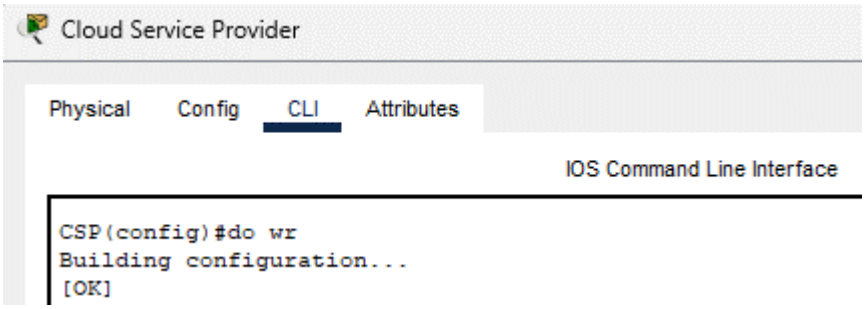

Рисунок 3.7 – Збереження внесених змін до статичного маршруту

Для перевірки внесених змін використовуємо команду (Рис 3.8):

do sh run

```
CSP(config)#do sh run
Building configuration...

Current configuration : 1115 bytes
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
ip route 209.165.200.224 255.255.255.224 209.165.200.226
ip route 10.10.10.0 255.255.255.0 192.0.2.1
```

Рисунок 3.8 – Перевірка внесених змін до статичного маршруту

Також додамо статичний маршрут для мережі офісу складу (172.18.1.0/24) через хмару:

ip route 172.18.1.0 255.255.255.0 192.0.2.1

Для маршрутизатора складу вказуємо статичний маршрут для мереж CSP (209.165.201.0/24) через хмару:

ip route 209.165.201.0 255.255.255.0 192.0.2.2

Також, для маршрутизатора ISP треба додати статичний маршрут для мережі CSP (209.165.201.0/24) через серійне з'єднання:

ip route 209.165.201.0 255.255.255.0 192.0.2.2

Далі треба налаштувати комутатори. Відкриваємо налаштування комутатора CSP SW, обираємо вкладку CLI, натискаємо Enter та послідовно вводимо наступні команди (Рис 3.9):

en //Перехід у привілейований EXEC режим

conf t //Перехід у глобальний режим конфігурації

interface range FastEthernet0/1 – 24 //Вибір діапазону інтерфейсів FastEthernet0/1 до FastEthernet0/24

switchport mode access //Встановлення режиму "access" для вибраних інтерфейсів

no shutdown //Активація вибраних інтерфейсів

exit //Вихід з режиму конфігурації інтерфейсу

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range FastEthernet0/1 - 24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#no shutdown
Switch(config-if-range)#exit
Switch(config)#
```

Рисунок 3.9 – Налаштування комутатора

Обов’язково треба зберегти зміни в налаштуванні комутатора (Рис 3.10):

copy running-config startup-config

```
Switch#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Рисунок 3.10 – Збереження змін після налаштування комутатора

Для перевірки внесених змін, використаємо команду (Рис 3.11):

show running-config

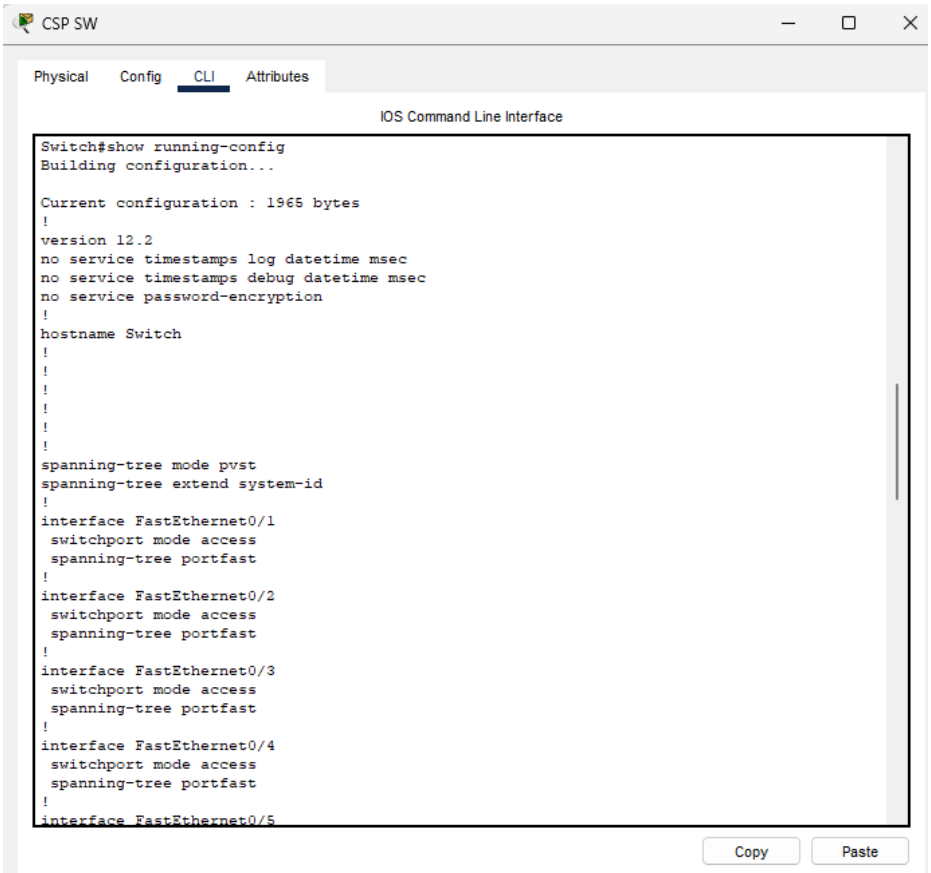

Рисунок 3.11 – Перевірка змінених налаштувань комутатора

Для комутатора складу (Warehouse SW), комутатора для офісу складу та комутатора для IoT пристроїв складу виконуємо ідентичні команди.

Для всіх пристроїв IoT вказуємо мережевий протокол DHCP для автоматичного отримання IP-адрес, шлюзів, масок та адрес DNS-серверів (Рис 3.12-3.13).

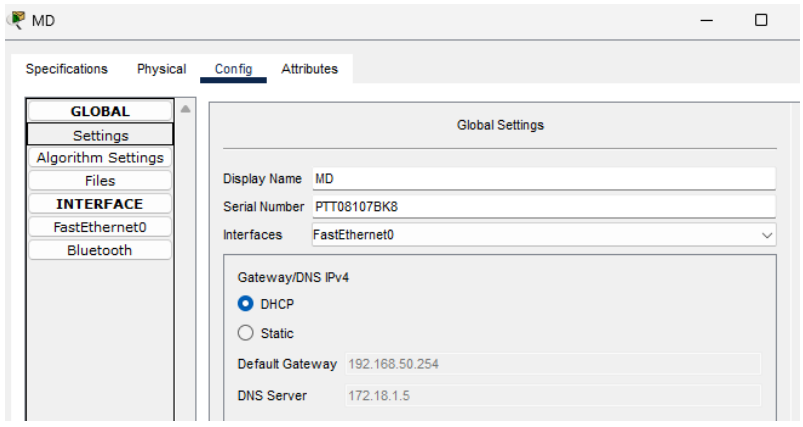

Рисунок 3.12 – Встановлення протоколу DHCP для отримання шлюзу та адреси DNS-серверу

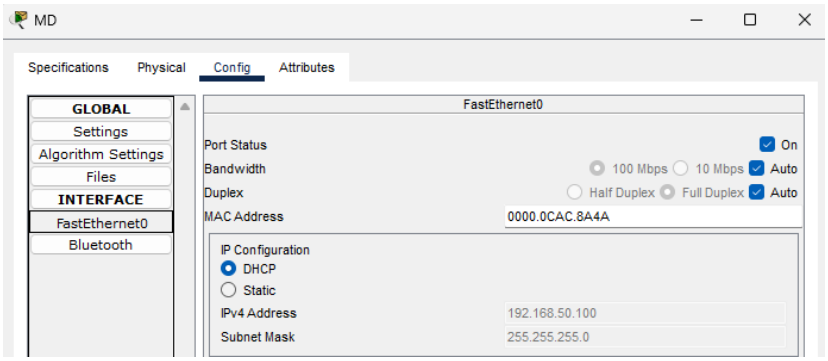

Рисунок 3.13 – Встановлення протоколу DHCP для отримання IP-адреси та маски

Для перевірки працездатності мережі, треба перевірити зв’язок між пристроями. Для цього натискаємо на PC1, обираємо меню Desktop, далі – Command Prompt. Вводимо наступну команду для перевірки зв’язку між PC1 та External PC (Рис 3.14):

ping 198.51.100.2

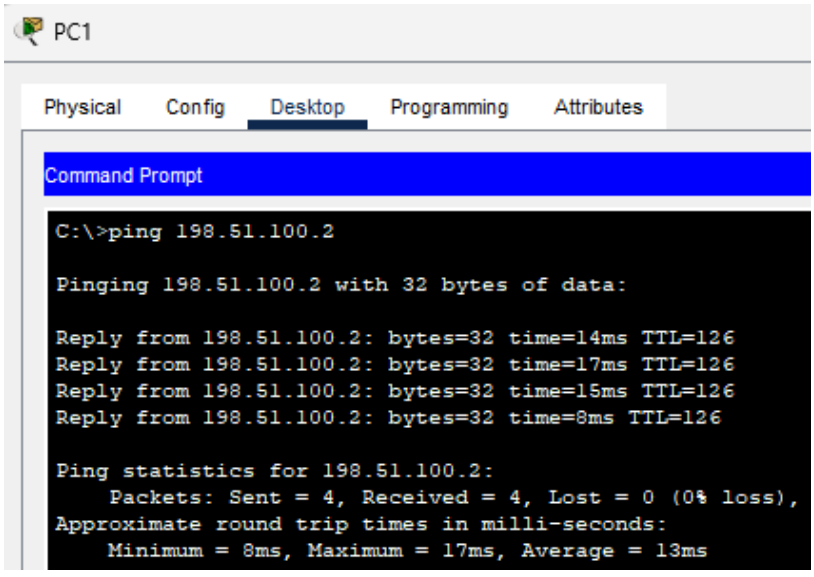

Рисунок 3.14 – Перевірка зв’язку між PC1 та External PC

На всіх пристроях, які було налаштовано, було використано команду copy running-config startup-config для збереження їх конфігурації.

3.2 Аналіз технологій захисту мережі

Сильні сторони IoT-мережі:

Розподіл мереж:

Мережа поділена на три зони: хмарний сервіс провайдера, зовнішня мережа та склад компанії. Це забезпечує сегментацію та ізоляцію, що підвищує безпеку, оскільки атаки не поширюються відразу по всій мережі.

Використання спеціальних каналів:

Лінії між різними зонами мережі використовують з’єднання через серії маршрутизаторів, що вказує на використання спеціальних каналів, які забезпечують шифрування трафіку та захист від прослуховування.

Контроль доступу:

Застосування комутаторів та маршрутизаторів дозволяє налаштовувати списки контролю доступу (ACL) для обмеження доступу до певних ресурсів на основі IP-адрес або інших параметрів.

Слабкі сторони IoT-мережі:

Відсутність явного захисту на IoT-пристроях:

Не використовуються додаткові механізми захисту для IoT-пристроїв, такі як брандмауери, механізми аутентифікації та авторизації.

Можливість компрометації пристроїв:

IoT-пристрої, такі як веб-камера, датчики руху та світло, можуть бути легко компрометовані, якщо вони не мають вбудованих засобів захисту. Якщо один пристрій буде зламано, це може дати зловмиснику доступ до всієї мережі.

Недостатній захист периферійних пристроїв:

Система керування світлом та інші сенсори можуть бути піддані фізичному втручанню, що може спричинити небажані зміни в мережі або порушення безпеки.

Залежність від хмарного сервісу:

Якщо хмарний сервіс провайдера буде зламаний або недоступний, це може вплинути на роботу всієї мережі. Мережа сильно залежить від зовнішніх

ресурсів, які можуть бути вразливими.

Відсутність явного механізму моніторингу:

Немає систем моніторингу безпеки або журнали аудиту, що могли б виявляти та реєструвати підозрілу активність в мережі.

Відсутність резервних каналів зв'язку:

В разі виходу з ладу основних каналів зв'язку (наприклад, між 1941 ISP та Cloud0), мережа може втратити зв’язок із хмарними сервісами, що може паралізувати роботу IoT-пристроїв.

Рекомендації:

Впровадження додаткових засобів захисту IoT-пристроїв:

Використання спеціалізованого ПЗ та апаратних рішень для захисту IoT-пристроїв від атак.

Сегментація та ізоляція критичних ресурсів:

Забезпечення додаткової сегментації мережі для ізоляції критичних пристроїв та ресурсів.

Резервні канали зв'язку:

Налаштування резервних каналів зв'язку для забезпечення безперервної роботи мережі в разі збоїв.

Моніторинг та управління подіями безпеки (SIEM):

Впровадження системи моніторингу безпеки для виявлення та реагування на підозрілу активність в реальному часі.

3.3 Налаштування моделі з елементами захисту

На цьому етапі перейдемо до налаштувань нашої моделі, що приведена на Рис.3.15.

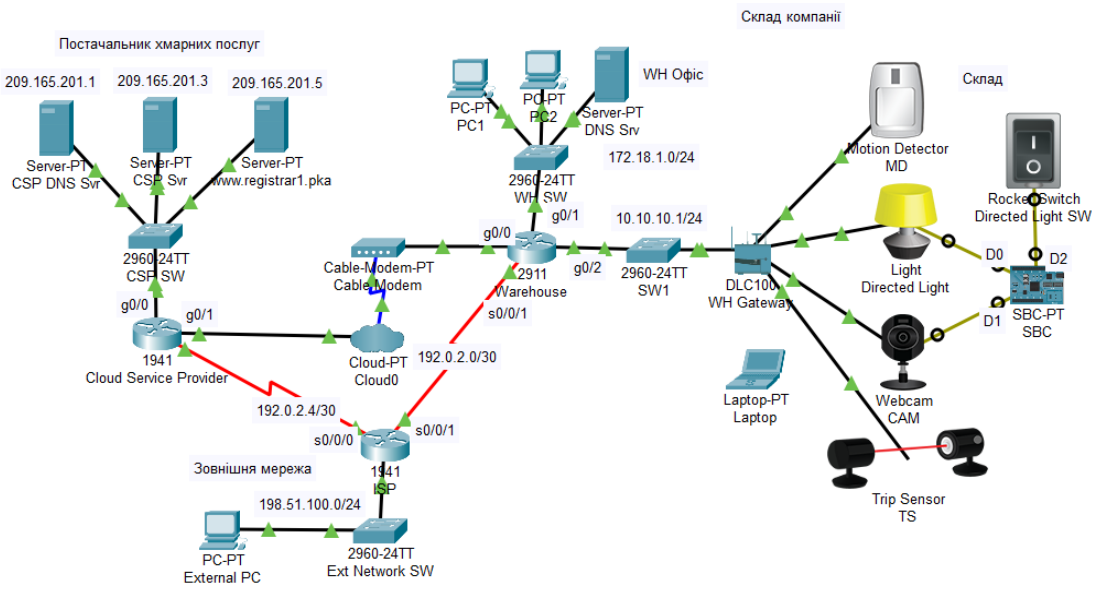

Рисунок 3.15 – Модель мережі з елементами захисту

Першим кроком буде реєстрація IoT-пристроїв на сервері реєстрації. Для цього спочатку додаємо уявного користувача до сервера www.registrar1.pka , обов'язково використовуючи надійний пароль.

Отже, у офісі WH , користуючись ПК відкриваємо вкладку Desktop, далі заходимо у веб-браузер і вводимо наше посилання та натискаємо Go, аби з'явилось вікно реєстрації, результат наших дій на Рис.3.16.

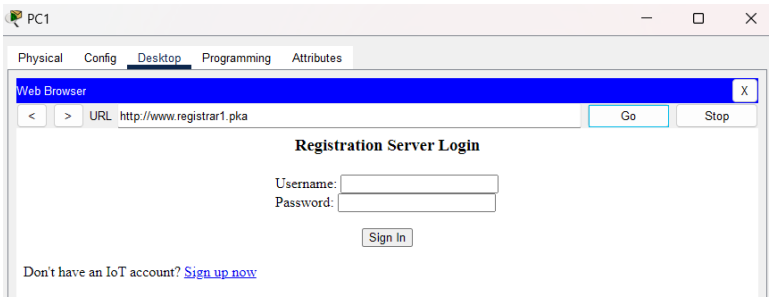

Рисунок 3.16 – Вікно реєстрації користувача

Натискаємо Sing up now та створюємо власний акаунт з надійним паролем, що буде включати в себе не менше 8 символів в комбінації різноманітних символів, цифр та великих літер, а саме ім'я PUDGE та пароль X45tr48Y!.

Далі реєструємо пристрої IoT, у межах нашого складу натискаємо на детектор руху, обираємо вкладку Config, в ній Remote Server у розділі сервера

IoT. Вводимо www.registrar1.pka як адресу сервера та натискаємо Connect. Після цього використовуємо данні створеного профілю нашого користувача. Виконанні дії зображенні на Рис.3.17.

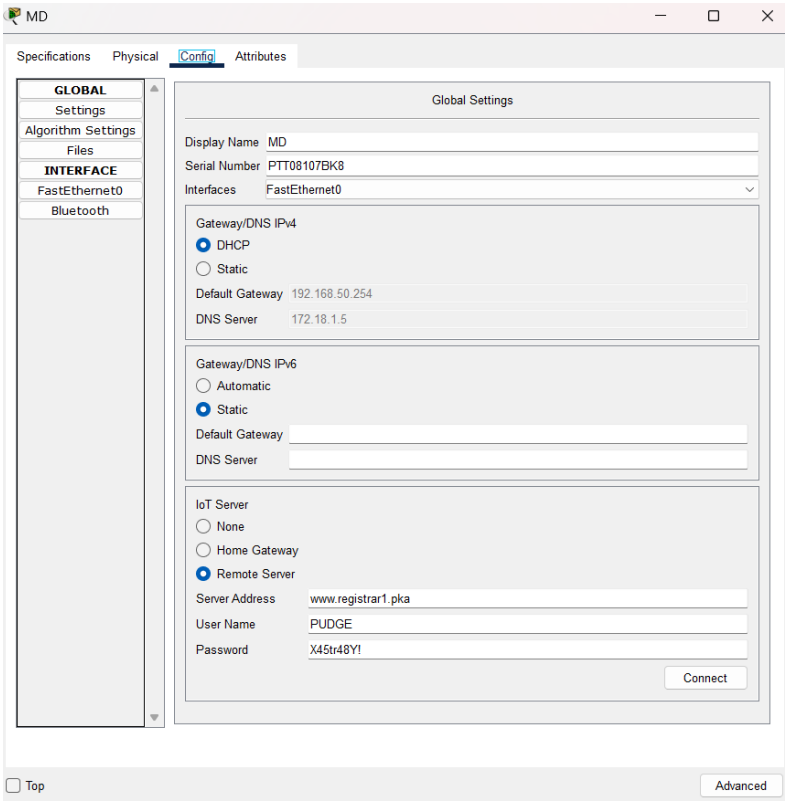

Рисунок 3.17 – Процес реєстрації детектору руху

В результаті наших дій ми повинні побачити детектор руху на сервері(Рис.3.18)

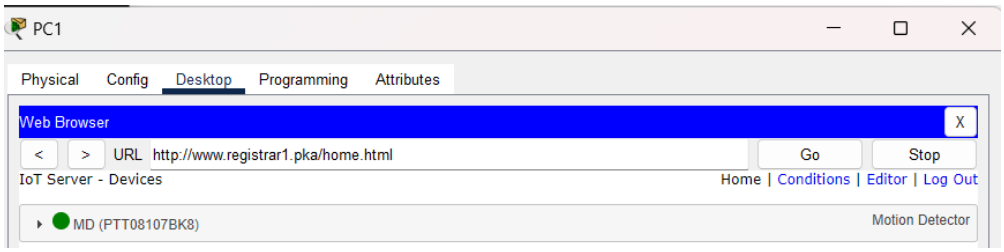

Рисунок 3.18 – Зареєстрований детектор руху на сервері реєстрації

По такій самій схемі будемо реєструвати датчик світла, веб-камеру та датчик відключення, в результаті чого вони також відобразяться на сервері

реєстрації.(Рис.3.19)

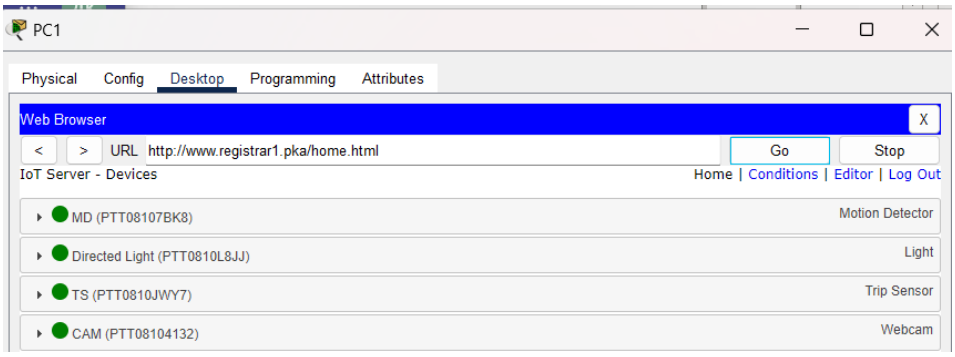

Рисунок 3.19 – Зареєстровані на сервері датчики

Надалі додамо умови на сервері реєстрації, щоб при активації датчика руху або датчика спотикання, спрямованнє світло та веб-камера були увімкненні. Аби це налаштувати ми входимо на сервер реєстрації та натискаємо Conditions додаючи три умови:

1. Якщо датчик руху буде в статусі «увімкненно», тоді наша камера та направлення світла теж повинні бути «увімкненні».(Рис.3.20)

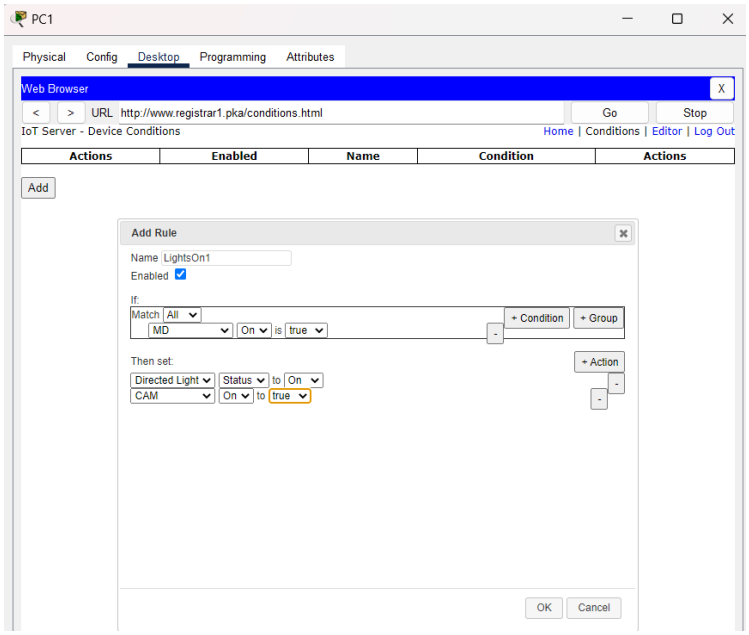

Рисунок 3.20 – Налаштування першої умови

2. Якщо у датчику спотикання статус «увімкненно», тоді стастус

направленного світла та камери теж «увімкненно».(Рис.3.21)

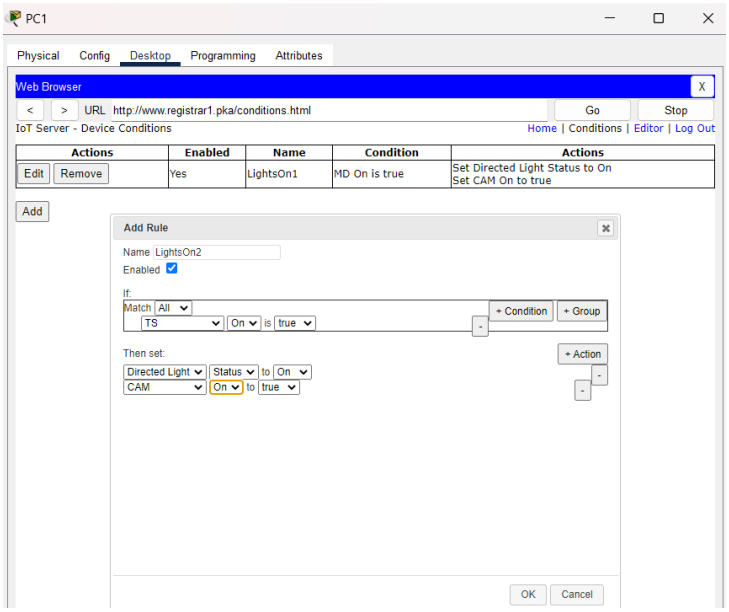

Рисунок 3.21 – Налаштування другої умови

3. Якщо статуси детектору руху «увімкненно» є хибними, та статус датчика спотикання «увімкнення» також хибним, то статус світла буде «вимкненно», а статус камери «увімкненно» є хибним. Рис.3.22.

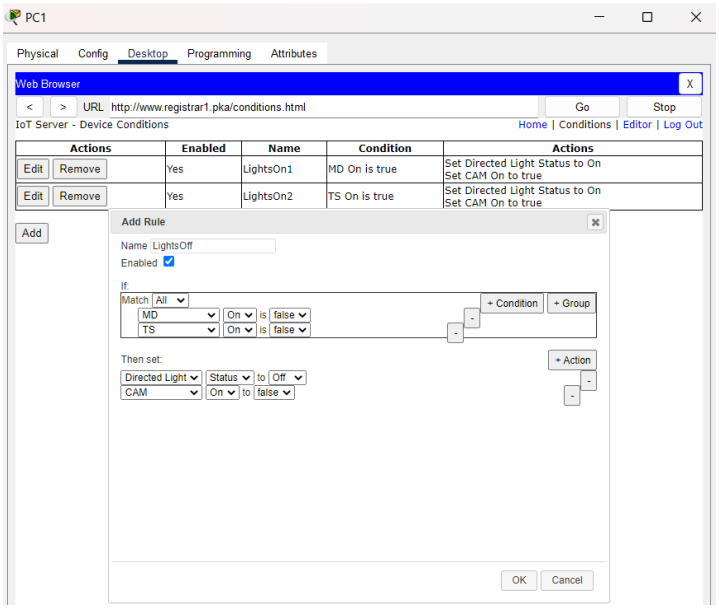

Рисунок 3.22 – Налаштування третьої умови

Наступним важливим кроком є налаштування на мережевих пристроях

надійної автентифікації. У межах нашого складу натискаємо на WH-шлюз, під вкладкою налаштувань, за допомогою опції Wireless встановлюємо SSID на WhGateway1, автентифікація на WPA2-PSK з паролем IoTWh001. Тип шифрування обираємо AES.(Рис.3.23)

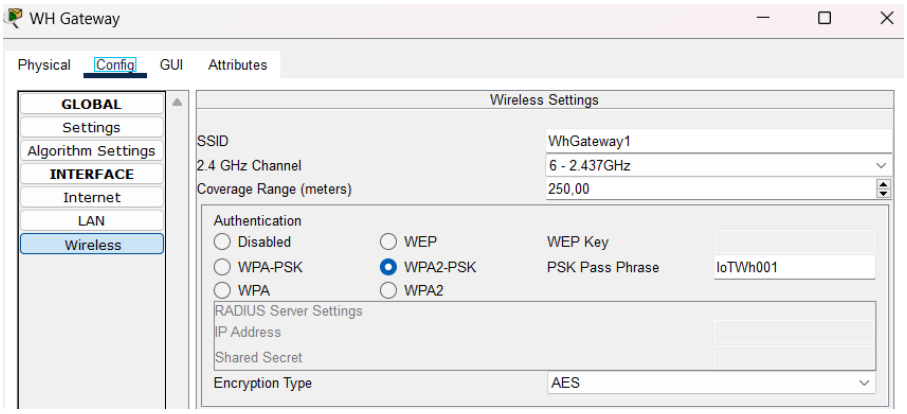

Рисунок 3.23 – Процес налаштування WH-шлюзу

Після цього переходимо до ноутбуку, під вкладкою налаштувань, за допомогою опції Wireless0, встановлюємо SSID на WhGateway1, автентифікацію на WPA2-PSK з паролем IoTWh001. Тип шифрування як AES.(Рис.3.24)

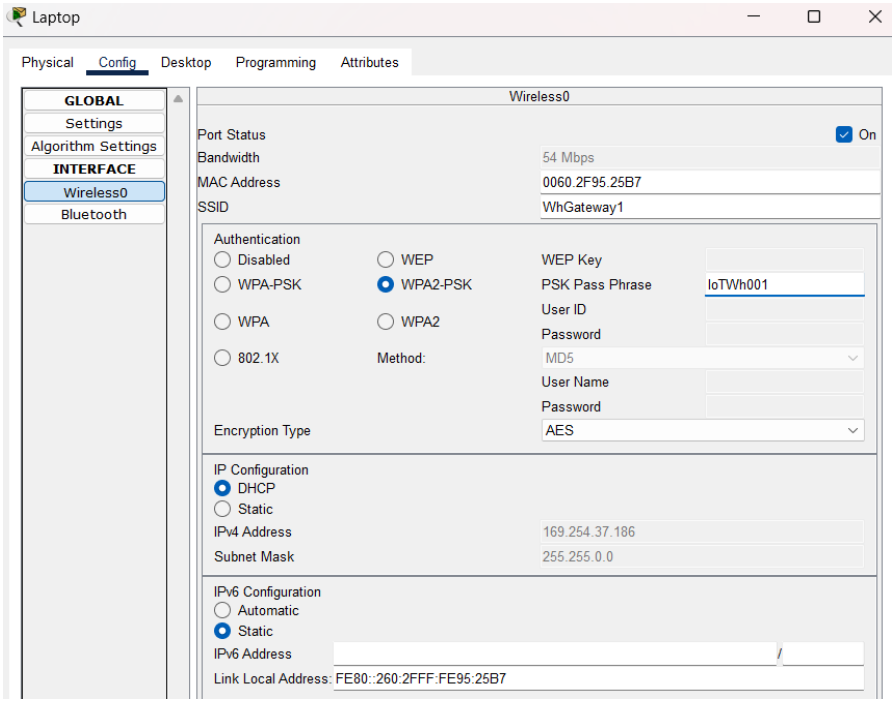

Рисунок 3.24 – Процес підключення ноутбуку до WH-шлюзу

В результаті наш ноутбук повинен успілшно підключитись до шлюзу.Рис.3.25.

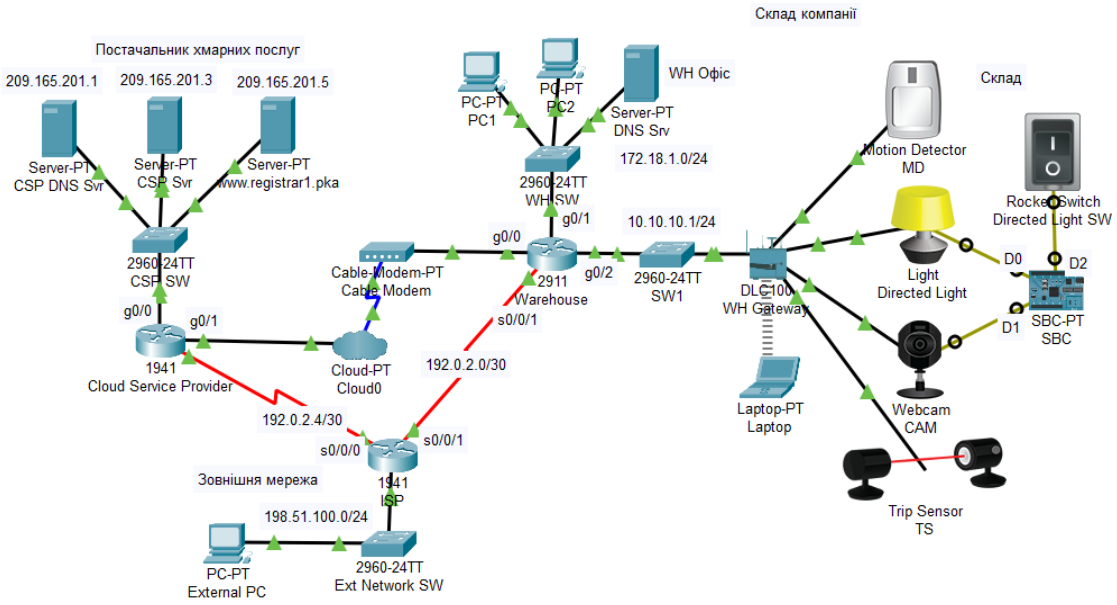

Рисунок 3.25 – Успішне підключення ноутбуку до WH-шлюзу

На складському маршрутизаторі зробимо банер для відображення попереджувального повідомлення про незаконний доступ. Хоча банерне повідомлення само по собі не є засобом безпеки, воно може діяти як стримуючий засіб для зловмисників. Зробимо зашифрований пароль для входу в режим Exec та налаштуємо локальний обліковий запис користувача для лінії консолі та віддаленого доступу.

Натискаємо на маршрутизатор складу 2911, в ньому обираємо CLI-вкладку, та вводимо наступні команди, наведені на Рис.3.26.

```
warehouse> enable
warehouse#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
warehouse(config)#banner login %Login with valid password%
warehouse(config)#banner motd %Authorized Access Only! Unauthorized access is subject to Federal
Prosecution.%
warehouse(config)#
```

Рисунок 3.26 – Команди для налаштування банеру

Налаштуємо безпечний пароль режиму Exec (Рис.3.27)

```
warehouse(config)#enable secret AbcWh001
warehouse(config)#exit
warehouse#
%SYS-5-CONFIG I: Configured from console by console
```

Рисунок 3.27 – Команди для налаштування безпечного паролю

Перейдемо до налаштування локального ім’я користувача для лінії консолі, та VTY.(Рис.3.28)

```
warehouse#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
warehouse(config)#username WhAdmin secret AbcLine001
warehouse(config)#line console 0
warehouse(config-line)#login local
warehouse(config-line)#exit
warehouse(config)#line vty 0 4
warehouse(config-line)#login local
warehouse(config-line)#end
warehouse#
%SYS-5-CONFIG_I: Configured from console by console

warehouse#
```

Рисунок 3.28 – Налаштування локального облікового запису користувача для лінії консолі та віддаленого доступу

Перейдємо до налаштування списку доступу для обмеження трафіку між пристроями IoT компанії та мережею постачальників хмарних сервісів, для цього на маршрутизаторі складу налаштуємо та застосуємо список доступу 10, щоб дозволити трафік тільки від DNS-сервера реєстраційного сервера для входу в мережу пристроїв IoT на склад компанії (Рис.3.29)

```
warehouse#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
warehouse(config)#access-list 10 permit host 172.18.1.5
warehouse(config)#access-list 10 permit host 209.165.201.5
warehouse(config)#interface g0/2
warehouse(config-if)#ip access-group 10 out
warehouse(config-if)#end
warehouse#
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 3.29 – Налаштування списку доступу 10

На маршрутизаторі провайдера хмарних сервісів установимо та застосуємо список доступу 110 для доступу до сервера реєстрації IoT-пристроїв лише зі складу нашої компанії (Рис.3.30)

```
CSP>enable
CSP#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CSP(config)#access-list 110 permit ip host 209.165.200.226 host 209.165.201.5
CSP(config)#access-list 110 deny ip any host 209.165.201.5
CSP(config)#access-list 110 permit ip any any
CSP(config)#interface g0/0
CSP(config-if)#ip access-group 110 out
CSP(config-if)#end
CSP#
%SYS-5-CONFIG_I: Configured from console by console
```

Рисунок 3.30 – Налаштування маршрутизатора хмарних сервісів

Останнім кроком є налаштування безпечної веб-комунікації на веб-сервері в мережі постачальників хмарних сервісів. Наша компанія використовує веб-сервери у постачальника хмарних послуг для частини своєї роботи, тож налаштуємо веб-сервер у хмарному сервісі провайдера, так , аби отримати доступ лише через HTTPS, для цього відкриваємо сервер CSP, та заходимо на вкладку Services, натискаємо на HTTP, та перевіряємо що HTTP вимкнено, а HTTPS увімкнено.(Рис.3.31)

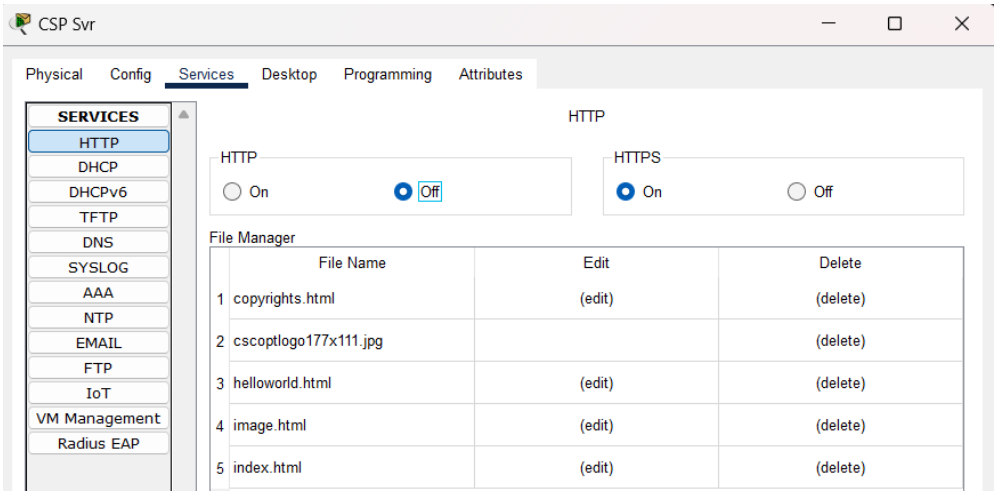

Рисунок 3.31 – Налаштування серверу CSP

3.4 Порівняння роботи IoT-мережі з захистом і без.

Настав час перевірити результати наших налаштувань і з’ясувати що змінилось, та навіщо.

Перше, що ми налаштовували у попередньому розділі, були IoT-пристрої для фізичного захисту. По-перше, сама наявність цих пристроїв може зупинити зловмисника на початкових етапах, коли він зрозуміє, наскільки ризики його виявлення зростуть. По-друге, окрім того факту, що ми їх додали, ми надали їм в налаштування умови, аби вони працювали не як окремі одиниці захисту, а як повноцінна система. Це корисно в тому плані, що навіть у ситуації, коли злочинець обійшов один із датчиків, є вірогідність спрацювання іншого, що по ланцюговій реакції спровокує повноцінну фіксацію злочину або зупинить його зовсім.

Перевіримо роботу наших датчиків до налаштувань умов і після. Для цього затискаємо клавішу Alt, паралельно проводимо курсором над датчиком руху та спотикання.(Рис.3.32-3.33)

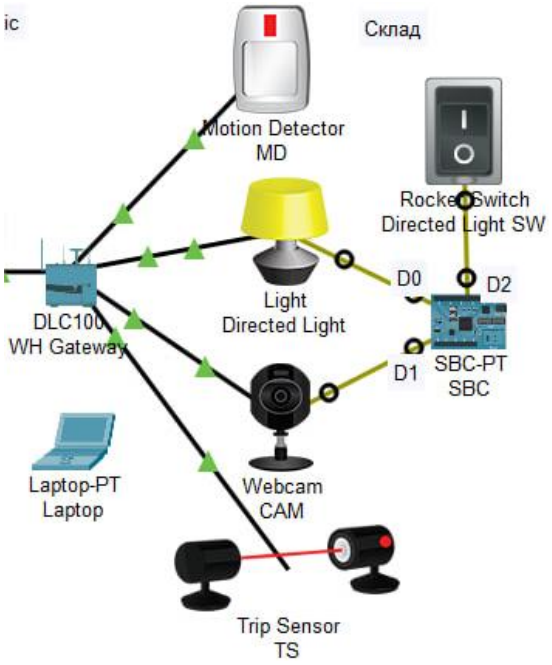

Рисунок 3.32 – Реагування датчиків без налаштованих умов

Хоча ми й зафіксували факт втручання, але, без налаштованих умов, не спрацьовує камера та спрямоване світло. З цього випливає, що зафіксувати

нашого зловмисника не вийде.

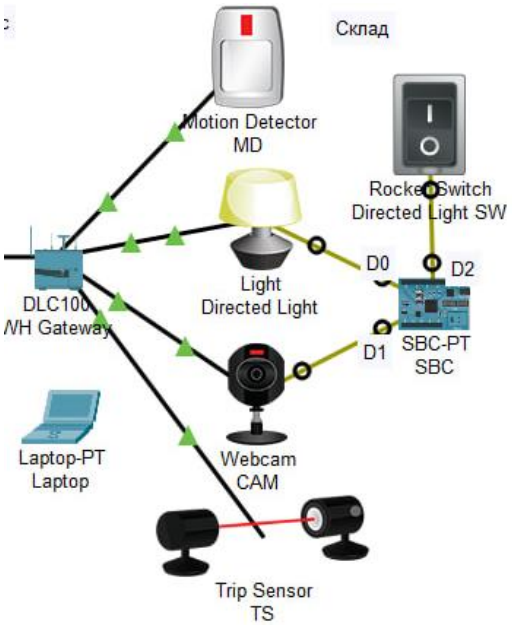

Рисунок 3.33 – Реагування датчиків при налаштованих умовах

При налаштованих умовах, ми бачимо, як вмикається запис камери та спрямоване світло. Завдяки цьому можливий крадій буде зафіксований. Може здатися, що раціональніше вести цілодобовий запис з камери, та не вимикати направлене світло, але це не зовсім економічно, та процес пошуку потрібного фрагменту запису буде забирати певний час, який краще не втрачати в подібній ситуації.

Другим етапом було налаштування надійної автентифікації на мережевих пристроях. Ми знову застосували психологічний момент, а саме зробили банерне повідомлення, що нагадує про відповідальність, яку понесе зловмисник за свої дії. Більш суттєве налаштування було встановлення паролю доступу, пам’ятаємо про правила для надійного паролю. Реагування системи наведено на Рис.3.34-3.35.

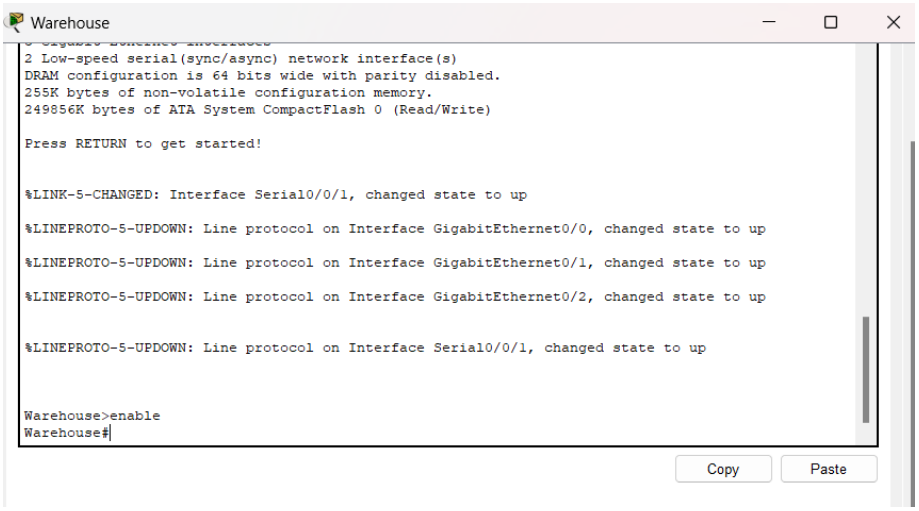

Рисунок 3.34 – Реагування системи до налаштувань

Спираючись на рисунок, бачимо, що кожна людина, яка має фізичний доступ до компонентів, може вносити свої зміни. Такий процес ніяк не в’яжеться з поняттям безпеки.

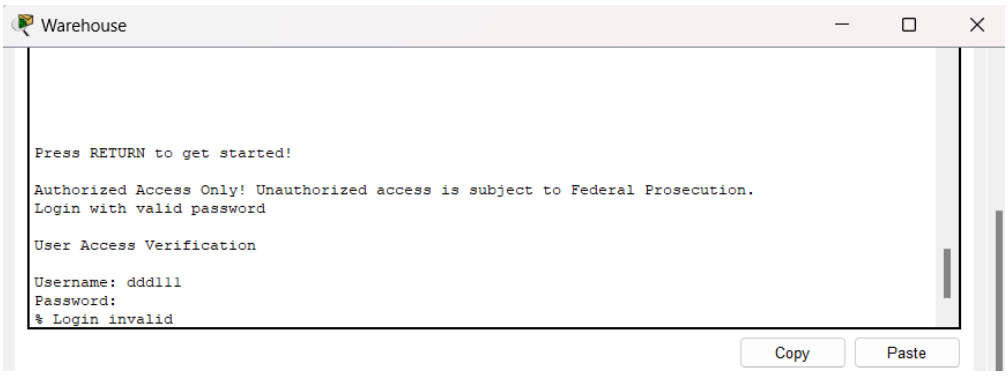

Рисунок 3.35 – Реагування системи після налаштувань

Тепер ми можемо бачити банерне сповіщення, про яке згадувалось раніше, а також, для початку роботи, система потребує логін і пароль, не допускаючи втручання без правильного введених даних.

Подібні налаштування є обов’язковими для будь-яких компонентів та систем. Окрім вилучення даних, хакери можуть переналаштувати пристрої таким чином, що ви або втратите доступ до них, або навіть не будете здогадуватись, скільки інформації перехоплюється кожну хвилину.

Не менш важливим кроком було налаштування списку доступу для

обмеження трафіку між пристроями IoT та мережею постачальників хмарних сервісів. Зловмисники лише зрадіють кількості доступних точок входу для своїх дій, тому варто надійніше розподіляти доступ до певних даних між пристроями.

До нашого втручання, ми могли переглядати сервіс реєстрації з будь-якого ПК. Зважаючи на те, що, через цей сервіс, можна переглянути список пристроїв, які забезпечують фізичний захист приміщення, надання публічного доступу до серверу реєстрації може бути небезпечним. Під час роботи ми надали доступ до серверу реєстрації лише ноутбуку, який може бути поза складом компанії, а ось на персональних комп'ютерах, які завжди на території компанії, ми цей доступ обмежили. Результати приведенні на Рис.3.36-3.38.

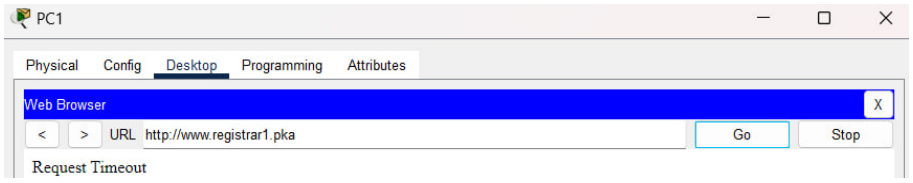

Рисунок 3.36 – Результат спроби підключення до серверу реєстрації з ПК1

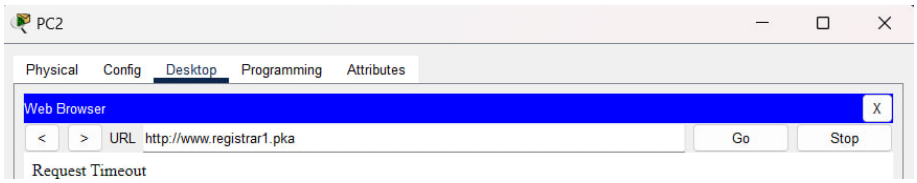

Рисунок 3.37 – Результат спроби підключення до серверу реєстрації з ПК2

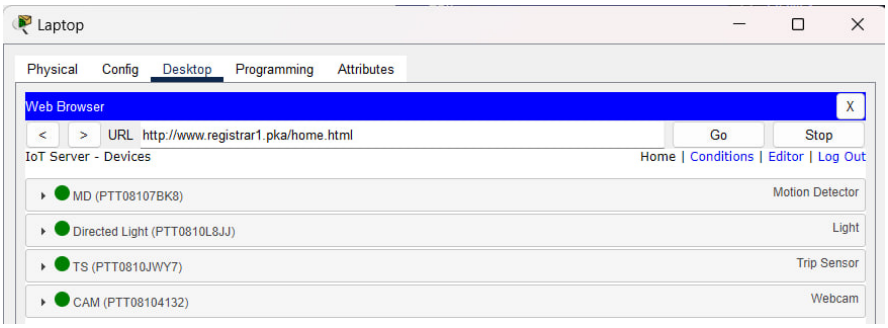

Рисунок 3.38 – Результат спроби підключення до серверу реєстрації з ноутбуку

Таким чином, ми можемо віддаленно спостерігати й переналаштовувати наші елементи захисту, та виключити момент стороннього втручання, як випадкового, так і навмисного.

Останне налаштування було пов’язанно з налаштуванням безпечної веб-комунікації на веб-сервері в мережі постачальників хмарних сервісів. Наразі, більшість людей розуміють, що протокол HTTPS є набагато безпечнішою та кращою версією протоколу HTTP. Але, для економії часу, грошей, або через незнання ризиків чи віру в перенавантаження систем, люди все ще нехтують моментом переходу до розширеного протоколу. Захищенність данних важлива протягом всього шляху, тому ми використали саме HTTPS протокол. Перевіримо, чи зможемо отримати данні, використовуючи HTTP без налаштувань. (Рис.3.39)

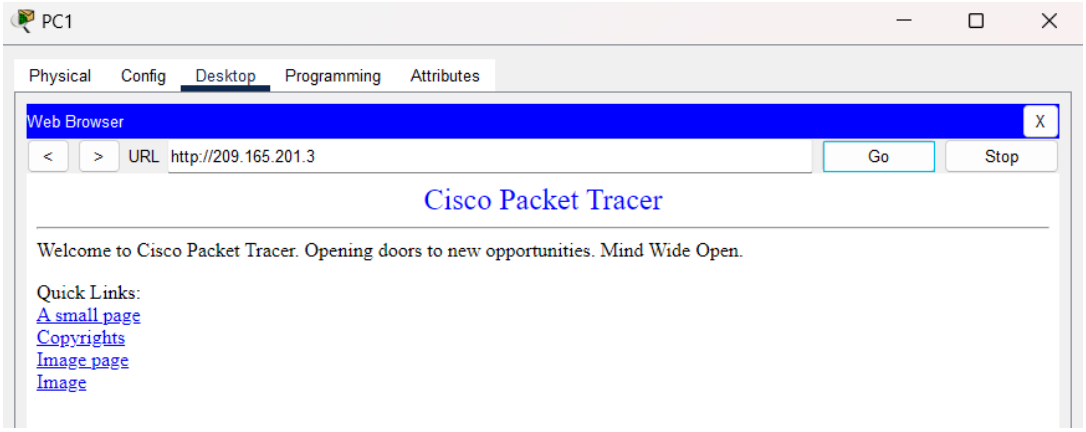

Рисунок 3.39 – Спроба доступу до веб-серверу через HTTP до налаштувань

Доступ ми отримали, але маємо розуміти, що дані протягом всього шляху були доступні для перехоплення та читання, що тягне за собою ризики витоку даних. Змінимо налаштування, та зробимо те саме.(Рис.3.40)

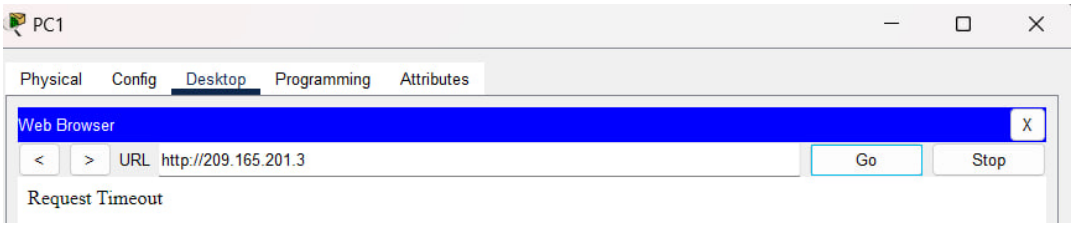

Рисунок 3.40 – Спроба доступу до веб-серверу через HTTP після налаштувань

Нам це не вдалося, бо такий запит є більш ризикованим, адже, наші дані можуть бути перехоплені та прочитані будь-якої миті в процесі їх відправлення чи отримання. Використаємо HTTPS.(Рис.3.41)

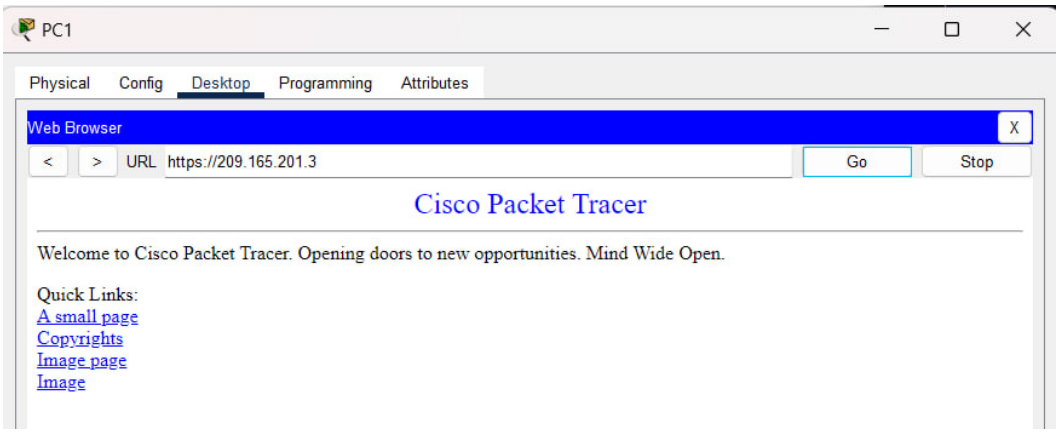

Рисунок 3.41 – Спроба доступу до веб-серверу через HTTPS після налаштувань

Ця спроба є вдалою, а головне безпечнішою.

Висновки до розділу 3

Кібербезпека вимагає всебічного підходу, що включає технологічні рішення, фізичні заходи та належне управління. Порівняння протоколів HTTP і HTTPS чітко показує важливість сучасних стандартів безпеки. HTTP передає дані у відкритому вигляді, роблячи їх легкодоступними для читання зловмисниками. Це призводить до перехоплення особистої інформації, паролів

та фінансових даних, а також до їх модифікації без відома користувачів. Натомість, HTTPS забезпечує шифрування переданих даних, захищаючи їх від перехоплення та змін. Використання цифрових сертифікатів у HTTPS також дозволяє перевіряти автентичність веб-сайтів, знижуючи ризик фішингових атак.

Фізична безпека є не менш важливою. Використання камер відеоспостереження, датчиків руху, спотикання та направленого світла значно підвищує рівень захисту об'єктів. Камери відеоспостереження не тільки відлякують потенційних зловмисників, але й дозволяють фіксувати та аналізувати події, що відбуваються в зоні їх дії. Датчики руху та спотикання автоматично реагують на підозрілу активність. Це забезпечує швидке реагування на потенційні загрози та мінімізує можливі збитки. Хитрощі, такі як попереджувальні банери, або муляжі камер, що будуть відволікати увагу від реальної веб-камери, також зменшать ризики.

Важливу роль також відіграють управління доступом та використання надійних паролів. Використання складних та унікальних паролів для кожного облікового запису значно ускладнює можливість їх злому. Впровадження двофакторної аутентифікації надає додатковий рівень захисту. Розподіл доступу, який включає надання прав доступу лише тим користувачам, які мають на це відповідні повноваження, також є ключовим елементом захисту. Це дозволяє обмежити доступ до конфіденційної інформації та критичних систем, знижуючи ризик внутрішніх загроз.

Поєднання цих підходів створює надійну систему кібербезпеки. Такий комплексний підхід забезпечує захист від різноманітних загроз, включаючи зовнішні атаки, внутрішні ризики та несанкціонований доступ. У сучасному світі, де кіберзагрози стають все більш витонченими, інтеграція цих заходів є критично важливою для захисту даних як організацій, так й індивідуальних користувачів.

ВИСНОВКИ

В умовах стрімкого розвитку технологій, Інтернет речей (IoT) набуває все більшого значення, надаючи безліч можливостей для управління побутовими та промисловими пристроями. Однак, зі зростанням кількості підключених до Інтернету пристроїв, підвищуються й ризики кіберзлочинності. Для забезпечення безпеки IoT-систем, необхідно впроваджувати комплексні заходи, які включають технологічні рішення, фізичний захист та належне управління.

По-перше, важливо розробляти надійні механізми аутентифікації та авторизації, використовувати шифрування для захисту даних та регулярно оновлювати програмне забезпечення. Також необхідно проводити аудит безпеки та моніторинг мережі для виявлення та запобігання потенційним загрозам, зокрема, атакам типу DDoS та іншим кібернападам.

По-друге, безпека IoT-мереж вимагає ретельного аналізу структури та загроз. Запобігання кіберзагрозам потребує оновлення програмного забезпечення, впровадження політик безпеки, моніторингу та шифрування. Лише комплексний підхід до захисту, систематичне впровадження рекомендацій та постійний моніторинг можуть забезпечити надійність та захищеність мережі.

По-третє, кібербезпека включає фізичні заходи, такі як використання камер відеоспостереження, датчиків руху та управління доступом. Використання складних паролів та двофакторної аутентифікації також є важливими елементами захисту.

Отже, для забезпечення стійкості та надійності IoT-мереж необхідно поєднувати технологічні рішення з фізичними заходами безпеки та ефективним управлінням. Комплексний підхід дозволить максимально використати потенціал IoT та забезпечити надійність і конфіденційність інформації в сучасному цифровому світі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Oracle: What is IoT? URL: https://www.oracle.com/cz/internet-of-things/what-is-iot/ (дата звернення: 09.04.2024).

2. Termin.in.ua: Інтернет речей (IoT) – що це таке і як працює, суть, технології і приклади. URL: https://termin.in.ua/internetrecheyiot/#google_vignette (дата звернення: 09.04.2024).

3. Sprintzeal: IoT Security Challenges and Best Practices-An Overview. URL: https://www.sprintzeal.com/blog/iotsecuritychallenges
(дата звернення: 10.04.2024).

4. Psacertified: The History of IoT Security. URL: https://www.psacertified.org/blog/a-historyofiotsecurity/ (дата звернення: 14.04.2024).

5. Check Point Research: The Tipping Point: Exploring the Surge in IoT Cyberattacks Globally. URL: https://blog.checkpoint.com/security/the-tipping-point-exploring-the-surge-in-iot-cyberattacksplaguingtheeducationsector/
(дата звернення: 14.04.2024).

6. Medium: What Are the Cyber Attacks on IoT Devices? URL: https://globalcybersecurityassociation.medium.com/what-are-the-cyber-attacks-on-iot-devices-fcc5e3b84526 (дата звернення: 14.04.2024).

7. Ophtek: 4 Real Life Examples of the IoT Being Hacked. URL: https://ophtek.com/4-real-life-examples-iot-hacked/ (дата звернення: 14.04.2024).

8. Doids on roids: 8 Key IoT Security Challenges and Proven Solutions from the Field. URL: https://www.thedroidsonroids.com/blog/iot-security-issues-internet-of-things-security#Best_IoT_security_practices (дата звернення: 16.04.2024).

9. IoT Security Foundation: Physical Security.An IoTSF Secure Design Best Practice Guide Article. URL: https://iotsecurityfoundation.org/best-practice-guide-articles/physical-security/ (дата звернення: 16.04.2024).

10. IoT for all: IoT Security and Physical Safety. URL:https://www.iotforall.com/iot-security-and-physical-safety (дата звернення: 18.04.2024).

11. Trend micro: IoT Security Issues, Threats, and Defenses. URL:

https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-security-101-threats-issues-and-defenses (дата звернення: 18.04.2024).

12. Expert insights: The Top 10 IoT Security Tools. URL: https://expertinsights.com/insights/the-top-iot-security-tools/ (дата звернення: 18.04.2024).

13. Б.Ю. Жураковський, І.О. Зенів. Технології Інтернету Речей: навчальний посібник. Київ: КПІ ім. Ігоря Сікорського, 2021. 271 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/dcd9e1aa-8bcc-4e76-b1e0-ed133bf616b2/content (дата звернення: 10.05.2024).

14. І.Є. Розанов, С.П. Сергієнко, Д.В. Чернов. Методичні вказівки до виконання лабораторних робіт з курсу Інтернет речей. Вінниця: ДонНУ ім. Василя Стуса, 2019. 60 с. URL:https://r.donnu.edu.ua/bitstream/123456789/1540/1/І.%20Є.%20Розанов%2С%20С.%20П.%20Сергієнко%2С%20Д.%20В.%20Чернов.%20МЕТОДИЧНІ%20ВКАЗІВКИ%20ДО%20ВИКОНАННЯ%20ЛАБОРАТОРНИХ%20РОБІТ%203%20КУРСУ%20ІНТЕРНЕТ%20РЕЧЕЙ%202019.pdf (дата звернення: 20.05.2024).

15. О.М. Густера. Інтернет речей: конспект лекцій. Київ: Національний Авіаційний Університет, 2019. 80 с. URL:https://er.nau.edu.ua/bitstream/NAU/44172/5/06_IP_КЛ.pdf (дата звернення: 03.06.2024).

ДОДАТОК А

Охорона праці, безпека в надзвичайних ситуаціях

А.1 Характеристика умов праці

Об'єктом дослідження є телекомунікаційна інфраструктура IoT-мережі, що включає мережеві пристрої, сервіси, і кінцеві IoT-пристрої. Сектор складу компанії займається вирішенням технічних питань, пов'язаних з роботою мережі, проблем користувачів мережі (як апаратним, так і програмним забезпеченням). Співробітники цього відділу працюють з комп'ютерним обладнанням, таким як ноутбуки або стаціонарні персональні комп'ютери.

Основними шкідливими факторами, зв'язаними з роботою на ПК є:

-напруга зорових органів та пов’язане з цим стомлення, захворювання і побічні ефекти;

-значне навантаження на пальці та кисті рук, що при відсутності профілактики та медичного контролю можуть викликати професійні захворювання;

-тривале перебування в одній і тій самій позі, що викликає застійні явища в організмі, та може сприяти різним захворюванням;

-випромінювання різного виду при використанні відеомоніторів на електронно-променевих грубках (м'яке рентгенівське випромінювання, ультрафіолетове випромінювання, видиме випромінювання, інфрачервоне випромінювання, низько і високочастотне електромагнітн випромінювання, електростатичні полючи);

-механічні шуми, що пов'язані з роботою електронно-механічного друкуючою пристрою (принтера), вентиляторів системи

-охолодження, приводів читання CD та DVD дисків та вібрація; іонізація повітря;

-наявність шкідливих хімічних речовин.

Дослідження науково-дослідного інституту гігієни праці та професійних

захворювань виявили зміни у функціональному стані зорового аналізатора у спеціалістів, які працюють з відеотерміналами, після чотирьох годин роботи.

Професійні захворювання при роботі з персональним комп’ютером:

-комп'ютерний зоровий синдром. Вплив роботи з монітором зазвичай залежить від віку користувача, від стану зору, а також від інтенсивності роботи з дисплеєм та організації робочого місця. В результаті тривалої роботи дуже великий ризик появи, або прогресивності вже наявної короткозорості.

-проблеми, що пов'язані з м'язами і суглобами. Нерухома напружена поза оператора, протягом тривалого часу прикутого до екрану монітора, призводить до втоми і виникнення болю в хребті, шиї, плечових суглобах, а також розвивається м'язова слабкість і відбувається зміна форми хребта. Інтенсивна робота з клавіатурою викликає больові відчуття в ліктьових суглобах, передпліччях, зап'ястях, в кистях і пальцях рук. Зазвичай присутні скарги на оніміння шиї, біль у плечах і попереку або поколювання в ногах. Але бувають, проте, і більш серйозні захворювання. Найбільш поширений кистьовий тунельний синдром, при якому нерви руки пошкоджуються внаслідок частої і тривалої роботи на комп'ютері. У найбільш важкій формі цей синдром проявляється у вигляді болісних відчуттів, що позбавляють людину працездатності.

-синдром комп'ютерного стресу. Постійні користувачі ПК зазвичай піддаються психологічним стресам, функціональних порушень центральної нервової системи, хвороб серцево- судинної системи.

-вплив на імунну систему. При впливі електромагнітного випромінювання (ЕМВ) порушуються процеси імуногенезу, опромінених ЕМВ, змінюється характер інфекційного процесу – протягом інфекційного процесу обтяжується. ЕМВ можуть сприяти неспецифічному пригнічення імуногенезу, посилення утворення антитіл до тканин плоду і стимуляції аутоімунної реакції в організмі вагітної самки.

-вплив на ендокринну систему і нейрогуморальну реакцію. При дії ЕМВ, як правило, відбувається стимуляція гіпофізарно- адреналінової системи, що

супроводжується збільшенням вмісту адреналіну в крові, активацією процесів згортання крові.

-вплив на статеву функцію. Порушення статевої функції зазвичай пов'язані зі зміною її регуляції з боку нервової та нейроендокринної систем.

Симптоми захворювання різноманітні та численні. Зазвичай виявлення одного симптому малоймовірно, оскільки всі функціональні органи людини взаємопов'язані.

1. Фізичні нездужання: сонливість, непроходяча втома; головний біль

після роботи; болі в нижній частині спини, в ногах, відчуття поколювання,оніміння, болі в руках; напруженість м'язів верхньої частини тулуба.

2. Захворювання очей: відчуття гострого болю, печіння, свербіння.

3. Порушення візуального сприйняття: неясність зору, яка збільшується протягом дня; виникнення подвійного зору.

4. Погіршення зосередженості і працездатності: зосередженість досягається за працею; дратівливість під час і після роботи; повітря робочої точки на екрані; помилки при друкуванні.

А.2 Вимоги до виробничик приміщень

До приміщення офісу та організації робочого місця з урахуванням шкідливих виробничих факторів пред'являється низка вимог. Приміщення з робочими місцями для ПК повинно мати природне освітлення, бажано з однобічним розміщенням вікон, площа скління яких не повинна перевищувати 25% від площі стіни з вікнами. Вікна повинні мати регульовані жалюзі чи занавіски або інші сонцезахисні пристрої. Розміщення робочих місць з ПК у підвальних та цокольних поверхах не допускається. Робочі місця з ПК рекомендується розміщувати в окремих приміщеннях. Площа на одного працюючого з ПК повинна складати 6 м², а об’єм – 20 м³.

Неприпустиме розташування ПК так, щоб користувач сидів обличчям або

спиною до вікон чи кімнати задньою частиною до ПК, у яку монтуються вентилятори. Забороняється використовувати для обробки інтер'єру приміщень з ПК полімерні матеріали, що виділяють у повітря шкідливі хімічні речовини у концентраціях, що перевищують гранично допустимі і не включені в «Перелік дозволених, МЗ» 1977-1985 років.

В офісі робочі місця з ПК розташовані від стіни з вікнами на відстані 1 м. Екрани моніторів ПК знаходяться на відстані 700 мм від очей користувачів. Робочі місця в сидячому положенні відповідають вимогам ДСТ 12.2.032–78 та ДСТ 12.2.029–77. Поверхня робочого столу розташована на висоті 0,75 м від підлоги, розміри робочої поверхні стільниці складають 1050х590 мм, а розміри вільного простору для ніг під столом – висота 650 мм, глибина 550 мм, ширина 450 мм. Робочий стілець оснащений підйомно-поворотним механізмом, що забезпечує регулювання висоти сидіння і спинки, пневматичними і гідравлічними амортизаторами, а також підлокітниками.

А.2.1 Освітлення

Правильно спроектоване та виконане освітлення покращує умови зорової роботи, знижує втому, підвищує продуктивність праці, позитивно впливає на виробниче середовище, забезпечує сприятливий психологічний ефект на працівника, підвищує безпеку праці та знижує травматизм. Недостатнє освітлення призводить до напруження зору, зниження уваги і передчасної втоми. Надмірна яскравість викликає осліплення, подразнення та біль в очах. Неправильний напрямок освітлення на робочому місці може створювати різкі тіні, відблиски і дезорієнтацію працівника. Усі ці фактори можуть призвести до нещасних випадків або професійних захворювань, тому важливий правильний розрахунок освітлення.

Згідно з СНиП II-4-79, у приміщенні необхідно застосовувати систему комбінованого освітлення. При виконанні робіт високої зорової точності (найменший розмір об’єкта розрізнення 0.3-0.5 мм) коефіцієнт природного

освітлення (КПО) повинен бути не нижче 1,5%. Для зорової роботи середньої точності (найменший розмір об’єкта розрізнення 0.5-1.0 мм) КПО повинен бути не нижче 1%. Як джерела штучного освітлення зазвичай використовуються люмінесцентні лампи типу ЛБ або ДРЛ, які попарно об'єднуються в світильники, розташовані над робочими поверхнями рівномірно.

Вимоги до освітлення у приміщеннях з комп'ютерною технікою наступні: при виконанні робіт високої зорової точності загальна освітленість повинна складати 400 лк, а комбінована – 750 лк; для робіт середньої точності – 200 лк і 300 лк відповідно. Крім того, усе поле зору повинно бути освітлене рівномірно, що є основною гігієнічною вимогою. Іншими словами, ступінь освітлення приміщення та яскравість екрану комп’ютера повинні бути приблизно однаковими.

А.2.2 Параметри мікроклімату

Параметри мікроклімату можуть змінюватися в широких межах, проте для підтримки життєдіяльності людини необхідна постійність температури тіла, що забезпечується терморегуляцією – здатністю організму регулювати тепловіддачу до навколишнього середовища. Принцип нормування мікроклімату полягає у створенні оптимальних умов для теплообміну тіла людини з навколишнім середовищем.

Комп'ютерна техніка є джерелом значних тепловиділень, що може призвести до підвищення температури та зниження відносної вологості в приміщенні. У приміщеннях з комп'ютерами повинні дотримуватися певні параметри мікроклімату. Згідно з санітарними нормами СН 245-71, встановлені величини параметрів мікроклімату, які забезпечують комфортні умови. Ці норми залежать від пори року, характеру трудового процесу та типу виробничого приміщення.

Об'єм приміщень, у яких розташовані робочі місця працівників офісу, не повинен бути меншим за 19,5 м³ на людину, з урахуванням максимальної

кількості одночасно працюючих у зміну.

Таблиця А.1-Параметри мікроклімату

Пора року	Параметри мікроклімату	Величина
Холодна	Температура повітря	22…24°С
	Відносна вологість	40…60%
	Швидкість руху повітря	До 0,1 м/с
Тепла	Температура повітря	23…25°С
	Відносна вологість	40…60%
	Швидкість руху повітря	0,1…0,2 м/с

Таблиця А.2-Норми подачі свіжого повітря в приміщення

Характеристика приміщення	Об’ємні витрати свіжого повітря, що подаєтьсяв приміщенні $м^3$/на одну людину в годину
Об'єм до 20 $м^3$ на людину	Не менш ніж 30
20.. .40 $м^3$ на людину	Не менш ніж 20
Більш ніж 40 $м^3$ на людину	Природня вентиляція

Для забезпечення комфортних умов використовуються як організаційні методи (раціональна організація проведення робіт залежно від пори року та часу доби, чергування праці та відпочинку), так і технічні засоби (вентиляція, кондиціювання повітря, опалювальна система).

А.2.3 Електромагнітне та іонізуюче випромінювання

Максимальний рівень рентгенівського випромінювання не перевищує 10 мкбер/год, а інтенсивність ультрафіолетового та інфрачервоного випромінювань від екрану монітора становить 10-100 мВт/м².

Таблиця А.3 – Показники допустимих значень параметрів неіонізуючихелектромагнітних випромінювань (згідно з СанПиН 2.2.2.542- 96)

Параметр	Допустимі значення
Напруженість електричної складової електромагнітного поля на відстані 50 см відповерхні монітору	10 В/м
Напруженість магнітної складової електромагнітного поля на відстані 50 см відповерхні монітору	0,3 А/м
Напруженість електростатичного поля не повинна перевищувати для дорослих користувачів	20 кВ/м

Для зниження дії цих видів випромінювань рекомендується застосовувати монітори з пониженим рівнем випромінювань, встановлювати захисні екрани, а також дотримуватися регламентованих режимів праці та відпочинку.

А.3 Заходи щодо поліпшення умов праці

А.3.1 Мікроклімат робочого місця

Приміщення має площину 27,5м2 (5,5 м* 5 м); висота усередині 2,5м, об’єм становить 68,75 м3. У приміщенні розташовані: 2 системних блока, 2 монітори, DNS сервер, комутатор, маршрутизатор, 1 кондиціонер. У приміщенні офісу є джерела тепловиділення, тому необхідно визначити необхідні умови його вентилювання. Витрату повітря в приміщенні з додатковим тепловиділенням визначаємо за формулою:

$$L = \frac{Q_{НАД}}{c \cdot p \cdot (t_В - t_Н)} \qquad (А.1)$$

де $Q_{НАД}$ -надлишкове виділення тепла в робочому приміщенні, ккал/год;

с – теплоємкість повітря (0,237 ккал/кг);

р – обсягова вага повітря (1,226 кг/м3);

t В – температура витяжного повітря (30$^{\circ}C$);

tН – температура приточного повітря (20$^{\circ}C$).

Розрахуємо надлишкове надходження тепла за наступною формулою:

$$Q_{НАД} = Q_{УСТ} + Q_{ПЕР} + Q_{ОСВ} + Q_{СР}, \quad (А.2)$$

Де $Q_{НАД}$-виділення тепла від устаткування;

$Q_{ОСВ}$-надходження тепла від електричного освітлення;

$Q_{СР}$-надходження тепла від сонячної радіації через вікна;

$Q_{ПЕР}$-виділення тепла робітниками.

Визначемо виділення тепла від устаткування за формулою:

$$Q_{УСТ} = P \cdot K_а \cdot K_б \cdot 860, \quad (А.3)$$

Де P – сумарна потужність устаткування, кВт/год;

$K_а$ - коефіцієнт установленої потужності (0,95);

$K_б$ - коефіцієнт одночасної роботи (1,0).

$$Q_{УСТ} = [(x_1 \cdot k_1) + (x_2 \cdot k_2) + (x_3 \cdot k_3) + (x_4 \cdot k_4) + (x_5 \cdot k_5) + (x_6 \cdot k_6)] \cdot K_а \cdot K_б \cdot 860, \quad (А.4)$$

Де $x_1, x_2, x_3, x_4, x_5, x_6$ - кількість системних блоків, моніторів, серверів, маршрутизаторів та комутаторів, кондиціонерів відповідно;

$k_1, k_2, k_3, k_4, k_5, k_6$ - їх потужність.

Розрахуємо:

$$Q_{УСТ} = [(2 \cdot 0,45) + (2 \cdot 0,1) + (1 \cdot 1,5) + (1 \cdot 0,35) + (1 \cdot 0,4) + (1 \cdot 0,25)] \cdot 0,95 \cdot 1 \cdot 860 = 2941,2 ккал / год.$$

Визначимо виділення тепла від обслуговування персоналу за допомогою наступної формули:

$$Q_{ПЕР} = n \cdot g = 2 \cdot 100 = 200 ккал / год, \quad (А.5)$$

Де *n* – кількість працюючих;

g – кількість тепла, що виділяє один працівник за годину (100 ккал/год).

Визначимо надходження тепла від електричного освітлення за формулою:

$$Q_{ОСВ} = E_M \cdot g_1 \cdot S = 400 \cdot 0,05 \cdot 27,5 = 550 ккал / год, \quad (А.6)$$

Де E_M - нормована освітленість для цієї зорової роботи, величина якої дорівнює 400 лк;

g_1 - питоме тепловиділення на 1 м^2 підлоги при 1 лк освітленості (для люмінесцентних ламп – 0,05 ккал/год);

S - площа приміщення, м^2.

Визначимо надходження тепла від сонячної радіації через вікна за наступною формулою:

$$Q_{СР} = F \cdot g_2 \cdot K_{ОСЛ} = 2,2 \cdot 65 \cdot 0,4 = 57,2 ккал / год, \quad (А.7)$$

Де F – площа віконних прорізів (2,2 м^2);

g_2 – кількість тепла, що надходить через 1 м^2 віконного прорізу (65 ккал/год);

$K_{ОСЛ}$ - коефіцієнт ослаблення, приймаємо 0,4.

Визначимо кількість надлишкового тепла:

$$= \quad Q_{НАД} = Q_{УСТ} + Q_{ПЕР} + Q_{ОСВ} + Q_{СР} = 2941,2 + 200 + 550 + 57,2 = 3748,4 ккал / год$$

Визначимо витрати повітря в приміщенні:

$$L = \frac{Q_{НАД}}{c \cdot p \cdot (t_В - t_Н)} = \frac{3748,4}{0,237 \cdot 1,226 \cdot (30-20)} = 1290,05 м^3 / год.$$

Існуюча в наявності система кондиціювання і вентилювання має продуктивність 2000 м^3/годину, що задовольняє необхідним нормативам.

А.3.2 Розрахунок системи загального рівномірного освітлення

Розміри прміщення: довжина (a=5,5), ширина (b=5), висота (h=2,5). Приміщення має світу побілку: коефіцієнт відбиття $P_{стелі}$=70%, $P_{стін}$=50%. Висота робочих поверхонь (столів) $h_р$=0,7 м. Для освітлення прийнято світильник типу УПМ-15, які підвищують до стелі, відстань від світильника до стелі $h_с$=0,4 м. Мінімальна освітленість за нормами E=200 лк.

1) Визначимо висоту підвісу світильників над підлогою:

$$h_0 = H - h_c = 2,5 - 0,4 = 2,1 м. \quad (А.8)$$

Для світильників загального освітлення з лампами розжарювання потужністю до 200 Вт мінімальна висота підвісу над підлогою відповідно до СНІП П-4-79 повинна бути у межах (2,5-4,0) м., залежно від характеристик світильника. В офісі відповідає цій вимозі.

2) Визначимо висоту підвісу світильника над робочою поверхнею:

$$h = h_0 - h_р = 2,1 - 0,7 = 1,4 м. \quad (А.9)$$

Рівномірність освітлення досягається при відповідному співвідношенні відстані між світильниками (L) та висоти їх підвісу (h).

3) Визначимо рекомендовану відстань між світильниками:

$$L = 0,7 \cdot h = 0,7 \cdot 1,4 = 0,98 м. \quad \text{(А.10)}$$

4) Розрахуємо необхідну кількість світильників:

$$N = \frac{a \cdot b}{L^2} = \frac{5,5 \cdot 5}{0,98^2} \approx 29 \quad \text{(А.11)}$$

Приймаємо, як 30 світильників, враховуючи розміри приміщення розміщуємо їх у 5 рядів, 6 штук.

5) Світловий потік лампи світильника ($Ф_Л$) визначається за формулою:

$$Ф_Л = \frac{E \cdot K_З \cdot S \cdot Z}{N \cdot n \cdot \eta}, \quad \text{(А.12)}$$

де E – нормативна освітленість,лк;

$K_З$ – коефіцієнт запасу, який враховує зниження освітленості в результаті забруднення та старіння ламп;

S - площа приміщення, що освітлюється, м2;

Z – коефіцієнт нерівномірності освітлення для ламп розширювання(1,15);

N – кількість світильників;

n – кількість ламп у світильнику;

η - коефіцієнт виокристання світового потоку, який визначається за світлотехнічними таблицями залежно від показника приміщення (i) та коефіцієнтів відбиття стін і стелі.

6) Визначимо показник приміщення:

$$i = \frac{a \cdot b}{h \cdot (a + b)} = \frac{5,5 \cdot 5}{2,5 \cdot (5,5 + 5)} = 1,05 \quad \text{(А.13)}$$

Коефіцієнт використання $\eta = 0,46$ для світильника УМП-15 (при i=1,05, $Р_{стелі}$=70%, $Р_{стін}$=50%).

Світловий потік одного світильника, а значить і лампи, оскільки за конструктивним виконанням у світильнику цього типу встановлена лише одна лампа, дорівнює:

$$\Phi_{Л} = \frac{E \cdot S \cdot Z}{N \cdot n \cdot \eta} = \frac{200 \cdot 27,5 \cdot 1,15}{30 \cdot 1 \cdot 0,46} = 458,3 лм \qquad (А.14)$$

9) Обираємо лампу Г-40 потужністю 40 Вт, світловий потік якої становить 500 лм. Хоча це значення на 9% більше розрахованого, однак не перевищує встановлену норму (- 0% $< \Phi_{Л} <$ +20%). Сумарна електрична потужність усіх світильників, встановлених у приміщенні становить:

$$P_{СВ} = P \cdot N = 40 \cdot 30 = 120 Вт \qquad (А.15)$$

А.4 Пожежна безпека

Найважливішою умовою роботи будь-якого підприємства є дотримання правил пожежної безпеки. В офісі основні заходи для забезпечення пожежної безпеки визначає «Інструкція про заходи пожежної безпеки для службових приміщень (офісів)». Вона є обов'язковою для всіх співробітників відділу. Згідно з цією інструкцією, у кожному приміщенні повинен бути призначений відповідальний за пожежну безпеку, а на видному місці має бути розміщена табличка з вказівкою його посади та прізвища.

Меблі й обладнання повинні розташовуватися таким чином, щоб забезпечувався вільний евакуаційний прохід до дверей виходу з приміщення (шириною не менше 1 м). Евакуаційні шляхи та виходи повинні бути постійно вільними, без будь-яких перешкод. Під час накопичення та по завершенню роботи пальні відходи слід збирати в спеціально відведені сміттєзбиральники.

Електромережі, електроприлади та апаратура повинні використовуватися тільки у справному стані, з урахуванням рекомендацій виробника. У разі

виявлення ушкоджень електромереж, вимикачів, розеток та інших електровиробів їх слід негайно відключити та вжити необхідних заходів для приведення у пожежобезпечний стан. Документи, папір та інші горючі матеріали повинні зберігатися на відстані не менш ніж 1 м від електрощитів, електрозбірок та електрокабелів, 0,5 м від світильників та 0,25 м від приладів опалення.

Засоби протипожежного захисту (пожежні крани, пожежна та охоронно-пожежна сигналізація, первинні засоби пожежогасіння тощо) повинні бути в справному стані. Усі працівники повинні пройти протипожежний інструктаж, вміти користуватися наявними вогнегасниками та іншими первинними засобами пожежогасіння, а також знати місця їхнього розташування. Відстань від найвіддаленішого місця в приміщенні до вогнегасника не повинна перевищувати 20 м.

А.5 Безпека при надзвичайних ситуаціях в компанії

Об’єктом дослідження з точки зору визначення потенційних надзвичайних ситуацій та їх наслідків є офісне приміщення. Однією з потенційних загроз є виникнення пожежі внаслідок короткого замикання в електромережах або статичних розрядів, що може призвести до серйозних пошкоджень будівлі, устаткування, комунікацій та виділення токсичних продуктів горіння.

Для забезпечення пожежної безпеки в офісі розроблено оперативний план гасіння пожежі, який визначає порядок дій персоналу у випадку виникнення пожежі, способи гасіння у електроустаткуванні, взаємодію з внутрішнім пожежним складом та використання засобів пожежогасіння з урахуванням заходів безпеки.

Також будівля обладнана мережею протипожежного водопостачання та системами виявлення та гасіння пожеж згідно з вимогами нормативно-технічних документів. Кожен співробітник повинен чітко знати та дотримуватися вимог пожежних правил і протиаварійного режиму, вміти користуватися вогнегасниками та іншими засобами первинного пожежогасіння, а також знати

місце їх розташування.

Меблі та обладнання мають бути розташовані таким чином, щоб забезпечувався вільний евакуаційний прохід до дверей виходу (шириною не менше 1 м), а евакуаційні шляхи і виходи мають залишатися вільними від перешкод.

У випадку виявлення пожежі необхідно негайно повідомити державну пожежну службу за телефоном «101», зазначивши адресу, кількість поверхів, місце виникнення пожежі та наявність людей. Також слід інформувати керівництво і, в нічний час, чергового охоронця. При можливості необхідно розпочати гасіння пожежі наявними засобами та організувати зустріч пожежних підрозділів.

Важливою складовою безпеки є ефективна евакуація людей з палаючої будівлі. Це досягається, коли час евакуації не перевищує час настання критичних фаз розвитку пожежі, таких як критичні температури, ступінь задимлення чи зниження концентрації кисню. Кількість евакуаційних виходів повинна бути не менше двох і вони повинні розташовуватися розсереджено.

Мінімальна відстань між найбільш віддаленими один від одного евакуаційними виходами із приміщень визначається за формулою:

$$l = 1,5 \cdot \sqrt{P} = 1,5 \cdot \sqrt{27,5} = 7,9 м, \qquad \text{(А.16)}$$

де P – периметр приміщення, м.

Офісне приміщення, як об’єкт дослідження з точки зору надзвичайних ситуацій, потенційно стикається з різними загрозами, серед яких особливе значення має пожежна небезпека, спричинена можливими короткими замиканнями в електромережах або статичними розрядами. Ці події можуть призвести до значних матеріальних збитків, пошкоджень будівельних конструкцій, обладнання та інфраструктури, а також виділення токсичних продуктів горіння.

Для забезпечення пожежної безпеки в офісі розроблено оперативний план

дій у разі пожежі. Цей план включає чіткі інструкції щодо поведінки персоналу, використання пожежних засобів та взаємодії з пожежними підрозділами. Важливо, щоб кожен співробітник був ознайомлений з цим планом і знав свої обов’язки у випадку пожежі.

У разі виникнення пожежі необхідно негайно повідомити державну пожежну службу за номером «101», точно вказавши адресу, кількість поверхів, місце виникнення пожежі та наявність людей. Після цього необхідно організувати евакуацію працівників, уникаючи паніки, і допомагати особам, які потребують допомоги, зокрема літнім і дітям.

Двері на евакуаційних шляхах повинні відкриватися у напрямку виходу з будівлі, щоб сприяти швидкій евакуації. В кожному приміщенні має бути вивішений план евакуації, який дозволяє працівникам швидко зорієнтуватися і вибрати найбезпечніший шлях виходу.

Якщо приміщення не охоплено пожежею, але ви знаходитесь у зоні диму чи високої температури, слід негайно закрити всі двері за собою, щоб уникнути поширення диму. Якщо вам доведеться перебувати в задимленому приміщенні, намагайтеся залишатися якомога нижче, дихаючи через вологу тканину, що може допомогти фільтрувати токсичні гази. При відсутності іншого виходу, яким є евакуаційні шляхи та сходи, залишіться вигодувати вікно, та зачекайте на прихода рятувальників.