

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему:

**«Методи та засоби підвищення рівня захищеності системи
обміну даними з громадським транспортом»**

Виконав студент 2-го курсу групи КБм-22-1
спеціальності 125 «Кібербезпека»



Михайло Хохлов

Керівник

професор кафедри комп'ютерної інженерії та кібербезпеки,
доктор технічних наук, доцент



Володимир Воротніков

Рецензент

доцент кафедри комп'ютерної інженерії та кібербезпеки,
кандидат технічних наук, доцент



Юрій Россінський

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

ЗАТВЕРДЖУЮ

Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
«13» жовтня 2023 р.

ЗАВДАННЯ

на випускнуну кваліфікаційну роботу магістра

Студент: Хохлов Михайло Олегович

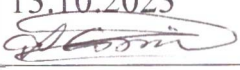
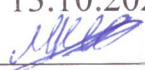
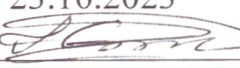
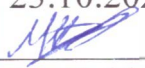
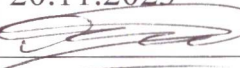
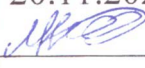
Тема роботи: «Методи та засоби підвищення рівня захищеності системи обміну даними з громадським транспортом»

затверджена Наказом університету від «13» жовтня 2023 р. № 572/с

Термін здачі студентом закінченої роботи «11» грудня 2023 р.

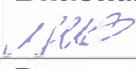
1. Вихідні дані роботи (зазначається предмет і об'єкт дослідження):
 1. Об'єктом дослідження є процес розробки проєкту системи підвищення захищеності інформації та алгоритму обміну даними.
 2. Предметом дослідження є методи та засоби забезпечення захищеності обміну інформації у громадському транспорті із центром обробки даних.
2. Обладнання та програмне забезпечення:
 1. Cisco Systems: Routers, Switches & Security Appliance
 2. Wireshark

3. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посади консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1	Андрій Єфіменко, завідувач кафедри кафедри КІ та КБ, к.т.н., доцент	13.10.2023 	13.10.2023 
2	Андрій Єфіменко, завідувач кафедри кафедри КІ та КБ, к.т.н., доцент	23.10.2023 	23.10.2023 
3	Андрій Єфіменко, завідувач кафедри кафедри КІ та КБ, к.т.н., доцент	20.11.2023 	20.11.2023 

4. Дата видачі завдання «13» жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів роботи	Примітка
1	Отримання завдання на кваліфікаційну роботу та його уточнення	13 жовтня 2023 – 14 жовтня 2023	Виконано 
2	Пошук та опрацювання літературних джерел. Вивчення існуючих аналогів систем захисту	15 жовтня 2023 – 24 жовтня 2023	Виконано 
3	Оформлення технічного завдання проекту захисту системи згідно державних стандартів НД ТЗІ та ДСТУ	25 жовтня 2023 – 31 жовтня 2023	Виконано 
4	Розробка структури проекту системи та UML-діаграм зв'язків між компонентами	1 листопада 2023 – 5 листопада 2023	Виконано 
5	Побудова та налагодження мережі та системи	6 листопада 2023 – 14 листопада 2023	Виконано 
6	Перевірка працездатності створеного проекту системи	15 листопада 2023 – 19 листопада 2023	Виконано 
7	Оформлення пояснювальної записки (чистовик)	20 листопада 2023 – 5 грудня 2023	Виконано 
8	Розробка тексту доповіді та презентації	6 грудня 2023 – 10 грудня 2023	Виконано 
9	Подання роботи керівнику та рецензенту для допуску до захисту	11 грудня 2023	Виконано 
10	Захист	27 грудня 2023	Виконано

Студент  Михайло Хохлов

Керівник  Володимир Воротніков

РЕФЕРАТ

Випускна кваліфікаційна робота магістра складається з дослідження та практичного застосування методів та засобів підвищення рівня захищеності системи обміну даними з громадським транспортом, топології мережі та пояснювальної записки. Текстова частина викладена на 83 сторінках. Пояснювальна записка до випускної роботи містить 79 ілюстрацій, 7 таблиць та 5 додатків. Список використаних джерел містить 48 найменувань.

Метою дослідження є вдосконалення теоретичних основ та формулювання рекомендацій щодо підвищення рівня безпеки цифрової інформації у громадському транспорті, шляхом розробки надійної системи захисту даних.

Представлена загальна топологія мережі, проведено опис характеристик мережевого обладнання та політики безпеки. Наведені результати практичних випробувань захисту системи обміну інформації.

КЛЮЧОВІ СЛОВА: МЕРЕЖА, VPN, CISCO, ЗАХИСТ МЕРЕЖ, Internet of Things.

ABSTRACT

The final qualification work of the master degree consists of research and practical application of methods and means of increasing the security level of the data exchange system with public transit, network topology and an explanatory note. The text part is laid out on 83 pages. The explanatory note to the final thesis contains 79 illustrations, 7 tables and 5 appendices. The list of used sources contains 48 names. The purpose of the study is to improve the theoretical foundations and formulate recommendations for increasing the level of data transmission security in public transport by developing a reliable information exchange system. The general topology of the network is presented, the characteristics of network equipment and security policy are described. The results of practical tests of protection of the information exchange system are given.

KEY WORDS: NETWORK, VPN, CISCO, NETWORK PROTECTION, Internet of Things.

ЗМІСТ

ВСТУП	8
РОЗДІЛ 1. ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИЩЕНОСТІ СИСТЕМ ОБМІНУ ДАНИМИ	12
1.1. ОБҐРУНТУВАННЯ АКТУАЛЬНОСТІ ПИТАННЯ ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ З ГРОМАДСЬКИМ ТРАНСПОРТОМ	12
1.2. АНАЛІЗ ПРИКЛАДІВ УДОСКОНАЛЕННЯ ЗАХИСТУ СИСТЕМ ОБМІНУ ДАНИМИ З ГРОМАДСЬКИМ ТРАНСПОРТОМ	16
1.3. ДОСЛІДЖЕННЯ СКЛАДОВИХ АРХІТЕКТУРИ INTERNET OF THINGS (IoT)	21
1.4. ДОСЛІДЖЕННЯ ТРАФІКУ ІНФОРМАЦІЙНОЇ СИСТЕМИ ТРАНСПОРТНОГО ЗАСОБУ	25
1.5. ПОСТАНОВКА ЗАВДАННЯ. ТЕХНІЧНІ ВИМОГИ ДО ПРОЄКТУ	31
1.5.1 Технічне завдання проєкту підвищення захищеності системи обміну даними з громадським транспортом	31
Висновки до розділу 1	45
РОЗДІЛ 2. РОЗРОБКА ПРОЄКТУ ЗАХИЩЕНОСТІ СИСТЕМИ ОБМІНУ ДАНИМИ З ГРОМАДСЬКИМ ТРАНСПОРТОМ	46
2.1. РОЗРОБКА СТРУКТУРНОЇ СХЕМИ МЕРЕЖІ ПРОЄКТУ СИСТЕМИ	46
2.2. ВИБІР ТЕХНІЧНИХ ЗАСОБІВ ДЛЯ РЕАЛІЗАЦІЇ СИСТЕМИ	53
2.3. ВИБІР ПРОТОКОЛУ ШИФРУВАННЯ ТА ЗАХИСТУ ІНФОРМАЦІЇ	61
2.4. СТВОРЕННЯ ДІАГРАМИ АКТИВНОСТІ ТА ФУНКЦІОНАЛЬНОЇ СХЕМИ	68
Висновки до розділу 2	71
РОЗДІЛ 3. ПРАКТИЧНА ПОБУДОВА ТА ПЕРЕВІРКА ПРАЦЕЗДАТНОСТІ ПРОЄКТУ СИСТЕМИ	72
3.1. СТВОРЕННЯ ПРАКТИЧНОЇ МОДЕЛІ ПРОЄКТУ, ПІДГОТОВКА ОБЛАДНАННЯ	72
3.2. НАЛАШТУВАННЯ СИСТЕМИ ТА ТЕСТУВАННЯ НА ПРАЦЕЗДАТНІСТЬ	78
3.3. РЕКОМЕНДАЦІЇ ПО ЗАСТОСУВАННЮ СТВОРЕНОЇ МОДЕЛІ СИСТЕМИ ЗАХИСТУ ..	92
Висновки до розділу 3	92
ВИСНОВКИ	94
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	96
ДОДАТКИ	102

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

DHCP – Dynamic Host Configuration Protocol

HSRP – Hot Standby Router Protocol, Hot Standby Redundancy Protocol

IKE – Internet Key Exchange

IP – Internet Protocol

IPSec – Internet Protocol Security

L2TP – Layer 2 Tunneling Protocol

LAN – Local Area Network

NTP – Network Time Protocol

OSI – Open Systems Interconnection

PPTP – Point-to-Point Tunneling Protocol

SYSLOG – System log

TCP – Transmission Control Protocol

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

WAN – Wide Area Network

WLAN – Wireless Local Area Network

БК – бортовий комп'ютер

ІС – інформаційна система

ОС – операційна система

ЦОД – Центр обробки даних

ВСТУП

Актуальність теми. Забезпечення безпеки інформації на сьогоднішній день стоїть серед найбільш актуальних викликів у сфері інформаційних технологій. Розвиток Інтернету речей у сучасному світі підкреслює важливість вирішення завдань по підвищенню інформаційної безпеки, які мають високий пріоритет. Глобальна мережа, швидко поширюючись і розвиваючись, встановлюється як ключовий і ефективний інструмент комунікації. Сьогодні неможливо уявити створення новітніх технологій, концепцій та стратегій без використання цього потужного засобу. Великі кластери мереж, які утворюють собою Інтернет, зробили можливим миттєвий доступ до будь-якої інформації для кожного. Мережі вже відіграють важливу роль у суспільному розвитку та реалізації різноманітних напрямків досліджень та відкриттів.

Навіть при наявності систем безпеки інформації та відносної безпеки даних компаній, інциденти витоку інформації все ж трапляються. Це стимулює необхідність створення та постійного удосконалення систем безпеки для компаній чи установ. При цьому слід враховувати економічну обґрунтованість та що саме очікується від таких систем, особливо беручи до уваги витрати на відновлення після кібератак.

Громадський транспорт – галузь, яка вже давно стала невід’ємною складовою суспільства, і розвивається й до нині. Ми кожен день, так чи інакше, користуємось ним: метро, автобус, трамвай, тролейбус, потяг – усе це та ще багато інших видів являють собою сучасні засоби переміщення населення.

Розвиток ІТ-технологій та жага перевізників до покращення обслуговування для пасажирів, призвели до появи цілої окремої гілки у сфері Інтернету речей (IoT) – Інформаційних систем громадського транспорту.

Підвищення рівня інформаційної безпеки на транспортному підприємстві стало важливим елементом для подальшого розвитку у комерційній та безпековій сферах. Хакерські угруповання постійно удосконалюють свої методи за засоби проведення атак на такі системи, тому питання безпеки приватних даних пасажирів та підприємств вимагає впровадження сучасних систем захисту.

Мета і завдання дослідження – метою написання кваліфікаційної роботи є удосконалення теоретичних основ та розробка проєкту системи підвищення рівня захищеності обміну даними з громадським транспортом.

Для досягнення мети необхідно виконати низку завдань:

- Ознайомлення з системами та засобами захисту інформації;
- Дослідження переваг та недоліків існуючих засобів захисту трафіку із транспортними засобами;
- Визначення архітектури Інтернету Речей (IoT);
- Вивчення та налаштування технічних засобів обміну інформації, протоколів шифрування даних;
- Розробка моделі проєкту підвищення захищеності системи обміну даними з громадським транспортом;
- Дослідження та порівняння пристроїв захисту інформації та алгоритмів шифрування;
- Розробка рекомендацій щодо застосування технології захищеного трафіку між віддаленою мережею транспортного засобу та центром обробки даних, задля запобігання вторгнень та витоку інформації у майбутньому.

Об’єктом дослідження є процес розробки проєкту системи підвищення захищеності інформації та алгоритму обміну даними.

Предметом дослідження є методи та засоби забезпечення захищеності обміну інформації у громадському транспорті із центром обробки даних.

Наукова новизна дослідження полягає у використанні новітніх теоретичних баз та побудові практичних рекомендацій щодо використання сучасних засобів захисту передачі інформації.

було порушено:

актуальну проблему захищеності інформації що передається всередині транспортних організацій з їх рухомим складом. Акцентовано увагу на важливості впровадження шляхів захисту від неавторизованого доступу та подальшого витоку інформації.

удосконалено:

методичні та практичні рекомендації щодо побудови захищеної мережі передачі інформації всередині транспортних організацій.

Практичне значення одержаних результатів. Одержані в роботі наукові результати доведено до рівня пропозицій, практична реалізація яких покращить рівень захисту даних що передаються між транспортом та центром обробки даних всередині організації. Розроблені рекомендації дозволять підвищити рівень обізнаності персоналу транспортних організацій, які працюють з інформаційно-комунікаційними системами.

Особистий внесок магістра. Випускна кваліфікаційна робота є самостійно виконаним науковим дослідженням. Автор особисто розробив пропозиції та рекомендації.

За результатами дослідження було опубліковано:

1. Хохлов М. О., Вакалюк Т.А. Захист передачі інформації на рухомому транспорті при використанні технології LTE // Тези V Всеукраїнської науково-практичної інтернет-конференції студентів, аспірантів та молодих вчених «Сучасні інформаційні системи та технології», м. Хмельницький, 30 листопада 2022 р. – Хмельницький: Херсонський національний технічний університет, 2022.

2. Хохлов М. О., Єфіменко А.А., Вакалюк Т.А. Організація системи захищеного обміну даними транспортного підприємства із рухомих складом // Тези III Всеукраїнської науково-практичної Інтернет-конференції «Сучасні комп'ютерні та інформаційні системи і технології», м. Київ, 12-19 грудня 2022 р. – Київ: Таврійський національний університет імені В. І. Вернадського, 2022.

Апробація результатів дослідження. Основні теоретичні положення та практичні результати дослідження апробовано у доповідях та обговореннях на V-й Всеукраїнській науково-практичній інтернет-конференції студентів, аспірантів та молодих вчених «Сучасні інформаційні системи та технології» (м. Хмельницький, 2022 р.), III-й Всеукраїнській науково-практичній Інтернет-

конференції «Сучасні комп'ютерні та інформаційні системи і технології». (м. Київ, 2022 р.).

Структура та обсяг роботи. Пояснювальна записка до випускної кваліфікаційної роботи складається з переліку умовних скорочень, вступу, трьох розділів, висновків, списку використаної літератури та додатків.

У першому розділі досліджено актуальність теми роботи, проаналізували відомі приклади та шляхи забезпечення інформації. Дослідили архітектуру Інтернету Речей (IoT) та провели дослідження рівня захищеності даних інформаційної системи громадського транспорту. Розробили технічні вимоги до підвищення захищеності систем обміну даними з громадським транспортом.

У другому розділі розроблено загальну топологію мережі, створено структурну та функціональну схеми проєкту, UML-діаграми: використання, активності, послідовності та класів. Описано деякі відомі серії обладнання для використання у проєкті, проведено аналіз їх технічних та якісних характеристик. Проаналізовано політики безпеки та протоколи захисту інформації.

У третьому розділі було налаштовано попередньо обране обладнання яке використовуватиметься розробленою моделлю захисту інформації з громадським транспортом. Наведені результати тестування коректності роботи створеної системи. Висновки містять інформацію щодо кінцевих результатів здійсненої роботи.

РОЗДІЛ 1. ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИЩЕНОСТІ СИСТЕМ ОБМІНУ ДАНИМИ

1.1. Обґрунтування актуальності питання підвищення рівня захищеності інформаційних систем з громадським транспортом

У кожному сегменті транспортно-логістичної галузі спостерігається зростання кількості кібератак. Наприклад, громадський транспорт стикається зі зростаючим рівнем хакерських атак з боку штучного інтелекту (AI) і автоматизованих систем. Злочинні організації все частіше застосовують схеми «crime-as-a-service», за якої синдикат продає свої навички для програм-вимагачів і розподілених атак типу «DDoS» окремим особам або організаціям. За останні п'ять років у секторі громадського транспорту спостерігається стабільний приріст кількості кібератак з боку злочинних організацій. Зокрема, збої в роботі залізниці через кіберзагрози мають серйозні наслідки – від спричинення дефіциту поставок та навіть до людських жертв. У березні цього року Агентство Європейського Союзу з питань кібербезпеки (ENISA) опублікувало свій перший звіт про область кіберзагроз, присвячену транспортному сектору, яка охоплює авіаційний, залізничний, морський і автомобільний транспорт. Проміжок часу звіту був зосереджений на періоді між січнем 2021 року та жовтнем 2022 року, в результаті чого було виявлено, що атаки програм-вимагачів були найпомітнішою загрозою для зазначеного сектору, причому кількість атак зросла майже вдвічі, з 13 відсотків у 2021 році до 25 відсотків у 2022 році. Більше половини інцидентів були пов'язані з кіберзлочинцями (55 відсотків).

Простір виявлених ризиків розтягнувся від програм-вимагачів до загроз, пов'язаних із даними, націлених насамперед на IT-системи, такі як пасажирські служби, системи продажу квитків та мобільні додатки. А хактивістські групи все частіше проводять DDoS-атаки на залізничні компанії, насамперед через вторгнення Росії в Україну. Загрози, пов'язані з даними (25 відсотків) і програми-

вимагачі (45 відсотків) були найбільшими ризиками для залізниць, а DDoS-атаки траплялися найчастіше в залізничній галузі.

Для подальшого захисту залізниць у Європі ENISA розробляє нову систему сертифікації кібербезпеки, яка встановить критерії та вимоги до сертифікації ІКТ-систем як безпечних і надійних. Проблема сьогодення полягає в тому, що інформаційні системи громадського транспорту суттєво трансформуються та інтегруються у глобальні мережі, зокрема Internet. Але далеко не кожне підприємство чи організація дбають про безпеку інформації. Комплексна інформаційна система транспортного засобу сьогодення складається з багатьох компонентів, зокрема, привабливих для кіберзлочинців: валідаторів системи оплати проїзду, бортових комп'ютерів (БК) тощо. І якщо з валідаторами можливо цілком зрозуміти ризики компрометації персональних даних усіх, хто ними користувався до процесу вивантаження інформації, то без коректної роботи останніх, транспортний засіб інколи неможливо буде навіть запустити (рис. 1.1).

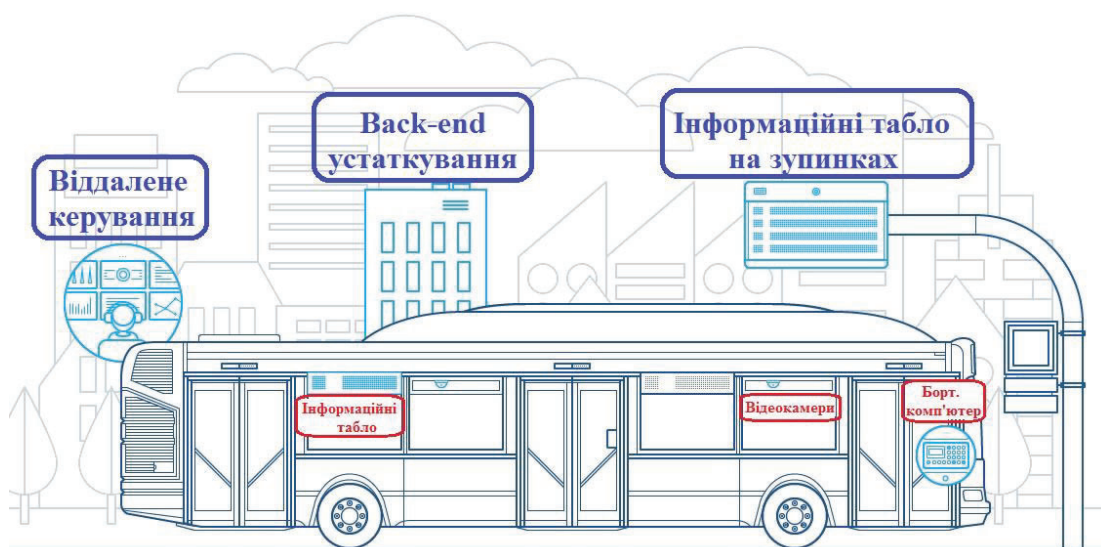


Рисунок 1.1 – Складові сучасної транспортної інформаційної системи

Хоча така інформація, як розклад, є загальнодоступною та не потребує шифрування, важливо захистити серверну систему чи систему зберігання даних, інакше зловмисник може отримати доступ до частин мережі, щоб змінити інформацію та спричинити перешкоди, показуючи на автобусних зупинках повідомлення, які можуть пропагувати екстремізм та насильство.

Ці інтерфейси стають все частішим об'єктом кібератак. Внутрішні служби безпеки та ІТ-сектор ведуть вдосконалюють свою роботу, засвоюючи новітні засоби захисту та контролю, корегуючи доступ сторонніх організацій до важливих інформаційних систем.

У тезах доповіді на тему: «Захист передачі інформації на рухомому транспорті при використанні технології LTE» до V-ої Всеукраїнської науково-практичної інтернет-конференції студентів, аспірантів та молодих вчених «Сучасні інформаційні системи та технології», було наголошено, що: «сучасні технології мережі LTE дозволяють підтримувати стабільний зв'язок навіть на високошвидкісних потягах та інших транспортних засобах» [3].

Галузь транспорту та логістики стикається з важливою різницею між великими підприємствами та дрібними транспортними компаніями. Проблеми, що виникають у великих підприємств, обумовлені потребою обслуговування великої кількості інтерфейсів і каналів для передачі трафіку з іншими організаціями. Ці дані можуть охоплювати не лише фінансові аспекти, але й включати характеристики руху та трафіку в мережі.

Розуміючи можливу загрозу розгорнутої кібератаки на сферу транспорту, яка може вплинути на світову торгівлю та економічну стабільність, регулюючі органи активізують свою роль і вимагають від компаній збільшеної захищеності їхніх мереж. Пропоновані чи вже прийняті інструменти регулювання включають Директиву ЄС щодо мережної та інформаційної безпеки (NIS), також вступають в силу стандарти CLC/TS 50701 і EN 50126 [4].

Пряме відношення до транспорту породжує питання забезпечення захисту персональних даних. Це викликає інтенсивні обговорення на міжнародному рівні, де політичні лідери різних країн намагаються знайти баланс між гарантуванням прав громадян на конфіденційність особистого життя та необхідністю посилення боротьби з тероризмом та кіберзлочинністю.

Проблеми, що виникають у громадському транспорті, включають:

- значну роз'єднаність бортових систем, що призводить до наявності кількох шлюзів LTE/SIM-карт і, відповідно, збільшеної вразливості всієї системи в цілому;
- архітектуру, спрямовану на застарілий логічний блок автомобіля (VLU), що обмежує використання новітніх технологій та надання послуг пасажиром;
- системи, які не пристосовані для віддаленого керування та вимагають присутності персоналу в Центрі управління операціями;

Найбільш типові дії злочинців, які вчиняють кібератаки на зараз, включають:

- несанкціонований доступ до сервера, на якому зберігаються конфіденційні дані;
- атаки на базу даних із інформацією про власників транспортних пластикових карт;
- здійснення атак на інтернет-сайти, бази даних та транспортні компанії різних країн;
- розповсюдження вірусів та навмисне створення перешкод у роботі мереж, що може призвести до припинення руху транспорту;
- здійснення Dos-атак (Denial of Service - "відмова в обслуговуванні") з метою порушення трафіку або взагалі його зупинення;

Впровадження сучасних систем захисту є важливим етапом у стратегії забезпечення цілісності інформації. Безпека мережі та даних є ключовим аспектом, що впливає на кінцеві цілі та авторитет організації. Ігнорування цього питання може призвести до серйозних втрат і пошкоджень корпоративного іміджу. З урахуванням зростаючого інтересу зловмисників до транспортного напрямку у галузі Інтернету речей, службам безпеки компаній слід приділяти значно більше уваги забезпеченню безпеки та конфіденційності даних користувачів.

Враховуючи вищенаведене, питання підвищення рівня захисту систем передачі трафіку з громадським транспортом є актуальним на сьогоднішній день.

1.2. Аналіз прикладів удосконалення захисту систем обміну даними з громадським транспортом

У сучасному світі обмін цифровою інформацією став невід'ємною частиною нашого життя, і це особливо стосується організацій та підприємств. Основним елементом будь-якої системи передачі трафіку є мережа.

Інтернет-мережі прийнято класифікувати на:

- приватні (або локальні);
- публічні;

Локальна комп'ютерна мережа (LAN) підприємства — це інфраструктура, яка дає змогу користувачам і пристроям отримувати доступ до мережевих послуг і ресурсів всередині одного поверху або будівлі. Ключовою задачею є створення мережі підприємства, яка об'єднує групу локальних мереж, розташованих у неподалік одна від одної. При плануванні таких мереж важливо враховувати, що вони можуть бути як малими, з одним комутатором, так і дуже обширними. Крім того, LAN використовується для з'єднання з глобальною мережею (Wide Area Network – WAN).

В свою чергу, це забезпечує:

- доступне LAN-з'єднання;
- IP-Multicast - оптимальний розподіл пакетів;
- підтримку мультимедійного обміну при налагодженому підключенні.

Застосовуючи ієрархічну модель проектування, дротова локальна мережа (LAN) підприємства може бути організована так, що різні функції розподіляються, що спрощує планування, створення та подальший контроль мережі.

LAN за рівнями ієрархії розподілена так:

- L3 – ядро;
- L2 – розподіл;
- L1 – доступ;

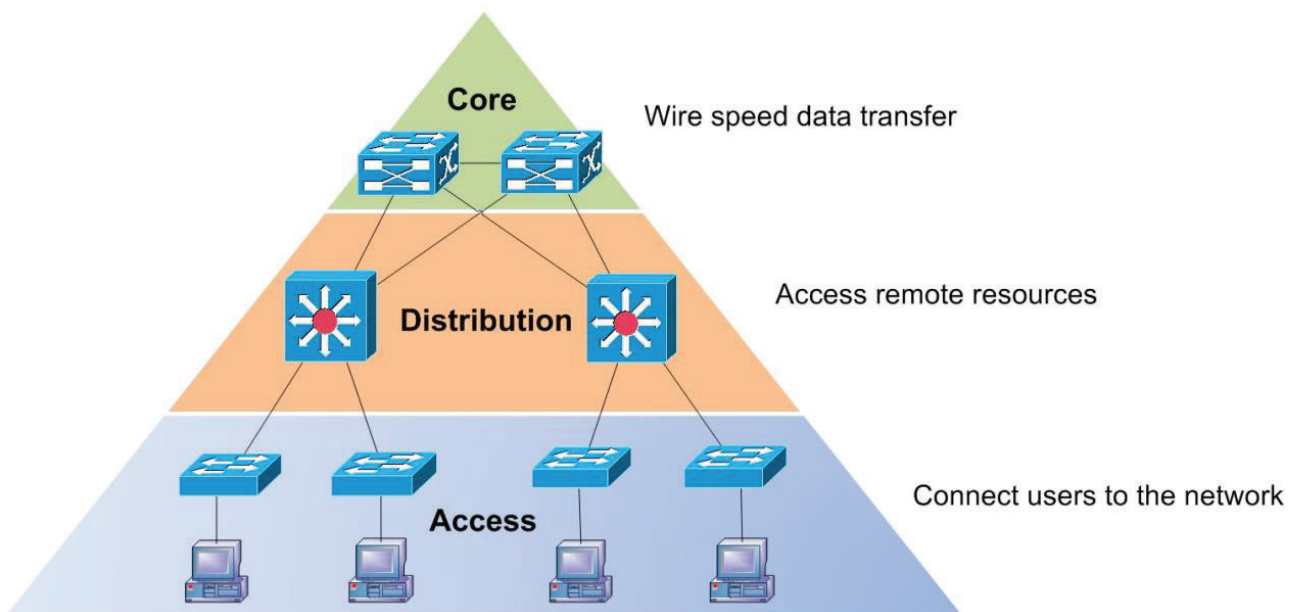


Рисунок 1.2 – Рівні ієрархії мережі

Нижче вказано ключові переваги впровадження локальних мереж у формі трирівневої архітектури:

1. Ієрархія:
 - чітко відводить роль пристроїв для різних рівнів;
 - робить розгортання легшим, що сприяє кращій експлуатації;
 - зменшує кількість помилок на кожному рівні.
2. Трансформованість - мережа може бути розширена без відчутних перепон.
3. QoS (Quality of Service) - якісно надає послуги користувачам.
4. Гнучкість – виконує функцію балансування потоку трафіку, розподіляючи його між мережевими ресурсами.

Кожен рівень володіє своїми унікальними функціональними та мережевими можливостями. Наприклад, рівень ядра встановлює зв'язок між рівнями розподілу великих локальних мереж. Рівень розподілення групує рівні доступу та забезпечує їх підключення до служб. Останній рівень, у свою чергу, забезпечує прямий доступ до мережі для кінцевих точок та користувачів [5].

Спираючись на останні технологічні тенденції, транспортні компанії включають у свої мережі технологію VPN. Цей метод передбачає створення захищеного шифрованого з'єднання між кількома мережами через публічну

мережу, таку як Інтернет. Використовуючи віртуальні канали, забезпечується захищене підключення через Інтернет від мережі організації до віддаленого вузла чи комп'ютера. Варто відзначити, що на сьогоднішній день технологія VPN використовується не тільки в мережах компаній, але й на персональних комп'ютерах та мобільних пристроях.

В багатьох сучасних організаціях встановлюють з'єднання між своїми відділами, використовуючи принципи кампусної мережі - тип комп'ютерної мережі, яка охоплює обмежену територію, таку як кампус університету, промислового підприємства, офісного комплексу або іншої подібної локації [5]. До прикладу, компанія Cisco має значний досвід у напрямі захисту потоку трафіку між організацією та її віддаленими локальними мережами. Готові рішення відрізняються від інших постачальників тим, що вони не пропонують лише точкові продукти для захисту деяких сегментів інформаційної системи, наприклад, на залізничному, авіаційному, морському, або автомобільному транспорті. Натомість, компанія постачає інтегровані додатки, які легко вбудовуються в інфраструктуру підприємства що дає більший захист від вторгнень.

Self-Defending Network - це стратегія компанії Cisco Systems, спрямована на захист бізнес-процесів у зростаючому середовищі загроз проти шкідливих програм і зловмисників, які можуть впливати на бізнес-процеси компанії як зсередини, так і ззовні. Ця стратегія передбачає використання інтегрованих заходів безпеки та автоматизованих систем для ефективного виявлення, блокування та реагування на потенційні загрози, що забезпечує надійний захист мережі та бізнес-інфраструктури компанії.

Cisco Threat Defense System (TDS) — це інтегрована система захисту від кіберзагроз, розроблена компанією Cisco. Ця система орієнтована на надійний захист мережної інфраструктури та даних від різних видів кібератак.

Основні характеристики та можливості Cisco Threat Defense System можуть включати:

- Виявлення загроз. TDS використовує різноманітні методи виявлення загроз, такі як аналіз підписів, аномалій, а також інтелектуальних алгоритмів, щоб розпізнавати та ідентифікувати потенційно небезпечні або некоректні дії в мережі.

- Блокування загроз. Після виявлення загроз TDS може автоматично вживати заходів для їх блокування або ізоляції, щоб запобігти подальшому поширенню загроз по мережі.

- Інтеграція з іншими додатками Cisco. TDS інтегрується з іншими продуктами та рішеннями Cisco, такими як мережеві брандмауери, системи ідентифікації та контролю доступу, що дозволяє створювати комплексні заходи забезпечення безпеки.

- Управління подіями та відслідковування. TDS може надавати інструменти для аналізу та відслідковування подій в мережі, щоб оператори могли швидко реагувати на потенційні загрози та вживати заходів для їх усунення.

- Широкий спектр захисту. Враховуючи постійний розвиток кіберзагроз, TDS надає можливість захищати мережу від різних видів атак, включаючи віруси, шкідливі програми, DDoS-атаки, а також дозволяє захищати критичне обладнання.

Важливо відзначити, що Cisco систематично оновлює свої продукти та впроваджує нові функції для відповіді на зростаючі вимоги щодо інформаційної безпеки.

Стратегія Cisco Secure Connectivity System використовує різні механізми автентифікації та шифрування для ефективного захисту передаваних даних. Ця стратегія забезпечує високий рівень безпеки для трафіку, який транслюється через різні канали, такі як система управління компанією, веб-сервер, голосові дані з IP-телефонії та відео з камер відеоспостереження або в рамках відеоконференцій. Цей захист застосовується як до провідних, так і до бездротових з'єднань і використовує такі технології, як IPSec, SSL, SSH, GRE та MPLS.

Прикладом готової до розгортання системи може слугувати рішення - Cisco Connected Mass Transit (CMT).

Cisco CMT - створює єдину, захищену мережу, яка охоплює транспортні засоби, back-end сервери обробки даних, зупинки громадського транспорту та обслуговуючі майданчики [6]. Це інтегроване рішення забезпечує багатосервісну, доступну, безпечну та стандартизовану інфраструктуру, спроможну підвищити якість обслуговування пасажирів та оптимізувати експлуатаційні можливості автобусів. Connected Mass Transit заміщує застарілі, патентовані та обмежені додатки. Використання CMT дозволяє зменшити загальні витрати на обслуговування системи, та зосередитись компаніям на підвищенні рівня привабливості у наданні своїх послуг, тоді як за безпеку даних користувачів подбає CMT.

Бізнес-операції включають у себе планування, комерційні обчислення, а також управління пасажирськими та фінансовими питаннями. Операції автопарку фокусуються на щоденній роботі транспортної служби в режимі реального часу, включаючи відстеження місцезнаходження транспортних засобів, контроль за пунктуальністю, відповідність маршрутам. Управління транспортними засобами орієнтоване на підвищення продуктивності автопарку, забезпечення технічного обслуговування, оновлення апаратної та програмної частини для збільшення прибутку підприємства.

Cisco Validated Designs (CVD) для громадського транспорту забезпечують основу для проєктування систем на основі перевірених та підтверджених шаблонів використання. Система включає в себе широкий набір продуктів, технологій, функцій і програм для виконання усіх поставлених завдань. Його всебічно протестовано та задокументовано інженерами Cisco та її партнерами, щоб забезпечити швидке, надійне та передбачуване розгортання.

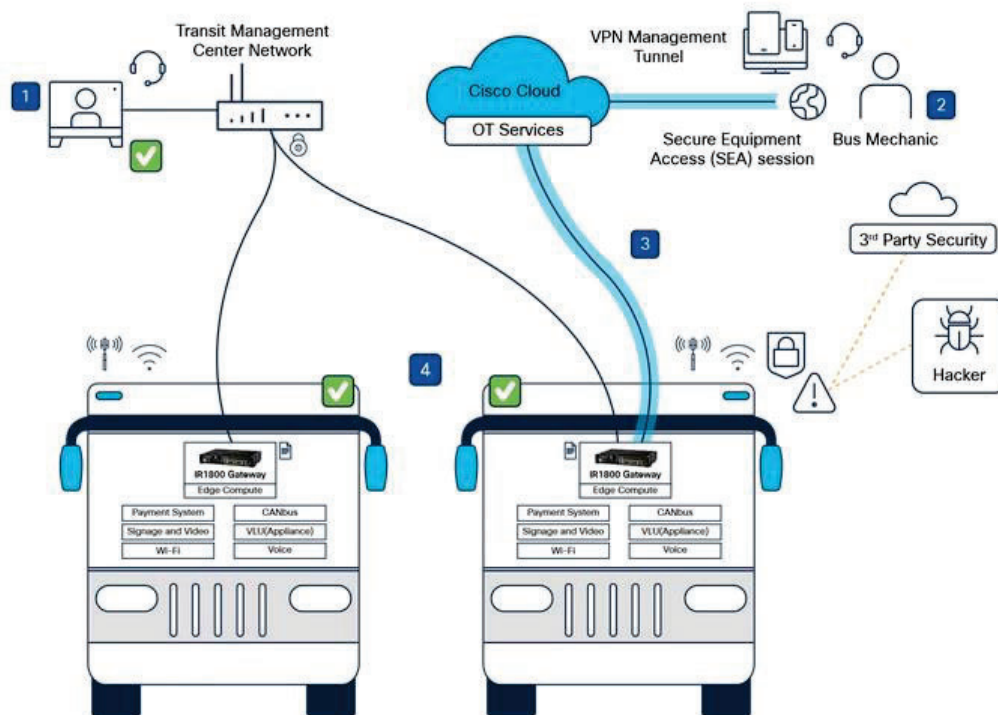


Рисунок 1.3 – Приклад простого додатку від Cisco Connected Mass Transit

Основні переваги системи включають:

- Можливість налаштовувати шаблони за допомогою зрозумілого та доступного інтерфейсу оператора, а також прив'язку шлюзів до унікального номера транспортного засобу.
- Адміністратори можуть розгорнути шлюзи через мобільний або веб-додаток.
- Єдину панель для активації/деактивації SIM-картки та управління тарифним планом за допомогою центру керування Cisco (який надається обраними постачальниками послуг).
- Забезпечення безпеки даних за допомогою сервісу Cisco Cloud.
- Потенційному кіберзлочинцю буде складніше провести кібератаку через наявність end-to-end наскрізного шифрування IPsec VPN або FlexVPN.

1.3. Дослідження складових архітектури Internet of Things (IoT)

Архітектура будь-якої інформаційної технології чи системи представляє собою комплекс взаємопов'язаних рішень, що базуються на основних принципах вибору стандартів та технологій. Ці рішення спрямовані на створення

взаємодіючих програм у ІТС і формування вимог до технологічних, технічних та телекомунікаційних засобів, а також інших засобів, необхідних для розробки та функціонування цих програм. Формування концептуального базису та визначення семантичної структури ключових розділів ІТС реалізується через розробку еталонних моделей, які утворюють ядро ІТС [7].

Наразі, створення послідовної, безсуперечної та розвиненої моделі архітектури Інтернету речей (IoT) - це завдання, що перебуває на етапі активного розвитку. Зацікавлені країни, такі як США, Німеччина, Європейський союз та інші, разом із великими міжнародними компаніями, такими як Cisco, AMD, Amazon, Microsoft та різноманітними організаціями (ITU, IEEE, ETSI, IWF, W3C), активно вносять свої моделі та приділяють значну увагу стандартизації на всіх рівнях архітектури IoT. Цей напрямок визначає майбутній розвиток технологій IoT та забезпечить взаємодію різноманітних систем у цьому просторі.

Враховуючи складність Інтернету речей (IoT), використання чотирирівневої еталонної моделі, яка рекомендується ITU-T Y.2060, дозволяє структурувати систему та визначити ключові компоненти, а також оцінити їх взаємодію [8]. Ця модель забезпечує зручний підхід до аналізу та розуміння різноманітних елементів, що входять у склад IoT, і надає фреймворк для вивчення взаємозв'язків між ними

Чотирирівнева модель описана наступним чином:

- рівень пристроїв;
- рівень мережі;
- рівень роботи з додатками та послугами;
- рівень додатку;

Порівнюючи із традиційними мережами зв'язку, управління Інтернетом речей включає наступні аспекти:

- виявлення несправностей;
- конфігураційне управління;
- облік;
- моніторинг роботи та організація безпеки.

Відповідно до рекомендацій Міжнародного союзу електрозв'язку зі стандартизації (ITU-T), Інтернет речей (IoT) представляє собою мережу пристроїв, які тісно взаємодіють із речами що навколо нас. Сенсорні та виконавчі пристрої співпрацюють із технічними об'єктами, взаємодія яких регулюється пристроями обміну трафіку або носіями інформації, що є підключеними або пов'язаними з фізичними об'єктами. Пристрої для збору даних можуть зчитувати інформацію з фізичних носіїв або записувати її на них.

Отже, IoT представляє собою сукупність фізичних або віртуальних об'єктів, які включають контролери, сенсори та виконавчі механізми, із підключенням до Інтернету. Згідно з цим, фізичний екземпляр обладнання IoT є об'єктом, що:

- має інтелектуальність, оснащений мікроконтролером та програмним забезпеченням для управління;
- може надавати інформацію чи взаємодіяти, включаючи датчик для вимірювання фізичних параметрів або виконавчий механізм, який можливо запрограмувати;
- доступний через мережу.

Формування архітектури Інтернету речей (IoT) також є предметом досліджень і розробок Всесвітнього форуму IoT (IoT World Forum, IWF). Ця щорічна подія залучає представників бізнесу, урядовців та науковців. У 2014 році керівний апарат з архітектури IWF представив свою версію ідеальної моделі IoT, яка доповнює підходи, представлені ITU-T. Порівнюючи моделі можливо помітити, що IWF приділяє увагу не лише рівням пристроїв і шлюзів, але й вищим рівням, що є важливим при розгортанні рішень проміжного програмного забезпечення та підтримки промислового Інтернету речей [10]. Дякуючи наявній моделі архітектури Інтернету речей (рис. 1.5), розробники пристроїв розуміють необхідний функціонал у сфері Інтернету речей та принципи їх взаємодії.

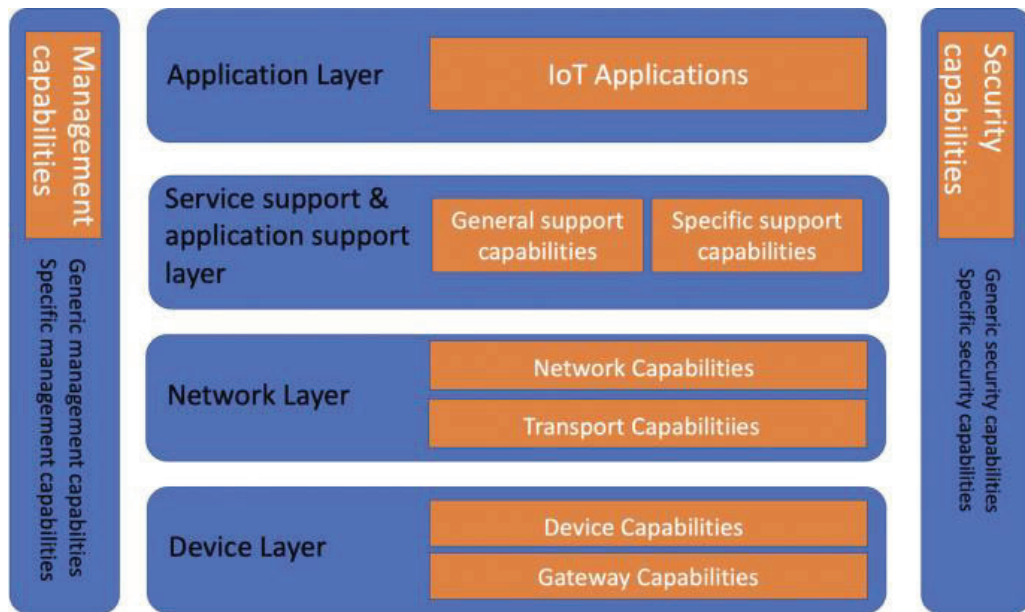


Рисунок 1.4 – Модель архітектури за рекомендацією ITU-T Y.4000/Y2060

Семирівнева модель за IoT World Forum зображена на рисунку нижче:

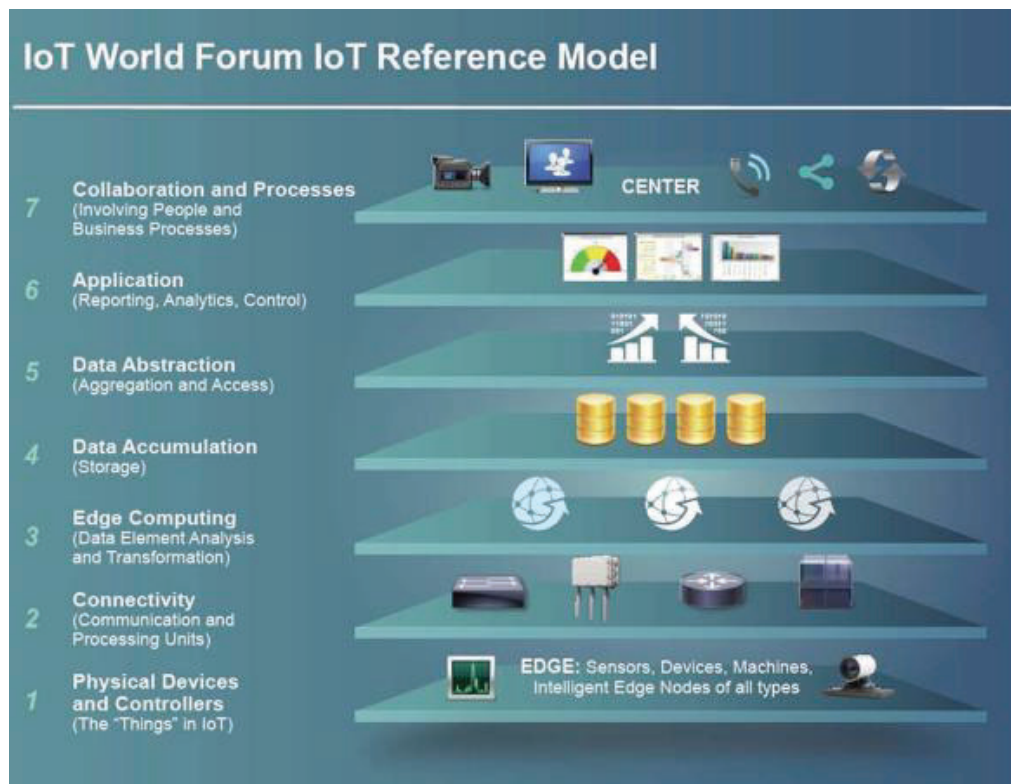


Рисунок 1.5 – Модель архітектури за рекомендацією IoT World Forum

Кожен рівень можливо описати наступним чином:

- На Рівні 1 розташовані фізичні пристрої та контролери (Physical Devices & Controllers). Елементи цього рівня – це пристрої, які взаємодіють з різними фізичними об'єктами: сенсорними або керуючими пристроями.

- Рівень 2 відповідає рівню з'єднань (Connectivity) і включає мережеві пристрої.
- Рівень 3 відповідає за аналіз та конвертацію даних, зменшуючи загальний обсяг інформації, що має зберігатись.
- Рівень 4 (Data Accumulation) - дані, отримані з пристроїв, проходять фільтрацію та обробку на рівні периферійних обчислень і зберігаються в сховищі, де вони стають доступними для подальшої обробки.
- Рівень 5 (Data Abstraction) може групувати та індексувати дані, що робить доступ додатків більш контрольованим та оптимальним.
- Рівень 6 (Application & Analytics), включає програми, які користуються даними Інтернету речей або керують web-пристроями. Програми рівня 6 взаємодіють з Рівнем 5 та даними що зберігаються.
- Рівень 7 взаємодії та процесів виник з усвідомлення того, що успіх Інтернету речей залежить від взаємодії людини з системою.

Беручи до уваги описані архітектурні моделі, характеристики будівництва кожного рівня, потужність інтеграції в існуючі системи та зростаючий попит на ринку, можна впевнено стверджувати, що роль Інтернету речей (IoT) буде лише зростати як у науковій, так і в повсякденній сферах нашого світу.

1.4. Дослідження трафіку інформаційної системи транспортного засобу

Розвиток технологій інформаційних систем тісно пов'язаний із зростанням попиту транспортних компаній у наданні більш якісних та сучасних послуг для пасажирів, зокрема різноманітних систем оплати проїзду, електронних маршрутних показників, систем точного місцезнаходження, комунікації з водіями тощо.

На даний час існує велике різноманіття виробників інформаційних систем, і кожен з них має свої власні підходи, починаючи від дизайну та необхідного функціоналу, і закінчуючи вибором стандарту комунікації. Це може бути як дротове, так і бездротове підключення. Не варто забувати і про сучасні вимоги

клієнтів таких виробників – транспортних компаній, які також мають своє бачення у процесі інтеграції систем зі своїм рухомим складом.

Загалом, транспортна інформаційна система складається з:

– «пульта керування», або цілого «Бортового комп'ютера». Його функціонал може охоплювати увесь можливий спектр роботи у сфері IoT: підключення до камер відеоспостереження, автоматизована система оплати проїзду, точне місцезнаходження транспортного засобу, керування оголошенням зупини, електронними табло, рекламними дисплеями, зв'язком водія із диспетчером, тощо. Або такий пристрій виконуватиме лише обмежені можливості з вищенаведеного переліку, все інше можуть виконувати додаткові окремі пристрої, з якими пульт може підтримувати обмін даними (рис. 1.6).



Рисунок 1.6 – Бортовий комп'ютер BUSE BS300

– електронне табло та/або інші прилади, що зображують інформацію для пасажирів. Вони можуть бути як зовнішні (зазвичай, для зображення кінцевих зупинок, куди прямує транспортний засіб), так і внутрішні (салонні, для відображення поточної зупинки, часу, тарифної зони та ін.), різні за розмірами та призначенням. Наприклад, існують табло-годинник (рис. 1.7), або табло-показчик номера графіку, за яким рухається транспортний засіб.



Рисунок 1.7 – Табло-годинник

- валідатор системи оплати проїзду. Термінал, розміщений в салоні транспортного засобу, за допомогою якого пасажери можуть сплатити за свій проїзд.
- інше додаткове обладнання. Для прикладу, система перемикання стрілок для тролейбусів або трамваїв, або пристрій для підрахунку кількості пасажирів.

Як можна побачити, функціонал та різноманітність компонентів ІС настільки великий, що їх детальний опис вийде за межі даної кваліфікаційної роботи. Ми зупинимось на аналізуванні трафіку з бортового комп'ютера однієї з популярних ІС в Україні, та дослідимо, які пакети даних надсилаються на сервер та чим цікава захоплена інформація. Для цього нам знадобляться програма-аналізатор трафіку – «Wireshark» та програмний додаток від виробника ІС для ПК.

Так як додадок ІС може використовувати декілька IP-адрес для надсилання даних та отримання запитів, для зручності створимо три базових http-сервера через командний рядок Windows, використовуючи **python 3** та адресу localhost. Для запуску http-сервера скористаємось наступною командою (рис. 1.8).

```
C:\Users\Admin>python3 -m http.server -b 127.0.0.1 1234  
Serving HTTP on 127.0.0.1 port 1234 (http://127.0.0.1:1234/) ...
```

Рисунок 1.8 – Вікно командного рядка для прослуховування на порту 1234

Заздалегідь відкриємо Wireshark та оберемо аналіз трафіку інтерфейсу “Adapter for loopback”. Нам також знадобиться «емуляція» GPS-модуля, який має бути підключений до БК, тому тут варто було б скористатись програмою для надсилання пакетів через віртуальний Serial-порт, наприклад PuTTY. Але в нашому випадку ми будемо надсилати вже заздалегідь зроблений дамп

інформації з GPS-модуля, приклад файлу з таким дампом можна побачити нижче (рис. 1.9).

```
$GPGGA,212019.000,5016.5879,N,02838.1402,E,1,3,4.34,121.6,M,28.7,M,,*5B
$GNGSA,A,2,,,,,,,,,,,,,4.45,4.34,1.00*1A
$GNGSA,A,2,76,66,77,,,,,,,,,4.45,4.34,1.00*1B
$GPGSV,1,1,00*79
$GLGSV,3,1,09,76,60,060,35,77,56,173,37,66,54,109,44,83,17,296,*62
$GLGSV,3,2,09,84,12,356,,75,08,029,,78,03,199,18,65,02,124,*61
$GLGSV,3,3,09,82,02,257,*54
$GNLL,5016.5879,N,02838.1402,E,212019.000,A,A*49
$GNRMC,212020.000,A,5016.5879,N,02838.1402,E,0.00,289.25,010623,,,A*76
$GPVTG,289.25,T,,M,0.00,N,0.00,K,A*39
$GPGGA,212020.000,5016.5879,N,02838.1402,E,1,3,4.34,121.6,M,28.7,M,,*51
$GNGSA,A,2,,,,,,,,,,,,,4.45,4.34,1.00*1A
$GNGSA,A,2,76,66,77,,,,,,,,,4.45,4.34,1.00*1B
$GPGSV,1,1,00*79
$GLGSV,3,1,09,76,60,060,35,77,56,173,37,66,54,109,44,83,17,296,*62
$GLGSV,3,2,09,84,12,356,,75,08,029,,78,03,199,18,65,02,124,*61
$GLGSV,3,3,09,82,02,257,*54
$GNLL,5016.5879,N,02838.1402,E,212020.000,A,A*43
$GNRMC,212021.000,A,5016.5879,N,02838.1402,E,0.00,289.25,010623,,,A*77
$GPVTG,289.25,T,,M,0.00,N,0.00,K,A*39
```

Рисунок 1.9 – Зразок дампу-файлу GPS за протоколом NMEA

Підготовлено все необхідне для запуску додатку БК. Запускаємо його та обираємо маршрут, нехай це буде №2 (рис. 1.10). Запам'ятаємо номер.

The screenshot shows a software window titled 'БК'. At the top, there is a button 'Проверить маршрут' (Check route) and a text field 'ЖКИ:' (JCI:) containing the text '#2->ВОКЗАЛ - СМО ЛЯНКА' followed by '-----'. Below this is a section 'Анализ GPS:' (GPS Analysis:) with several input fields and checkboxes. A checkbox is checked. The fields contain: 'Широта: 50.2765', 'Долгота: 28.6357', 'Скорость (км/ч): 0.0', 'Время: 07:12:45 07-06-2023', 'До остановки, м: 3176', and 'До ПРМЖ, м: 3103'. There is a 'Калькулятор' (Calculator) button. Below the calculator are three buttons: 'Начало остановки' (Start stop), 'Сохранить коорд.' (Save coordinates), and 'Средние:' (Averages:). To the right of these buttons are three input fields labeled 'Шир.' (Latitude), 'Долг.' (Longitude), and 'Скорость' (Speed).

Рисунок 1.10 – Вікно програми «БК» з обраним маршрутом

Маршрут обрано, а це означає що БК вже мав надіслати пакети даних до наших «серверів», переконаємось у цьому, розгорнувши Wireshark (рис. 1.11).

127.0.0.1	TCP	44 1234 → 51201 [ACK] Seq=1 Ack=1062 Win=27 Len=0
127.0.0.1	TCP	77 51201 → 1234 [PSH, ACK] Seq=1062 Ack=1 Win=32 Len=33
127.0.0.1	TCP	44 1234 → 51201 [ACK] Seq=1 Ack=1095 Win=27 Len=0
127.0.0.1	TCP	77 51201 → 1234 [PSH, ACK] Seq=1095 Ack=1 Win=32 Len=33
127.0.0.1	TCP	44 1234 → 51201 [ACK] Seq=1 Ack=1128 Win=27 Len=0
127.0.0.1	TCP	101 51201 → 1234 [PSH, ACK] Seq=1128 Ack=1 Win=32 Len=57
127.0.0.1	TCP	44 1234 → 51201 [ACK] Seq=1 Ack=1185 Win=27 Len=0
127.0.0.1	TCP	101 51201 → 1234 [PSH, ACK] Seq=1185 Ack=1 Win=32 Len=57
127.0.0.1	TCP	44 1234 → 51201 [ACK] Seq=1 Ack=1242 Win=27 Len=0
127.0.0.1	TCP	101 51201 → 1234 [PSH, ACK] Seq=1242 Ack=1 Win=32 Len=57
127.0.0.1	TCP	44 1234 → 51201 [ACK] Seq=1 Ack=1299 Win=26 Len=0
127.0.0.1	TCP	53 51223 → 1236 [PSH, ACK] Seq=64 Ack=1 Win=8192 Len=9
127.0.0.1	TCP	44 1236 → 51223 [ACK] Seq=1 Ack=73 Win=7936 Len=0

Рисунок 1.11 – Результат захоплення пакетів Wireshark на інтерфейсі loopback

Можна побачити активний обмін пакетів, значить підключення відбулось успішно і додаток надсилає усі дані до нас. Давайте уважніше дослідимо один із таких пакетів даних. Оберемо його та подивимось у вікні даних (рис. 1.12).

```

02 00 00 00 45 00 00 61 0f 80 40 00 80 06 00 00 .....E..a..@.....
7f 00 00 01 7f 00 00 01 c8 01 04 d2 a0 d0 7a c7 .....z..
1d 37 d0 41 50 18 00 20 fe 55 00 00 01 81 fd 00 ..7..AP.. ..U.....
39 00 45 01 32 2c 31 30 31 33 33 36 2c 30 37 30 9..E..2,10 1336,070
36 32 30 32 33 2c 35 30 2e 32 37 36 35 2c 32 38 62023,50 .2765,28
2e 36 33 35 37 2c 30 2e 30 30 30 30 2c 33 34 2e .6357,0. 0000,34.
37 2c 30 33 06 7,03

```

Рисунок 1.12 – Вікно з детальною інформацією про дані всередині пакету

Якщо уважно проаналізувати їх, то можна побачити, що це дані поточного маршруту та GPS-інформації (час, дата, координати, швидкість тощо).

Давайте подивимось пакети до інших двох портів, на яких встановлено з'єднання (рис. 1.13).

```

02 00 00 00 45 00 00 75 06 01 40 00 80 06 00 00 .....E..u..@.....
7f 00 00 01 7f 00 00 01 04 d4 c9 aa f9 3e cf d2 .....>..
6b a9 65 97 50 18 00 20 fe 69 00 00 32 32 30 2d k..e..P.. ..i..220-
46 69 6c 65 5a 69 6c 6c 61 20 53 65 72 76 65 72 FileZill a Server
20 31 2e 37 2e 33 0d 0a 32 32 30 20 50 6c 65 61 1.7.3.. 220 Plea
73 65 20 76 69 73 69 74 20 68 74 74 70 73 3a 2f se visit https:/
2f 66 69 6c 65 7a 69 6c 6c 61 2d 70 72 6f 6a 65 /filezil la-proje
63 74 2e 6f 72 67 2f 0d 0a ct.org/.

```

Рисунок 1.13 – Дані пакету, що надсилався на порт 1236

Даний пакет вже набагато цікавіший, наочно видно, що БК намагається підключитись до FTP-серверу, подивимось наступні пакети (рис. 1.14).

```

.....E..6..@.....      .....E..9..@.....      .....E../..@.....
.....k..e..              .....k..e..              .....k..e..
>..P.. ..*..USER      >..BP.. ..PASS      >..YP.. ..#..CWD
myLogin ..              mypassw ord..      /..

```

Рисунок 1.14 – Наступні запити БК до FTP-сервера

Отже, аналізуючи вищенаведені рисунки, можна дійти висновку що інформація, яку надсилає БК на той чи інший сервер не захищена жодним чином, особливо це стосується логіну користувача та пароля. Зловмисник може скористатись даною вразливістю та отримати доступ до серверу.

На підставі проведеного дослідження вразливостей та прогнозу подальшого розвитку у цифровізації, навіть у сфері громадського транспорту необхідний захист від можливого несанкціонованого вторгнення в систему, крадіжки персональних даних, виводу з ладу пристроїв та серверів, або навіть припинення нормальної роботи всієї системи організації.

Сформульовані такі вимоги до створення проєкту захисту системи обміну даних з громадським транспортом:

- Спершу, важливо впроваджувати технологію тунелювання трафіку (VPN), яка гарантує високий рівень шифрування трафіку, який передається між сервером організації та віддаленим транспортним засобом. При підключенні пристрою користувача, сервер доступу вимагає пройти процес ідентифікації, а потім автентифікації. Тільки після вдалого проходження обох етапів, віддалений користувач чи мережа отримають повноваження для взаємодії в мережі, що визначає процес авторизації.

- Створення захищеної внутрішньої мережі на підприємстві: гарантує, що потенційні зловмисники не матимуть можливості проникнення в мережу та завдання шкоди.

- Застосування шифрування та складних паролів є важливим елементом. Розмежування повноважень користувачів до інформації та фізичне обмеження доступу до серверів сприяє усіляким заходам безпеки.

- Важливим є постійне вдосконалення процесів автентифікації та авторизації для забезпечення максимального рівня безпеки інформації.

1.5. Постановка завдання. Технічні вимоги до проєкту

У цьому дослідженні детально аналізується питання забезпечення безпеки системи обміну даних з громадським транспортом. Узагальнюючи, важливо визначити наступні аспекти:

- Цілісний захист системи передачі трафіку: Необхідно забезпечити повноцінний захист системи передачі трафіку шляхом використання загальних функціональних цілей, тісного взаємозв'язку між складовими системи та ієрархічної структури системи управління захистом передачі інформації.

- Забезпечення комплексного контролю за безпекою інформації: підвищення рівня захищеності системи повинно включати ефективний контроль за безпекою інформації та ресурсів інформаційних систем. Такий захист має гарантувати захист інтересів учасників інформаційних відносин та убезпечувати від несанкціонованого доступу зловмисників до інформації.

- Прозорий захист засобів шифрування: Забезпечення захищеності системи обміну даними у громадському транспорті, де використовуються методи і засоби шифрування, має бути максимально прозорим для легітимного користувача. Це означає, у тому числі, уникання перешкод у роботі та забезпечення зручного доступу до даних під час роботи із системою.

1.5.1 Технічне завдання проєкту підвищення захищеності системи обміну даними з громадським транспортом

1. ЗАГАЛЬНІ ВІДОМОСТІ

1.1. Повне найменування та умовне позначення

Повне найменування: Захищена мережа потоку даних ДП «Альфа-Т».

1.2. Шифр теми

Шифр теми: "ЗМПД-РТ-ДПАТ"

1.3. Найменування підприємства-розробника ТЗ

Розробник: ТОВ «Нові технології». Юридична адреса: Україна, 10001, м. Житомир, вул. Київська, 1-А. Фактична адреса: Україна, 10001, м. Житомир, вул. Київська, 1-А, оф. 4. Тел. +38(0412)44-44-01. Код ЄДРПОУ: 12345689.

1.4. Найменування замовника

Замовник: Державне підприємство «Альфа-Т». Юридична адреса: Україна, 01604, м. Київ, вул. Гарматна, буд. 12. Тел. +38(044)544-01-02. Код ЄДРПОУ: 03328320.

Власник (розпорядник) ЗМПД: Державне підприємство «МТА-Транс». Юридична адреса: Україна, 01604, м. Київ, вул. Гарматна, буд. 12.

1.5. Підстави для розробки ТЗ

Розробка даного ТЗ здійснюється на підставі Договору від 01 травня 2023 року № 123-45 (далі – Договір) між ТОВ «Нові технології» та Державне підприємство «Альфа-Т» (далі – Сторони).

1.6. Планові терміни початку й закінчення роботи з проектування ТЗ

У розділі Додатку 2 до Договору («Календарний план на проектування технічного завдання») визначені терміни (строки) надання послуг.

Початок робіт: дата укладання Договору Сторонами.

Закінчення робіт: дата підписання Акту приймання-передачі наданих послуг.

1.7. Відомості про джерела і порядок фінансування робіт

Джерелом фінансування робіт з проектування ТЗ на ЗМПД є кошти загального фонду Державного бюджету України.

1.8. Порядок подання результатів робіт

Передача оформленої у встановленому порядку документації, як за окремими етапами Договору так і по роботі в цілому, здійснюється за супроводжувальними документами Розробника відповідно до умов Договору.

Порядок оформлення та подання результатів роботи з проектування технічного завдання повинен відповідати вимогам: ДСТУ 3396.1-96, РД 50-34.698-90, НД ТЗІ 2.5-004-99, НД ТЗІ 3.7-003-05.

Роботи з побудови ЗМПД вважаються закінченими за умов підписання Акту приймання-передачі наданих послуг при додачі до нього звітних документів, передбачених ТЗ на ЗМПД.

2. ПРИЗНАЧЕННЯ ТА МЕТА СТВОРЕННЯ ЗМПД

2.1. Мета створення ЗМПД

Метою створення ЗМПД РТ ДПМТАТ є забезпечення інформаційного обміну та захисту інформації, що передається між транспортними засобами та Підприємством, від НСД, несанкціонованої модифікації та знищення, а також забезпечення доступності зазначеної інформації для авторизованих користувачів.

При розробці та впровадженні ЗМПД повинні бути враховані існуючі тенденції розвитку захищених інформаційних технологій, розробки відповідних засобів захисту інформації, розвитку державної нормативної бази з технічного захисту інформації, зокрема:

- каналоутворче обладнання ЗМПД повинно мати діючі експертні висновки Державної служби спеціального зв'язку та захисту інформації щодо відповідності вимогам нормативних документів з питань криптографічного захисту інформації в Україні;
- - каналоутворче обладнання ЗМПД повинно мати діючі експертні висновки, зареєстровані в Адміністрації Державної служби спеціального зв'язку та захисту інформації України, щодо відповідності вимогам нормативних документів системи технічного захисту інформації в Україні.

2.2. Функціональне призначення ЗМПД

ЗМПД призначена для:

- швидкого, надійного та безперебійного обміну трафіку між РТ ДПАТ;
- реалізації політики безпеки інформації, заданої в ЗМПД;
- забезпечення розмежування повноважень користувачів до об'єктів, що містять інформацію, яка підлягає захисту, у відповідності до прийнятої політики безпеки;
- забезпечення централізованого керування та моніторингу політик безпеки в єдиній системі з можливістю делегування прав щодо налаштування та моніторингу шлюзів безпеки на рівень адміністраторів підрозділів;

- забезпечення цілісності та доступності відкритої інформації, що передається між РТ ДПАТ, а також конфіденційності та цілісності конфіденційної (персональних даних) та технологічної інформації;
- забезпечення захисту інформації від внесення в ЗМПД шкідливого програмного коду (вірусів, троянських програм та ін.);
- захист від мережесих атак (кібератак), в тому числі від DOS-атак, спроб блокування функціонування ЗМПД;
- забезпечення доступності інформації та функцій ЗМПД для її користувачів, а також відмовостійкості компонентів ЗМПД;
- забезпечення спостереження за діями користувачів та персоналу ЗМПД, реєстрації, збору, зберігання, обробки, даних про події, які мають відношення до безпеки інформації, сповіщення адміністратора безпеки про такі події;
- реалізації функцій КЗІ, що передається каналами зв'язку між компонентами ЗМПД та іншими елементами, що беруть участь в обробці інформації;
- створення механізму та умов оперативного реагування на зовнішні та внутрішні загрози з метою забезпечення безпеки інформації та оперативного сповіщення адміністратора безпеки про факти НСД до інформації;
- ефективного попередження, своєчасного виявлення та знешкодження загроз для ресурсів ЗМПД, причин та умов, які спричиняють або можуть призвести до порушення її нормального функціонування;
- забезпечення працездатності та оперативного відновлення ЗМПД при виникненні позаштатних чи аварійних ситуацій;
- забезпечення захисту обчислювальних ресурсів та компонентів ЗМПД від атак та НСД з боку мережі Інтернет (в тому числі унеможливлення попадання шкідливого ПЗ до ЗМПД).

3. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ЗМПД ТА УМОВ ЇЇ ФУНКЦІОНУВАННЯ

3.1. Загальна характеристика ЗМПД

Захищена мережа потоку даних ДП «Альфа-Т» являє собою територіально розгалужене середовище обміну трафіку та каналоутворюючого обладнання з функціоналом захисту інформації.

Архітектурно ЗМПД складається з трьох рівнів:

- рівень центру управління (адміністрації);
- рівень центру обробки даних (ЦОД);
- рівень транспортних засобів;

Пропускна здатність каналів зв'язку коливається в межах від 10 Мбіт/с до 20 Мбіт/с на рівні транспортних засобів, від 500 Мбіт до 2 Гбіт/с на рівні ЦОД, а також від 1 Гбіт/с на рівні центру управління.

Для маршрутизації трафіку між вузлами використовуються протоколи статичної та динамічної (OSPF) маршрутизації. Для підключення до обладнання оператора трафіку мережі використовуються як оптичні, так і мідні лінки.

В якості комутаційного обладнання ЛОМ центрального вузла з підрозділами використовується обладнання Cisco, HP, 3COM тощо.

Доступ до ресурсів мережі Інтернет організовано централізовано на рівні центрального вузла.

3.2. Умови функціонування ЗМПД

ЗМПД працює в безперервному режимі (цілодобово, протягом семи днів на тиждень) за винятком часу проведення планових профілактичних робіт та позапланових технічних перерв.

ЗМПД повинна забезпечувати цілодобову передачу даних. Тимчасове припинення роботи ЗМПД для проведення технічних профілактичних робіт можливе лише у неробочий час надання технічної підтримки.

Повідомлення про час і терміни проведення планових профілактичних робіт, під час яких не здійснюється робота ЗМПД, надсилаються відповідним

адміністраторам ЗМПД для розміщення не пізніше ніж за 2 (два) дні до дати початку проведення таких робіт.

Згідно з НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» ЗМПД відноситься до АС класу «З».

4. ВИМОГИ ДО ЗМПД

4.1. Вимоги до проектування

Підхід до проектування ЗМПД визначається наступними критеріями побудови мереж передачі інформації, а саме:

- логічна модель комунікаційного середовища повинна ґрунтуватися на семирівневій моделі 7498 ISO;
- продуктивність мережної інфраструктури має забезпечити безперебійну роботу кінцевих застосувань;
- дотримання ієрархічного принципу побудови мережі (визначення рівнів магістралі («ядра») мережі, мережі розподілення та мережі доступу);
- рішення повинно забезпечити логічне розподілення корпоративної мережі на декілька підсистем, кожна з яких виконує окремі функції: (транспортну, комутації та маршрутизації, управління, захисту);
- доступність мережі має забезпечуватись 24 години на добу 365 днів на рік;
- забезпечення прозорого керування та адміністрування мережею;
- забезпечення кількісного та якісного розвитку мережі без змін її архітектури;
- стійкість до дестабілізуючих чинників та надійність;
- здатність до розширення мережі (масштабованість);
- мережа повинна володіти достатніми ресурсами для передачі інформації зі швидкостями, що забезпечать якісну роботу кінцевих застосувань (доступність).

При створенні ЗМПД необхідно також взяти до уваги наступні вимоги, а саме:

- наявність на рівні центрального вузла двох каналів передачі трафіку від різних провайдерів, що надають послуги з доступу до мережі Інтернет та мають чинні атестати відповідності системи захисту ЗВІД, для забезпечення відмовостійкості роботи;
- переключення з основного на резервний канал передачі трафіку у разі проблем з основним каналом має відбуватися автоматично;
- ЗМПД, що створюється, повинна забезпечувати шифрування даних, які передаються через ЗМПД, за допомогою сучасних алгоритмів криптографічного захисту інформації з достатньою стійкістю та відповідністю вимогам нормативних документів з питань криптографічного захисту інформації в Україні.
- усі маршрутизатори мають включати функціонал QoS або надання пріоритету пакетам певних типів;

4.2. Технічні вимоги до обладнання ЗМПД

4.2.1 Вимоги до кластеру маршрутизаторів центрального вузла

Кластер маршрутизаторів центрального вузла призначений для маршрутизації мережевого трафіку ЗМПД організації VPN-тунелів, фільтрації мережевого трафіку між центральним та іншими вузлами і має відповідати наступним характеристикам:

Таблиця 1

Вимоги до кластеру маршрутизаторів центрального вузла

Вимога	Параметри
Можливість монтажу в стійку	Обов'язково
Кількість блоків живлення з можливістю гарячої заміни	Не менше 2-х
Тип накопичувачів	Не гірше CF
Кількість накопичувачів з можливістю гарячої заміни (для кожного пристрою)	Не менше 2-х
Об'єм кожного накопичувача	Не менше 4 ГБ
Об'єм оперативної пам'яті	Не менше 8 ГБ
Робоча напруга блоків живлення	220В +/- 5%
Робоча частота блоків живлення	50 Гц +/- 5%
Підтримка протоколів побудови VPN мереж	IPSec, IKE
Підтримка динамічної конфігурації IPsec VPN в топології "зірка/star" або "кожний з кожним/Mesh" без статичної конфігурації кожного тунелю	Обов'язково
Підтримка протоколів шифрування	AES-128, AES-256

Швидкість шифрування AES-128 без втрат пакетів	Не менше 10 Гбіт/с
Кількість одночасних IPsec VPN з'єднань	Не менше 300
Протокол динамічної маршрутизації	OSPF
Підключення до ЛОМ та каналів оператора (вбудовані або встановлені модулі)	Ethernet 1 Гбіт/с не менше 3 шт.
Пропускна спроможність міжмережевого екрану	Не менше 20 Гбіт/с
Пропускна спроможність IPS	Не менше 2 Гбіт/с
Максимальна кількість нових з'єднань за секунду	Не менше 105000
Підтримка функції Stateful inspection міжмережевого екрану	Обов'язково
Підтримка можливості створення кластеру високої доступності з 2х пристроїв	Обов'язково
Функції інтеграції з Microsoft Active Directory	Обов'язково
Функції ідентифікації термінальних користувачів Microsoft RDP	Обов'язково
Функціонал попередження вторгнення (IPS)	Обов'язково
Функціонал потокового антивірусу	Обов'язково
Функціонал фільтрації по типу застосувань	Обов'язково
Функції ідентифікації застосувань у трафіку	Обов'язково
Функціонал фільтрації по URL	Обов'язково
Кількість сигнатур застосувань	Не менш 7000
Функціонал інспекції шифрованого HTTPS трафіку	Обов'язково
Функціонал інспекції шифрованого HTTPS трафіку з ключем більше 2048	Обов'язково
Підтримка SSL VPN, для віддаленого доступу PC на базі ОС Windows, Mac OS, Linux	Обов'язково
Захист від загроз «нульового дня»	можливість застосування за рахунок розширення ліцензії

4.2.2 Вимоги до маршрутизаторів рівня Адміністрації

Таблиця 2

Вимоги до маршрутизаторів рівня Адміністрації

Вимога	Параметри
Можливість монтажу в стійку	Обов'язково
Об'єм накопичувача	Не менше 4 ГБ
Об'єм оперативної пам'яті	Не менше 8 ГБ
Робоча напруга блоків живлення	220В +/- 5%
Робоча частота блоків живлення	50 Гц +/- 5%
Підтримка протоколів побудови VPN мереж	IPsec, IKE
Підтримка протоколів шифрування	AES-128, AES-256
Пропускна здатність міжмережевого екрану	Не менше 5 Гбіт/с
Швидкість шифрування AES-128 без втрат пакетів	Не менше 1 Гбіт/с
Протокол динамічної маршрутизації	OSPF
Підключення до ЛОМ та каналів оператора (вбудовані або встановлені модулі)	Ethernet 1 Гбіт/с не менше 3 шт.
Підтримка кластеризації	Обов'язково

Підтримка функції Stateful inspection міжмережевого екрану	Обов'язково
Функції інтеграції з Microsoft Active Directory	Обов'язково
Функції ідентифікації термінальних користувачів Microsoft RDP	Обов'язково
Функціонал попередження вторгнення (IPS)	Обов'язково
Функціонал потокового антивірусу	Обов'язково
Функціонал фільтрації по типу застосувань	Обов'язково
Функції ідентифікації застосувань у трафіку	Обов'язково
Функціонал фільтрації по URL	Обов'язково
Кількість сигнатур застосувань	Не менш 7000
Функціонал інспекції шифрованого HTTPS трафіку	Обов'язково
Функціонал інспекції шифрованого HTTPS трафіку з ключем більше 2048	Обов'язково
Підтримка SSL VPN, для віддаленого доступу PC на базі ОС Windows, Mac OS, Linux	Обов'язково
Захист від загроз «нульового дня»	можливість застосування за рахунок розширення ліцензії

Необхідно передбачити наявність щонайменше одного резервного комплекту обладнання кластеру з метою оперативної заміни у разі виходу з ладу обладнання.

4.2.3 Вимоги до маршрутизаторів рівня транспортних засобів

Маршрутизатор рівня транспортного засобу призначений для маршрутизації мережевого трафіку ЗМПД, організації VPN-тунелів, фільтрації мережевого трафіку на рівні свого вузла і повинен відповідати наступним характеристикам.

Таблиця 3

Вимоги до маршрутизаторів рівня транспортних засобів

Вимога	Параметри
Підтримка протоколів побудови VPN мереж	IPsec, IKE
Підтримка протоколів шифрування	AES-128, AES-256
Швидкість шифрування AES-128 без втрат пакетів	Не менше 20 Мбіт/с
Протокол динамічної маршрутизації	OSPF
Підтримка міжмережевого екрану	Так
Підтримка кластеризації	Обов'язково
Підтримка функції Stateful inspection міжмережевого екрану	Обов'язково
Пропускна здатність міжмережевого екрану	Не менше 100 Мбіт/с
Підключення до локальної мережі	Ethernet
Підключення до каналу передачі трафіку 1	Wireless LAN
Додаткові порти локальної мережі (вбудовані або встановлені модулі)	Не менше 4 шт.
Функції інтеграції з Microsoft Active Directory	Обов'язково

Функції ідентифікації термінальних користувачів Microsoft RDP	Обов'язково
Функціонал попередження вторгнення (IPS)	Обов'язково
Функціонал потокового антивірусу	Обов'язково
Функціонал фільтрації по типу застосувань	Обов'язково
Функції ідентифікації застосувань у трафіку	Обов'язково
Функціонал фільтрації по URL	Обов'язково
Функціонал інспекції шифрованого HTTPS трафіку	Обов'язково
Функціонал інспекції шифрованого HTTPS трафіку з ключем більше 2048	Обов'язково
Захист від загроз «нульового дня»	можливість застосування за рахунок розширення ліцензії

Додатково необхідно передбачити наявність щонайменше 10-ти резервних пристроїв з метою оперативної заміни у разі виходу з ладу обладнання.

4.2.3 Вимоги до програмного забезпечення керування ЗМПД

Таблиця 4

Вимоги до програмного забезпечення керування ЗМПД

Вимога	Параметри
Наявність засобів аналізу, контролю, а також засобів моніторингу і аналізу трафіка мережі в режимі реального часу	Обов'язково
Графічне зображення пристроїв, окремих портів та їх поточного стану	Обов'язково
Перегляд журналу подій інформаційної безпеки з можливістю створення фільтрів по подіям інформаційної безпеки	Обов'язково
Наявність адміністраторів різного рівня доступу, з можливістю обмеження прав кожного облікового запису до різних підсистем адміністрування	Обов'язково
Можливість одночасного доступу адміністраторів системи в режимі редагування з метою здійснення змін в різних політиках	Обов'язково
Вбудований функціонал інфраструктури відкритих ключів згідно стандарту x.509	Обов'язково
Підтримка сторонніх центрів сертифікації	Обов'язково
Єдина консоль керування міжмережевими екранами, VPN, IPS, потокового антивірусу, фільтрації по URL	Обов'язково
Функціонал централізованого керування ліцензіями	Обов'язково
Можливість адміністрування окремих пристроїв мережі	Обов'язково
Можливість адміністрування груп пристроїв мережі на основі профілів безпеки	Обов'язково
Можливість створення резервних копій попередніх конфігурацій мережних пристроїв, перенесення резервних копій на зовнішні носії та повернення, до попередньої конфігурації	Обов'язково
Наявність механізму побудови звітів про події інформаційної безпеки з можливістю автоматичної розсилки відповідним адміністраторам	Обов'язково

4.3. Вимоги до мережевого захисту інформації ЗМПД

Засоби мережевого захисту повинні розміщуватись на межі підсистем і забезпечувати виконання наступних функцій:

- фільтрація та аналіз трафіку на рівнях L3-L7 моделі OSI;
- розмежування доступу між ЛОМ вузлів та зовнішніми мережами (в т.ч. мережею оператора передачі трафіку);
- інспекцію мережевого трафіку та блокування пакетів або сесій, що є підозрілими;
- маскування топології і мережевих адрес ЗМПД від публічного перегляду;
- забезпечення проходження між вузлами ЗМПД лише дозволених інформаційних потоків згідно визначених протоколів;
- виявляти комп'ютерні атаки і несанкціоновану мережеву активність;
- здійснювати фільтрацію та аналіз мережевого трафіку за протоколами, портами і IP-адресами відправника й одержувача;
- забезпечувати завершення з'єднання з вузлом, у разі атаки;
- здійснювати протоколювання (реєстрацію) подій, що мають відношення до безпеки.

4.4. Вимоги щодо забезпечення криптографічного захисту

З метою забезпечення конфіденційності та цілісності об'єктів захисту ЗМПД, які передаються через незахищене середовище між вузлами ЗМПД, мають використовуватися криптографічні способи захисту. Засоби КЗІ повинні мати чинний позитивний експертний висновок або сертифікат відповідності за результатами державної експертизи в сфері КЗІ Адміністрації Держспецзв'язку.

В ЗМПД достатньо використовувати криптографічні засоби захисту, можливість використання яких дозволено цими експертними висновками для КЗІ з обмеженим доступом (крім службової інформації та інформації, що становить державну таємницю) та відкритої інформації, вимоги щодо захисту якої встановлено законом.

4.5. Вимоги до адміністрування ЗМПД

Керування засобами захисту та мережевим обладнанням, що відноситься до ЗМПД, а також моніторинг їх стану здійснюється з використанням локального або віддаленого доступу до відповідного обладнання.

У випадку здійснення віддаленого адміністрування повинні використовуватись криптографічні засоби захисту, які повинні мати діючий експертний висновок або сертифікат відповідності за результатами державної експертизи в сфері КЗІ.

В ЗМПД повинен бути реалізований адміністративний принцип керування доступом. Потоки інформації всередині ЗМПД встановлюються адміністраторами ЗМПД і не можуть бути змінені іншими користувачами.

5. ВИМОГИ ДО СКЛАДУ ПРОЕКТНОЇ ТА ЕКСПЛУАТАЦІЙНОЇ ДОКУМЕНТАЦІЇ

Комплект проектної документації на ЗМПД повинен повною мірою визначати склад та структуру ЗМПД, містити докладний опис механізмів мережної взаємодії та захисту інформації, реалізованих програмно-апаратними засобами, та організаційних заходів.

Мінімальний перелік проектної та експлуатаційної документації, яка повинна бути розроблена при проектуванні ЗМПД, наступний:

- Відомість технічного (техноробочого) проекту;
- Пояснювальна записка до технічного (техноробочого) проекту;
- Функціональна схема ЗМПД;
- Специфікації обладнання з прив'язкою до місць розміщення;
- Інструкції адміністраторів ЗМПД та користувачів (за необхідності);
- Конфігурації обладнання;
- Програма та методика попередніх випробувань;
- Акти введення в дослідну та/або промислову експлуатацію.

Повний перелік проектної та експлуатаційної документації уточнюється на етапі технічного проектування.

6. ЕТАПИ ВИКОНАННЯ РОБІТ

При побудові ЗМПД повинні дотримуватися вимоги до обсягу і послідовності виконуваних робіт відповідно до Постанови Кабінету Міністрів України від 4 лютого 1998 р. №121 «Про етапність робіт у процесі проектування, впровадження й експлуатації систем і засобі автоматизованої обробки і передачі інформації».

Основні етапи робіт з побудови ЗМПД наведено в таблиці 6.1

Етапи побудови ЗМПД мають визначатися в Календарному плані робіт з побудови ЗМПД, який має бути невід'ємним додатком до Договору між Замовником та Виконавцем комплексу робіт з проектування, монтажу, пусконаладження та введення в експлуатацію ЗМПД, що створюється.

Таблиця 5

Основні типові етапи виконання робіт

Етап	Зміст робіт
1. Розробка технічного (техноробочого) проекту ЗМПД	1.1 Розробка пояснювальної записки до технічного (техноробочого) проекту 1.2 Розробка функціональної схеми ЗМПД, детальних специфікацій та схем розміщення обладнання
2. Постачання обладнання	2.1 Закупівля та постачання Замовнику обладнання
3. Попередні випробування	3.1 Розробка програми та методики проведення попередніх перевірок 3.2 Проведення попередніх перевірок 3.3 Оформлення результатів попередніх випробувань та акту про введення ЗМПД до дослідної експлуатації
4. Дослідна експлуатація	4.1 Підготовка персоналу 4.2 Пусконаладжувальні роботи 4.3 Проведення дослідної експлуатації, доопрацювання складових частин ЗМПД та корегування робочої документації за результатами дослідної експлуатації 4.4 Проведення приймальних випробувань та акт впровадження ЗМПД в промислову експлуатацію

7. ПОРЯДОК ВНЕСЕННЯ ЗМІН ТА ДОПОВНЕНЬ

Зміни затвердженого ТЗ на побудову ЗМПД, необхідність внесення яких виявлена в процесі виконання робіт, оформляється окремим доповненням, яке погоджується і затверджується в тому ж порядку і на тому ж рівні, що і основний документ.

Доповнення до даного ТЗ складається з вступної частини та розділів (підрозділів), до яких вносяться зміни. У вступній частині зазначається причина випуску доповнення. У розділах (підрозділах), до яких вносяться зміни, наводяться їх номери та зміст змін, а також номери та зміст нових пунктів та/чи таких, що скасовуються.

8. ПОРЯДОК ПРОВЕДЕННЯ ВИПРОБУВАНЬ ЗМПД

Об'єктом випробувань є ЗМПД РТ ДПАТ. Метою випробувань є встановлення відповідності досягнутих в ЗМПД показників щодо обміну та захисту інформації вимогам цього ТЗ та визначення її готовності до експлуатації.

Передбачається проведення таких видів випробувань: попередні випробування, дослідна експлуатація, приймальні випробування. Для проведення випробувань їх виконавцем повинна бути розроблена та затверджена у встановленому порядку відповідна програма та методика випробувань. Обсяг випробувань повинен забезпечити вичерпну оцінку усіх показників функціонування ЗМПД.

Випробування проводяться за умови наявності усієї сукупності апаратних та програмних засобів ЗМПД, а також проектної та експлуатаційної документації на ЗМПД, що створюється згідно з вимогами цього ТЗ.

Для проведення попередніх випробувань, дослідної експлуатації та приймальних випробувань призначається комісія.

За результатами дослідної експлуатації, усунення недоліків у випадку їх наявності та коригування проектної та експлуатаційної документації оформлюється акт про завершення дослідної експлуатації, який повинен містити висновки щодо можливості проведення приймальних випробувань та впровадження ЗМПД в промислову експлуатацію.

9. ВИМОГИ ІЗ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ПРИ ВИКОНАННІ РОБІТ

Перелік осіб, які можуть бути ознайомлені з матеріалами проектної та експлуатаційної документації ЗМПД, визначається замовником та розробником.

Порядок доступу цих осіб до матеріалів установлюється відповідно до діючих нормативних документів України.

Висновки до розділу 1

У цьому розділі виконано аналітичну та дослідницьку роботи, оцінивши актуальність теми дослідження та розглянувши сучасні види загроз. Проаналізовано наявні засоби захисту потоку трафіку з громадським транспортом. Проведено тестування на вразливості пристрою інформаційної системи шляхом сканування пакетів через програму Wireshark та виявлено критичні недоліки безпеки даних що передаються. Розглянуто архітектуру Інтернету речей (IoT).

Сформульовано конкретні вимоги до систем захисту передачі трафіку, серед яких важливі такі аспекти як:

- Використання мережевого брандмауера (Network Firewall);
- Застосування програмних та апаратних інструментів для сканування мережі на предмет небезпечного програмного забезпечення;
- Забезпечення засобами захисту від витоку даних, що передаються.

Також визначено конкретний перелік вимог до підвищення рівня захищеності системи передачі трафіку з громадським транспортом.

РОЗДІЛ 2. РОЗРОБКА ПРОЄКТУ ЗАХИЩЕНОСТІ СИСТЕМИ ОБМІНУ ДАНИМИ З ГРОМАДСЬКИМ ТРАНСПОРТОМ

2.1. Розробка структурної схеми мережі проєкту системи

При плануванні мережі, інфраструктура може базуватися на різних архітектурних шаблонах [25], що визначає обсяг впливу на безпеку мережі і розрізняє між уразливою та захищеною мережею. Оскільки архітектура та топологія є ключовими принципами безпеки мережі, промислові стандарти безпеки, зокрема ISO/IEC 62443, були розроблені для створення мереж, що надає адміністраторам обладнання та інтеграторам систем чіткий напрямок для створення великих та ефективних мережевих структур.

Один з ключових принципів при проектуванні мереж – розподіл на зони та канали. Згідно з цим принципом, промислова мережа розділяється на функціональні зони. Трафік між такими зонами передається за налаштованими правилами.

З організаційної точки зору, підприємство поділяється на кілька будівель, включаючи будівлю центру обробки даних та ще дві офісні споруди. Крім цього, існує майданчик для зберігання транспорту, де встановлено мережеві пристрої, для забезпечення зв'язку та передачі інформації до серверів обробки. Структурні підрозділи організації відповідають за керування процесами обробки інформації що надходить (рис. 2.1).

При реалізації системи зон та каналів важливо враховувати кілька аспектів. Необхідно вживати технічні заходи для належного налаштування контролю переходу між зонами. Зазвичай, найбільш ефективними методами залишаються використання файерволів та списків контролю доступу для забезпечення потрібного рівня безпеки.

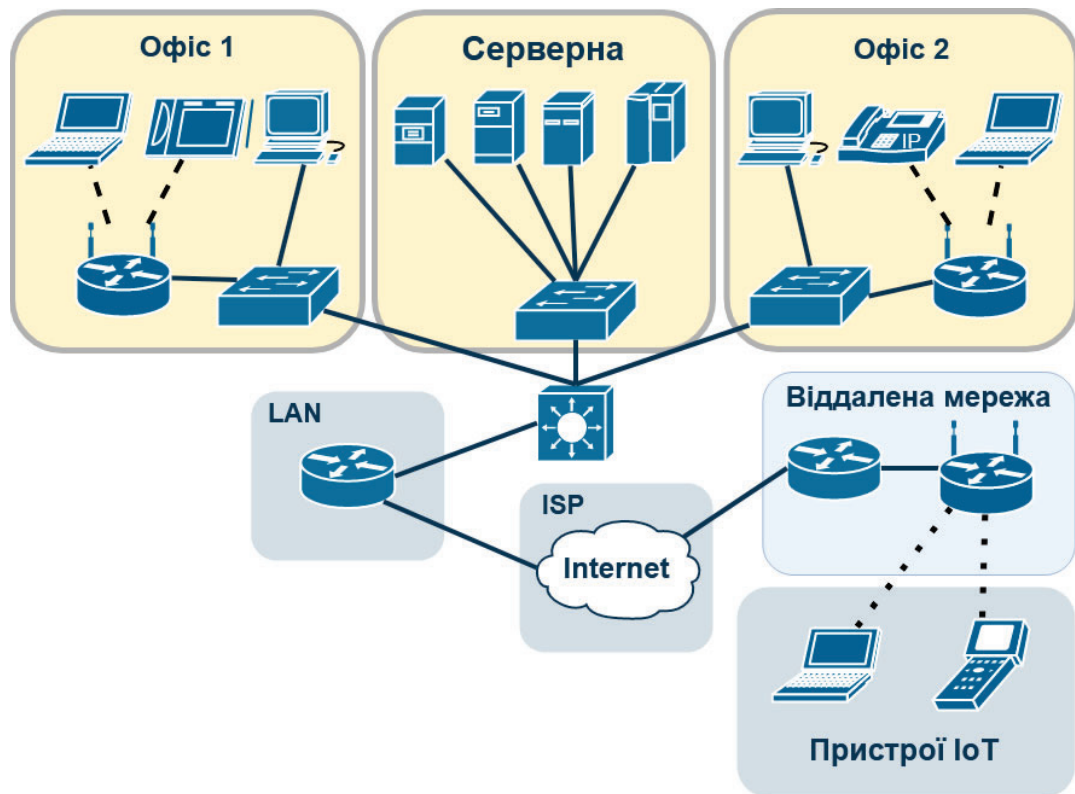


Рисунок 2.1 – Структурна схема проекту системи

У межах кожної зони також встановлені обмеження трафіку від пристроїв за допомогою Ethernet-комутаторів, що використовують ACL-списки. Крім того, крім розділу мереж на зони, важливо забезпечити захист доступу до конкретних зон. Найкращим варіантом для цього може бути технологія, наприклад, IEEE 802.1X та RADIUS - як протокол автентифікації.

Мережева сегментація на індивідуальні зони виконується за допомогою файрволів або шлюзів на рівні застосунків, після визначення правил фільтрації пакетів. Заборонений трафік буде блокований фаєрволом та списками контролю доступу, проходячи через фільтрацію трафіку, що ґрунтується на аналізі метаданих з'єднання (IP-адреси, MAC-адреси, номер порту, прапорці протоколу).

Розглянемо шаблони та анти-шаблони проектування розподільних мереж. Мережеві екрани можна налаштовувати в різних місцях в мережі. Розташування визначає, наскільки система, яка захищена файрволом, може протистояти загрозам в конкретній точці. Розглянемо приклади анти-шаблонів для дизайну мереж.

Анти-шаблони проєктування мереж

Назва шаблону	Відомі властивості
Плоска мережа	Відсутність розподілу на зони характеризується тим, що всі пристрої розташовані в межах однієї великої зони. Це зручно для будь-яких мереж завдяки відсутності обмежень у з'єднаннях між пристроями. Однак це може призвести до повної втрати контролю над мережею під час хакерської атаки та надає обмежені можливості забезпечення додаткового захисту вразливим об'єктам. Такий шаблон не може забезпечити ефективний захист мережі.
Екранований хост	Використовується фаєрвол для проєктування окремих зон, проте існує вразливість для проходження міжзонального з'єднання через цей фаєрвол. Це зазвичай відбувається при наданні послуг хостами однієї зони хостам, які розташовані в іншій.

Далі представлено приклад стосовно другого анти-шаблону (рис. 2.2)

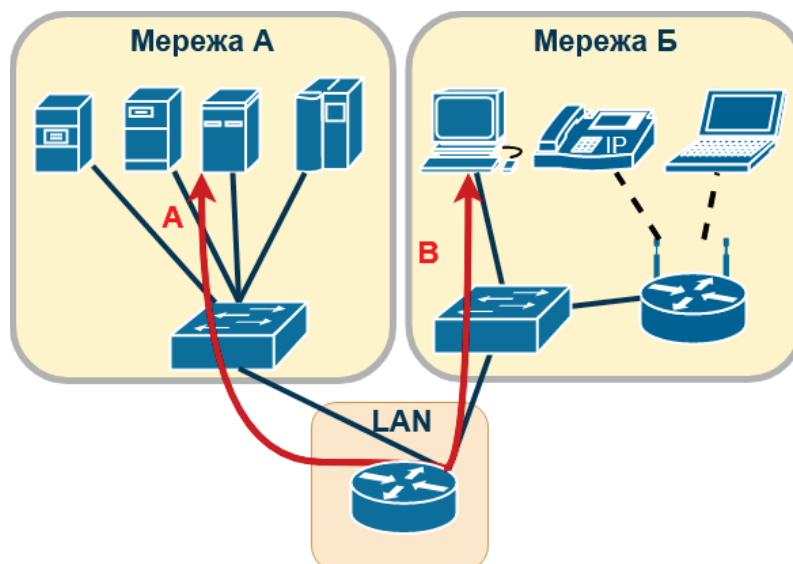


Рисунок 2.2 – Анти-шаблон «Екранований хост»

Для того щоб дозволити пристроям поза межами організаційної зони підключатися до нашого сервера (хоста А), системний адміністратор додає правило до файрволу, що робить мережу більш уразливою перед можливими атаками. За таким самим принципом відкритий доступ ззовні буде досягнутий для хоста В. Досвід на практиці показує, що потенційні зловмисники використовують вразливості програмного забезпечення служб А або В, щоб подальше захоплення сервера протоколу чи хоста В. Це дасть можливість отримати доступ до пристроїв і завдати шкоди організації.

Вирішення даної проблеми може бути здійснене шляхом відокремлення сервісів А та В. Однією з ефективних моделей для цього є архітектура «Екранованої підмережі». Зазвичай, служби та пристрої мережі, які є особливо вразливими, рекомендується відокремлювати до «демілітаризованих зон» (DMZ). Ці зони призначені для обслуговування веб, DNS та поштових серверів і знаходяться на периметрі мережі організації, біля точки виходу до Інтернету. Такий підхід сприяє підвищенню безпеки та захисту основних служб та пристроїв від потенційних загроз.

Отже, враховуючи проведений аналіз шаблонів побудови архітектури мереж, постає завдання у побудові відповідної UML-діаграми, що полегшить подальшу розробку на етапі проєктування системи.

Завдяки розробленій UML-діаграмі використання (рис. 2.3), можна чітко визначити принцип роботи системи, враховуючи користувальницькі взаємодії, аналітику з безпеки, та процеси автентифікації та авторизації.

Діаграма надає детальний огляд функцій системи, які взаємодіють з користувачем, а також визначає ключові моменти забезпечення безпеки та контролю доступу.

На схемі зображено елементи:

- Діючі Особи (Actors);
- Залежності (Dependencies);
- Імплементации (Implementations);
- Асоціації (Associations);
- Варіація розширення (Extend);
- Варіація включення (Include).

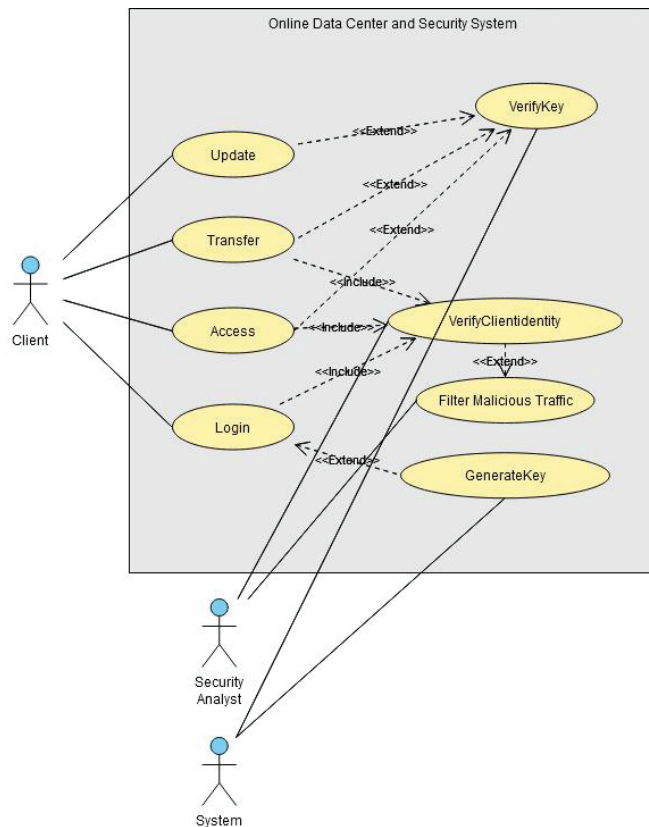


Рисунок 2.3 – UML-діаграма використання проєкту захисту системи

Діюча особа Security Analyst - має повноваження до виявлення та фільтрації підозрілого трафіку від підключених клієнтів, перевірки валідності даних клієнтів та їх прав в системі.

Діюча особа Client - має повноваження до підключення до захищеної мережі передачі трафіку, яка надає йому захищений доступ до центру обробки даних організації для подальшої роботи із базами даних, обміну інформації та віддаленим оновленням вбудованих додатків.

Діюча особа System генерує ключі доступу до системи для клієнтів та проводить верифікацію дій клієнтів із центром обробки даних.

Варіації розширення (Extend) та включення (include), поєднані прямими залежностями та/або асоціаціями, котрі вказано на схемі на кожному етапі роботи системи.

Класичні методи обмеження доступу до мережі за ідентифікаторами, такими як MAC та IP-адреса, стають швидко уразливими перед зловмисниками. Тому важливо використовувати надійні паролі та/або служби автентифікації з відкритим ключем. Наприклад, WiFi-маршрутизатор, розташований на

майданчику відпочинку, налаштовано за паролем доступом до мережі, тоді як пристрої Інтернету речей транспортних засобів мають необхідні параметри для підключення. Це сприяє забезпеченню безпеки мережі та захисту від неавторизованого доступу (рис. 2.4).

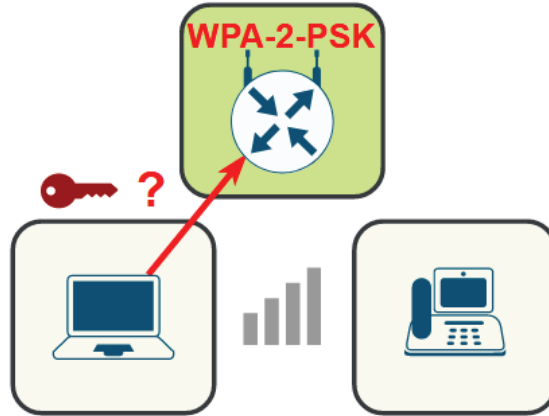


Рисунок 2.4 – WiFi – точка доступу з налаштованим паролем захистом

Мережу можна захищати ще декількома методами автентифікації. Ці методи дозволяють створити додатковий шар безпеки, контролюючи доступ користувачів до мережі за допомогою ефективної системи автентифікації. При використанні стандарту IEEE 802.1X, користувачі повинні представити валідні автентифікаційні дані, перш ніж отримати доступ до мережі. Протокол RADIUS відповідає за централізоване управління автентифікацією та авторизацією, забезпечуючи високу ступінь безпеки для мережі в цілому.

IEEE 802.1X — стандарт Інституту інженерів електротехніки та електроніки, який дозволяє обмежувати фізичний доступ до мережі і контролювати, які пристрої можуть взаємодіяти з мережею [26]. Принцип роботи IEEE 802.1X полягає в тому, що перед тим, як пристрій отримає доступ до мережі, він повинен пройти процес автентифікації. Це може бути реалізовано за допомогою ідентифікаційних даних, таких як ім'я користувача та пароль, або за допомогою інших методів автентифікації. Якщо пристрій успішно автентифікується, йому надається доступ до мережі, в іншому випадку доступ блокується.

RADIUS (Remote Authentication in Dial-In User Service) - це протокол мережної автентифікації та авторизації користувачів [27]. Використовується для

централізованого управління інформацією про користувачів, які намагаються отримати доступ до мережі або інших ресурсів. Основна функція RADIUS полягає в тому, щоб перевіряти ідентифікаційні дані користувача, такі як ім'я користувача та пароль, та визначати, чи може цей користувач отримати доступ до мережі чи інших ресурсів. RADIUS також може використовуватися для збору інших атрибутів користувача, таких як IP-адреса або рівень привілеїв.

Протокол часто використовується в сферах, де важливо забезпечити централізовану автентифікацію та авторизацію, такі як системи доступу до мережі Інтернет, віртуальні приватні мережі (VPN) та інші.

Використання стандарту IEEE 802.1X у комбінації з протоколом RADIUS дозволяє забезпечити ефективну та безпечну автентифікацію та авторизацію користувачів у мережевому середовищі:

- RADIUS використовується для централізованого управління процесами автентифікації та авторизації. це означає, що дані автентифікації зберігаються на центральному сервері radius, а не локально на кожному пристрої в мережі. це полегшує управління правами доступу та забезпечує їхню єдність;
- використання протоколу radius дозволяє шифрувати дані, які передаються під час автентифікації. це забезпечує конфіденційність інформації, такої як ім'я користувача та пароль, під час їхньої передачі по мережі;
- IEEE 802.1X дозволяє встановлювати механізми контролю доступу на основі ідентифікації користувача. це дозволяє управляти тим, які ресурси мережі можуть бути доступні для конкретного користувача або пристрою;
- система на базі IEEE 802.1X та RADIUS може легко підтримувати багато різних типів пристроїв та користувачів, включаючи комп'ютери, мобільні пристрої, іот-пристрої тощо;
- RADIUS дозволяє вести журнал подій, що полегшує виявлення та вирішення проблем безпеки в мережі. також можна використовувати дані з журналування для моніторингу активності користувачів та пристроїв.

Загалом, ця комбінація дозволяє створити ефективну та безпечну інфраструктуру мережі, що відповідає вимогам сучасного інформаційного середовища.

2.2. Вибір технічних засобів для реалізації системи

Розміри та масштаби впровадження мережі на підприємствах значно відрізняються. З метою розуміння необхідного функціоналу та потужностей обладнання, була створена UML-діаграма класів. На цій діаграмі відображено прямі зв'язки та успадкування між кожним із класів, що охоплюють весь цикл обробки даних, починаючи від авторизації клієнта та закінчуючи аналізом та фільтрацією підозрілого трафіку апаратними засобами (рис. 2.5).

Одними з вимог до обладнання є: фільтрація підозрілого трафіку, розподіл користувачів за рівнем доступу до мережі, а також ведення журналів логування.

З'ясуємо який саме функціонал має бути присутнім на обладнанні для виконання вимог проекту системи:

- доступ до мережі лише після автентифікації за користувачами та паролями;
- функція авторизації для працівників, які обслуговують мережеве обладнання;
- «білі» та «чорні» списки IP та MAC-адрес з яких можливе або заблоковане підключення до локальної мережі;
- шифрування персональної та критичної інформації, наявність тунелювання підключення.

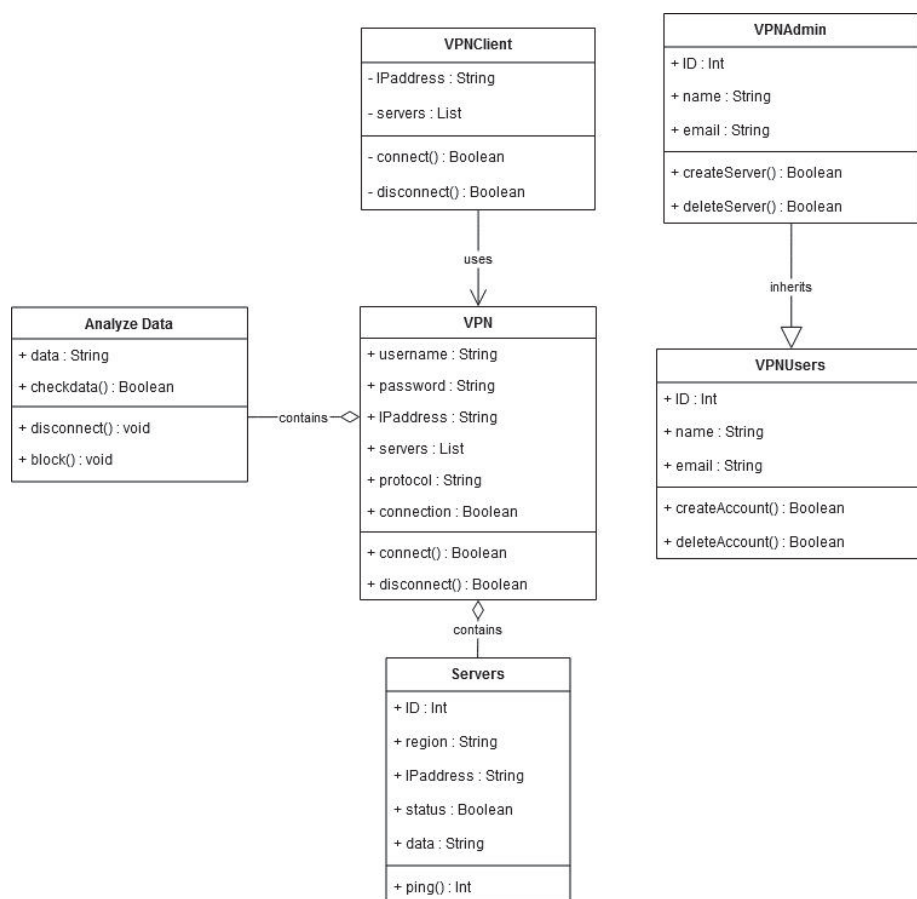


Рисунок 2.5 – Побудована UML-діаграма Класів проєкту захисту системи

На схемі зображено елементи:

- класи;
- методи;
- об'єкти;
- змінні.

Враховуючи необхідний функціонал на пристроях, зображений на діаграмі вище, ми можемо перейти до безпосереднього пошуку та аналізу сучасних зразків мережевого обладнання.

Компанія Cisco пропонує широкий, багатий портфель різноманітного обладнання для реалізації зазначеної стратегії захисту системи. Для рівня ядра необхідно шукати маршрутизуючі рішення.

Розглядаючи бюджетні варіанти, варто згадати за відому серію маршрутизаторів Cisco ISR800 (рис. 2.6).



Рисунок 2.6 – Маршрутизатор серії Cisco ISR800

Маршрутизатори Cisco ISR 800 призначені для використання в невеликих комерційних компаніях. Вони володіють широким функціоналом, сучасними методами управління та забезпечення безпеки. За допомогою цих пристроїв власник має швидкий доступ до WAN та налаштувань бездротові мережі [28]. Аналогічні пристрої інших виробників не володіють таким розмаїттям функцій. Cisco успішно об'єднує найсучасніші технологічні рішення, виходячи вперед серед інших виробників у цьому сегменті.

Розглянемо комутаційне обладнання Cisco Catalyst. Пристрої призначені для адаптивних бізнес-рішень, враховуючи індивідуальні вимоги клієнта. Системи, які пропонують різну щільність портів, продуктивність комутації, масштабованість та надійність, надають користувачам можливість проектувати та будувати ефективну та доступну мережеву інфраструктуру.

На рівні розподілу Cisco пропонує серію комутаторів Cisco Catalyst 3650 (рис. 2.7).



Рисунок 2.7 – Серія комутаторів Cisco Catalyst 3650

Ці комутатори використовують розроблені компанією Cisco електронні компоненти, такі як чіпи UADP. Ці чіпи дозволяють здійснювати кодування і декодування сигналу на швидкості носія без затримок і втрат продуктивності. Крім того, наявність технології Power over Ethernet (PoE) дозволяє надавати електричне живлення для підключених пристроїв.

Це лінійка стекових комутаторів, оснащених технологією StackWise-160. Застосування електронних схем UADP дозволяє налаштовувати роботу бездротових мереж разом з провідними за допомогою одних і тих самих інструментів, що забезпечує єдиноцільне управління всіма компонентами [29].

Комутатори Cisco Catalyst 2960-X можливо розглянути як практичне та оптимальне рішення (рис. 2.8).



Рисунок 2.8 – Серія комутаторів Cisco Catalyst 2960-X

Серія комутаторів Cisco Catalyst 2960-X - це стекові комутатори Gigabit Ethernet із фіксованою конфігурацією, які надають доступ корпоративного класу для застосувань у кампусах та філіях. Вони використовують програмне забезпечення Cisco IOS і дозволяють легко керувати пристроями та мережею, забезпечуючи швидке конфігурування з'єднань, логування та виправлення помилок [30].

Для ефективної роботи мережі організації були вибрані оптимальні маршрутизатори та комутатори від компанії Cisco, які підтримують модульну модернізацію. Нижче наведено опис та характеристики використаних пристроїв для побудови мережі.

Для виконання поставлених вимог організації та забезпечення функції якості обслуговування (QoS) мережі, були обрані маршрутизатори серії Cisco ISR4331 (рис. 2.9).



Рисунок 2.9 – Маршрутизатор Cisco Integrated Services Router 4331

Маршрутизатор Cisco ISR4331 належить до покоління пристроїв Cisco ISR (Integrated Services Routers) 4000 серії. Ці пристрої властиві високою пропускнуою здатністю до 2 Гбіт/с, вбудованими WAN (GibE) та SFP портами. До функціональності платформи Cisco ISR4300 і Cisco ISR4400 можна віднести гнучку систему налаштування, з можливістю додавання модулів до слотів розширення. Обладнання підтримує 2 або 3 слоти для встановлення модулів. Оперативна пам'ять представлена вбудованими 4GB з можливістю розширення до 16GB за рахунок окремих модулів, що підходить для створеного технічного завдання проєкту системи. Модель підтримує резервне живлення в разі відключення струму. Доступні усі необхідні мережеві протоколи, зокрема: NAT, IPSec та VPN, маршрутизації: RIP v1/v2, EIGRP, OSPF, BGP, PBR, PfR, IPv4 та IPv6 адресацію. Пристрої серії ISR4300 надають можливості використовувати якісний сервіс та гнучке налаштування, при цьому не витрачаючи бюджет на великі витрати [31].

Маршрутизатор Cisco ISR4331 з мережевими сервісами є оптимальним рішенням для проєктування мереж у малих та середніх установах або організаціях. Ця модель базово оснащена 4 ГБ вбудованої (з можливістю

апгрейду) та 4 ГБ флеш-пам'яті, а також має ліцензовану підтримку протоколу VPN, таким чином, надаючи можливість створення захищеного з'єднання.

На рівні розподілу, маршрутизація відведена для комутаторів серії Cisco Catalyst 3650 (рис. 2.10).



Рисунок 2.10 – Багаторівневий комутатор Cisco Catalyst 3650

Cisco Catalyst 3650 – комутатори з підтримкою роботи у стеку для надання оптимального доступу та вбудованим контролером бездротового зв'язку ASIC, які працюють на базі операційної системи IOS XE [29].

Особливості моделей Catalyst 3650 включають незмінну конфігурацію з 24 або 48 портів 10/100/1000 з підтримкою PoE+ (до 30 Вт на порт), вбудовані uplink 4 x Gigabit Ethernet, 2 x 10 Gigabit Ethernet або 4 x 10 Gigabit Ethernet з можливістю використання трансиверів SFP і SFP+, підтримку до 2 джерел живлення різної потужності і 3 кулерів для охолодження. Крім того, Catalyst 3650 має підтримку технології стекінгу StackWise (максимум 9 пристроїв) за використання додаткових модулів стекування з пропускну здатністю 160 Гб/с включаючи вбудований алгоритм SSO (Stateful Switch Over), пропускну здатність для бездротового зв'язку 40 Гб/с завдяки ASIC UADP (Unified Access Data Plane) та операційної системи IOS XE, а також підтримку до 25 точок доступу та 1000 бездротових клієнтів на один комутатор 3650 або один стек StackWise.

Проектування мережі на майданчику відпочинку вимагає надійне та кероване рішення, здатне задовольнити потребу у віддаленому керуванні і

водночас якісній передачі інформації. Тому вибір був зупинений на міжмережевому екрані Cisco Meraki MX65W-HW (рис. 2.11).



Рисунок 2.11 – Міжмережевий екран Cisco Meraki MX65W-HW

Міжмережевий екран Cisco MX65-HW представляє собою ефективний пристрій з функціями маршрутизатора, з пропускною здатністю до 250 Мбіт/с. Хоча максимальна швидкість VPN обмежена 100 Мбіт/с, пристрій обладнаний x10 GbE (RJ45) LAN-портами, а також двома GbE WAN-портами і USB-портом для підключення модулів 3G/4G. З цих десяти портів, два LAN-порти підтримують технологію PoE+, що робить можливим живлення підключених пристроїв через мережевий кабель. Особливістю моделі MX65W є підтримка стандарту Wi-Fi 802.11ac.

Оскільки MX керується повністю у хмарі, встановлення та віддалене керування робиться дуже простим та зрозумілим для користувача. MX має повний набір мережевих послуг, в результаті чого зникає потреба у декількох пристроях. Ці послуги включають можливості SD-WAN, міжмережевий екран на основі програм, фільтрація контенту, фільтрація веб-пошуку, виявлення та запобігання кібеатакам на основі SNORT®, Cisco Advanced Malware Protection (AMP), веб-кешування тощо.

Для рівня доступу був обраний комутатор Cisco Catalyst 2960 (рис. 2.12).



Рисунок 2.12 – Комутатор Cisco Catalyst 2960

Компанія Cisco створила обладнання, яке взаємодіє з різноманітними типами інформації, включаючи відео та VoIP. Продукція з серії Catalyst 2960 Switch відповідає сучасним стандартам і широко використовується компаніями як ефективний інструмент для передачі різноманітної інформації. Це обладнання готове до масштабування своїх функцій, щоб задовольнити усі потреби підприємства [34].

Комутатори Cisco Catalyst з серії 2960 володіють інтуїтивним інтерфейсом, призначеним для зручності користувача. Для першої конфігурації доступний пакет утиліт під назвою Cisco Network Assistant, який сприяє налаштуванню робочого середовища, підвищує його продуктивність та швидкість відповіді.

Cisco Catalyst 2960 може бути використаний у різних типах мережевого зв'язку, включаючи провідну і бездротову мережі, що робить ці продукти дуже популярними. Ці комутатори володіють значними обчислювальними можливостями. Користувачеві потрібно визначити параметри передачі трафіку, встановити пріоритети, вказати тип передачі інформації та обрати швидкість виконання всіх операцій. Хоча при виконанні складних завдань продуктивність цих комутаторів може зменшуватися, впроваджені технології дозволяють системі швидко впоратися з великим навантаженням.

Серед характеристик комутаторів цієї серії можна відзначити можливість індивідуального налаштування швидкості передачі на кожному порту з кроком в 64 Кбіт/с, підтримку об'єднання портів (Link Aggregation) для створення більш швидкісних з'єднань між комутаторами і серверами, а також здатність

організовувати транкові з'єднання на кожному порту, використовуючи теги 802.1Q.

Більшість лінійок комутаторів Cisco Catalyst 2960 не мають можливостей маршрутизації, але вони можуть проводити фільтрацію трафіку на основі інформації 3-го рівня, а саме IP-адрес.

2.3. Вибір протоколу шифрування та захисту інформації

Політика фільтрації має враховувати використання основних протоколів для пропуску пакетів, таких як DNS, NTP і т. д. Це включатиме трафік через інтерфейс "Za" для IKEv1 або IKEv2 та IPsec ESP в тунельному режимі. Крім того, сама архітектура LTE передбачає використання стандарту AES та алгоритмів шифрування, зокрема відомого SNOW-3G [35].

Для ретельного аналізу протоколів захисту інформації важливо розібратися в тому, як саме буде відбуватися обмін інформацією в системі. З цією метою була створена UML-діаграма послідовності дій, яка детально описує шлях потоку даних між клієнтом та сервером, включаючи процеси перевірки валідності клієнта та шифрування трафіку (рис. 2.13).

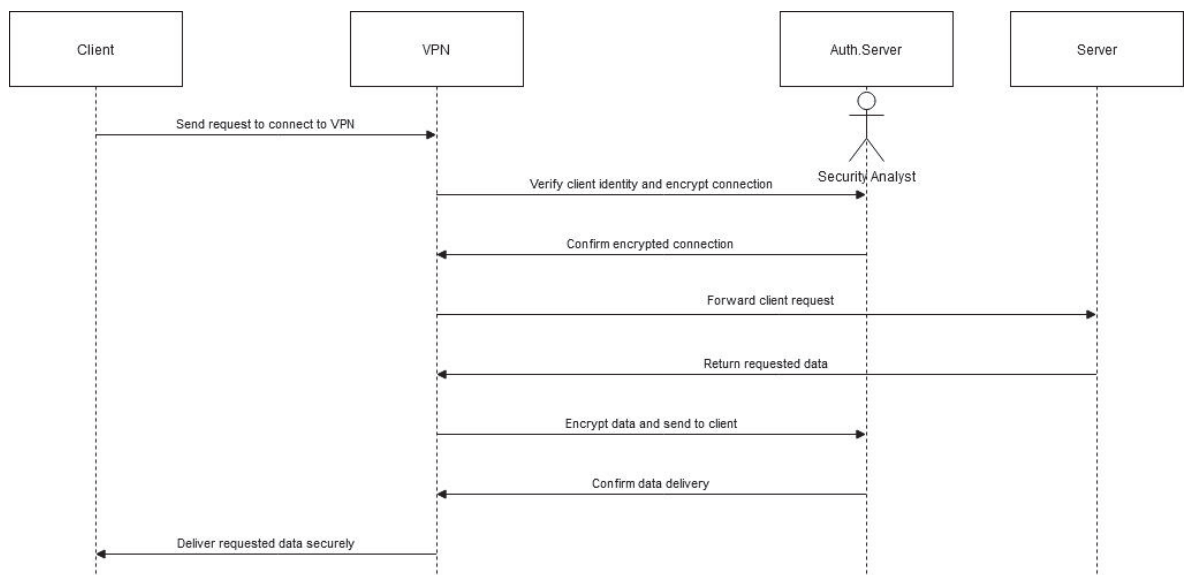


Рисунок 2.13 – UML-діаграма послідовності дій проєкту системи

Послідовність дій за діаграмою виглядає наступно:

- клієнт надсилає запит для отримання доступу до захищеного підключення до цод;
- шлюз отримує запит і передає його серверу автентифікації;
- фахівець з кібербезпеки перевіряє ідентифікаційні дані клієнта та трафік від нього; якщо все добре, він висилає підтвердження для підключення користувача до захищеної мережі;
- клієнт виконує запити до бази даних;
- перевірка запитуваних даних відбувається після отримання підтвердження від фахівця (або автоматичною системою), але до їхньої передачі клієнту;
- запитувані дані надходять до клієнта у безпечному режимі.

Більшість технологій шифрування віртуальних приватних мереж розроблені Національним Інститутом Стандартів та Технологій (NIST). Давайте розглянемо, наскільки надійні ці заходи безпеки, проаналізуємо основні різниці між протоколами VPN та їх вплив на користувачів, а також питання, пов'язані із шифруванням.

РРТР - це протокол тунелювання «точка-точка», що використовується для створення віртуального приватного каналу між користувачем і приватною мережею через Інтернет. РРТР дозволяє безпечно передавати дані через неприватні мережі, такі як Інтернет, шляхом створення зашифрованого тунелю між пристроями [36].

Зокрема, РРТР використовується за замовчуванням на багатьох пристроях, оскільки його легкість налаштування і висока швидкість зробили його популярним серед користувачів. Завдяки мінімальним вимогам до обчислювальних ресурсів, цей протокол є привабливим вибором для тих, хто цінує ефективність та простоту використання.

Незважаючи на його поширеність, РРТР має серйозні недоліки з точки зору безпеки, зокрема вразливість автентифікації MS-CHAP v2, що призводить до можливості зламування за короткий час. На сьогоднішній день рекомендується

використовувати більш безпечні протоколи, такі як SSTP або L2TP, щоб гарантувати надійний рівень захисту даних. Це особливо важливо в контексті того, що розшифрування PPTP може бути проведено навіть з врахуванням заходів безпеки, вжитих Microsoft.

L2TP/IPsec - (англ. Layer 2 Tunneling Protocol – протокол тунелювання другого рівня) – є протоколом тунелювання, який дозволяє створювати віртуальні приватні мережі (VPN) через неприватні мережі, такі як Інтернет. Він використовує механізм тунелювання для передачі трафіку між двома кінцевими точками тунелю, створюючи логічний зв'язок між ними. L2TP сам по собі не забезпечує шифрування або автентифікацію, тому часто використовується в поєднанні з протоколом IPsec для забезпечення додаткових заходів безпеки [36]. Однією із особливостей L2TP є те, що цей протокол дозволяє побудувати тунель навіть у мережах: Frame Relay, X.25 або ATM.

Основні характеристики L2TP/IPsec включають:

- використовується для шифрування даних, які пересилаються через тунель L2TP, забезпечуючи конфіденційність і захист від несанкціонованого доступу;
- дозволяє проводити автентифікацію сторін, що з'єднуються, за допомогою різних методів, таких як публічні ключі, передача паролів або інші механізми;
- створює тунель між кінцевими точками. Це дозволяє ізолювати трафік віртуальної мережі від інших мережевих ресурсів;
- є популярним для встановлення VPN на мобільних пристроях, таких як смартфони і планшети.

L2TP/IPsec є одним із стандартів для захисту трафіку через неприватні мережі і знаходить широке застосування у сфері бізнесу та особистому користуванні.

OpenVPN - це відкрите програмне забезпечення для створення віртуальних приватних мереж (VPN). Воно надає можливість безпечної передачі трафіку через неприватні мережі, такі як Інтернет. Однією з основних переваг

OpenVPN є його відкритий код, що означає, що вихідний код програми є відкритим і доступним для перегляду та аудиту користувачами та розробниками [37]. OpenVPN використовує SSLv3/TLSv1 разом із бібліотекою OpenSSL та іншими передовими технологіями, що створює потужне та надійне VPN-рішення для користувачів. Цей протокол відрізняється високою гнучкістю у налаштуванні та найкраще працює через UDP-порт, однак можливе налаштування його для роботи через будь-який інший порт. Наприклад, використання інших портів, таких як ті, що використовуються сервісами, подібними до Google, ускладнює їх блокування.

Ще однією важливою перевагою є те, що бібліотека OpenSSL підтримує різні алгоритми шифрування, такі як Blowfish, 3DES, AES, Camellia, CAST-128. Однак провайдери VPN, як правило, використовують в основному або Blowfish, або AES. За замовчуванням OpenVPN надає 128-бітне шифрування Blowfish, яке, як правило, вважається безпечним, але були виявлені певні недоліки.

Перш за все, швидкість OpenVPN визначається рівнем шифрування, хоча в більшості випадків вона вища, ніж у IPSec. Важливо відзначити, що хоча OpenVPN є стандартом підключення для більшості VPN-провайдерів за замовчуванням, його підтримка може бути обмеженою на деяких платформах. Проте існують сторонні програми, що активно розробляються, зокрема для платформ Android або iOS.

Розгортання OpenVPN є більш складним порівняно з L2TP/IPSec та PPTP. Необхідно не лише завантажити та встановити клієнт, але також витратити час на налаштування файлів конфігурації. Деякі постачальники VPN надають готові клієнти «з коробки» для спрощення цього процесу.

SSTP (Secure Socket Tunneling Protocol) - це протокол тунелювання, який забезпечує безпечний обмін даними між клієнтом і VPN-сервером через протокол HTTPS (HTTP over SSL/TLS) [38]. Основною особливістю SSTP є те, що він використовує SSL/TLS для шифрування трафіку, що робить його дуже ефективним у запобіганні перехопленню інформації.

Основні характеристики SSTP:

- використовує SSL/TLS для шифрування трафіку, що забезпечує високий рівень безпеки передачі трафіку;
- важко блокується чи перехоплюється в силу того, що використовує стандартний порт HTTPS (443), який зазвичай відкритий в більшості мереж;
- підтримується на операційних системах Windows, Linux, і деяких інших платформах;
- працює на захищених мережах, що блокують інші VPN-протоколи;
- легко налаштовується на серверах з ОС Windows Server;
- часто проходить через брандмауери і фільтри, оскільки використовує стандартний HTTPS-порт;
- важко заблокувати через використання HTTPS, що робить його ефективним у країнах чи мережах, які намагаються обмежити використання VPN;
- вбудований в операційні системи Windows, що дозволяє легко використовувати його для забезпечення безпеки з'єднань.

Хоча SSTP має свої переваги, важливо також враховувати, що він не є так поширеним як, наприклад, OpenVPN. Також, він може бути обмежений підтримкою лише на платформах Windows, що може бути чинником вибору в залежності від конкретних потреб.

Internet Key Exchange version 2 (IKEv2) - це протокол, призначений для автоматичного обміну ключами та установлення безпечного з'єднання (тунелю) між двома пристроями в мережі, такими як VPN-клієнт і VPN-сервер. Цей протокол часто використовується для створення з'єднань з великою мірою мобільності, таких як VPN для мобільних пристроїв [39].

Основні характеристики IKEv2:

- забезпечує високий рівень безпеки через використання сучасних шифрувальних алгоритмів та інших криптографічних методів;
- підтримує різні алгоритми шифрування та автентифікації, що робить його витриманим до різних видів атак;

- Оптимально підходить для мобільних пристроїв та робочих станцій, які можуть змінювати своє місцезнаходження та з'єднання;
- здатний відновлювати з'єднання після втрати мережевого зв'язку, зміни IP-адреси або переходу між мережами (наприклад, від Wi-Fi до мобільного зв'язку);
- має механізми зменшення латентності та оптимізації шляху для покращення ефективності потоку даних;
- використовується з IPsec для створення безпечного тунелю та захищеного обміну трафіку;
- здатний підтримувати одночасні тунелі для різних потоків даних, що підвищує продуктивність;
- ймовірність перехоплення атак є низькою завдяки використанню сучасних методів шифрування та автентифікації;
- має можливість розширюватися за допомогою додаткових модулів та функцій для адаптації до конкретних вимог;

IKEv2 є одним із найсучасніших та найбільш безпечних протоколів для налаштування VPN-з'єднань, зокрема для мобільних платформ.

Шифри - представляють собою математичні алгоритми, які використовуються для процесу шифрування. Найпростіші з них, як правило, виявляються більш вразливими перед потенційними атаками хакерів, оскільки можуть дозволяти легше дешифрування переданих даних. На сучасному етапі розвитку криптографії двома найбільш відомими та широко використовуваними шифрами є AES та Blowfish, які застосовуються в більшості сервісів VPN. Крім того, для операцій шифрування та дешифрування використовується RSA, в той час як алгоритми хешування SHA-1 та SHA-2 використовуються для автентифікації.

На сьогоднішній день найбільш безпечним шифром для VPN вважається Advanced Encryption Standard (AES). AES широко використовується у різних сферах, включаючи інформаційну безпеку та криптографію. Його застосовують уряди та багато компаній через його надійний рівень безпеки. AES має різні

ключі (128 біт, 192 біти та 256 біт), і більш великий розмір ключа забезпечує ще вищий рівень захисту.

Найпростіший спосіб зрозуміти, скільки часу потрібно для дешифрування даних - це врахувати довжину ключа та можливу кількість комбінацій бітів, які використовуються у шифрі. В разі методу підбору "brute force" відбувається послідовна спроба дешифрувати ключ, перевіряючи всі можливі комбінації, доки не буде знайдено відповідний ключ. Зазвичай ключі VPN мають довжину від 128 до 256 біт, де вищі рівні використовуються для автентифікації. Для зламу 128-бітного шифру потрібно близько $3,4 \times 10^{(38)}$ операцій. Зрозуміло, що для 256-bit потрібно в два рази більше обчислень. Таким чином, підбір такого шифру вимагатиме приблизно $3,31 \times 10^{(65)}$ операцій, що рівносильно кількості атомів у нашому всесвіті.

Проаналізуємо таблицю переваг та недоліків серед відомих проколів, та оберемо з них найбільш надійний варіант.

Таблиця 7

Властивості серед протоколів VPN

	PPTP	L2TP/IPSec	OpenVPN	SSTP	IKEv2
Переваги	– ефективна продуктивність – вбудований клієнт, доступний на різних платформах – легке налаштування	– протоколи з високим рівнем надійності – підтримка на різноманітних пристроях і системах	– детальне налаштування – відкритий код – є підтримка багатьох алгоритмів шифрування	– підтримка від компанії Microsoft – обране шифрування впливає на захищеність	– підтримка різноманітних алгоритмів шифрування: 3DES, AES, та AES 256 – автоматичне підключення після розірвання з'єднання – інтуїтивно зрозумілі налаштування – вища швидкість порівняно з L2TP, PPTP, SSTP

Недоліки	– не забезпечує абсолютну захищеність даних – вразливий до вторгнень	– менш швидкий у порівнянні з OpenVPN – значна кількість додаткової інформації, яка включається до вихідного пакету	– складний процес конфігурації – необхідність використання додаткового програмного забезпечення – обмежена підтримка мобільних додатків	– підтримує лише Windows	– обмежена сумісність – UDP 500 може бути легше заблоковано, ніж порти SSTP або OpenVPN – закритий вихідний код – складна конфігурація на серверах
----------	---	--	---	--------------------------	---

Після ретельного аналізу вищезазначених протоколів, врахування переваг та недоліків кожного з них а також потреб підприємства, було вирішено спроектувати VPN-тунель, використовуючи протоколи L2TP/IPSec. Це обрано як просте, але в той же час надійне та ефективне з точки зору витрат рішення забезпечення доступу, яке доступне на різних платформах.

2.4. Створення діаграми активності та функціональної схеми

Розглянемо мережу організації, яка складається з одного офісу і включає три зони, а також віддалену локальну мережу майданчику транспортних засобів, до якої підключатимуться їх бортові пристрої. Дві зони схожі між собою і формують робочі зони організації. Система розрахована на можливість розширення мережі шляхом збільшення кількості пристроїв, підключених до портів комутаторів, а також можливість додавання подібних зон. У третій зоні розташовані обчислювальні потужності, де зосереджено збір усієї інформації та встановлення зв'язу з транспортними засобами. Враховуючи усі умови, була створена трирівнева мережа. Топологія мережі доступна на рис. А.1.

У процесі проектування була створена діаграма активності (IDEF3) проєкту підвищення рівня захищеності системи обміну даними з громадським транспортом (рис. 2.14).

Діаграма описує як саме користувач комунікує із системою та за яких умов йому може бути відмовлено у доступі.

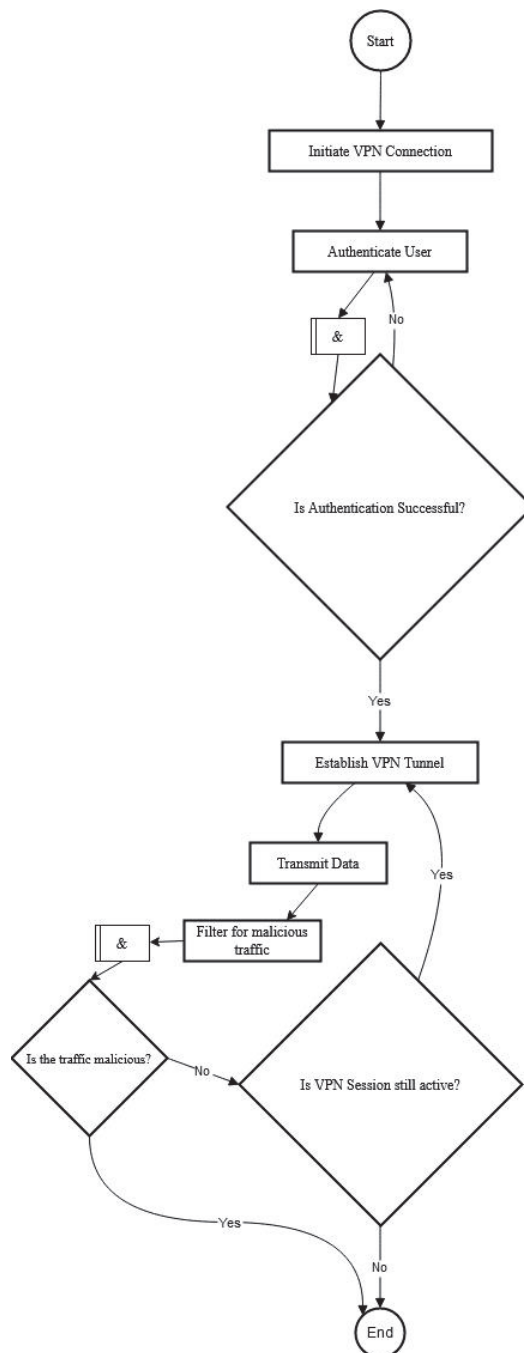


Рисунок 2.14 – Діаграма активності проекту

Процес підключення користувача та його автентифікації в системі виглядає наступно:

- Автономний пристрій або клієнт користувача ініціює VPN-з'єднання;
- Сервер автентифікації перевіряє відповідність даних та надає або відмовляє у доступі;

- Якщо все гаразд, налагоджується VPN-підключення по якому відбувається обмін даними з віддаленою мережею;
- Під час обміну, трафік перевіряється на наявність підозрілих пакетів, якщо обладнання помітить такий пакет, підключення буде розірвано.

В процесі проектування була створена функціональна схема проєкту підвищення рівня захищеності системи обміну даними з громадським транспортом (рис. 2.15).

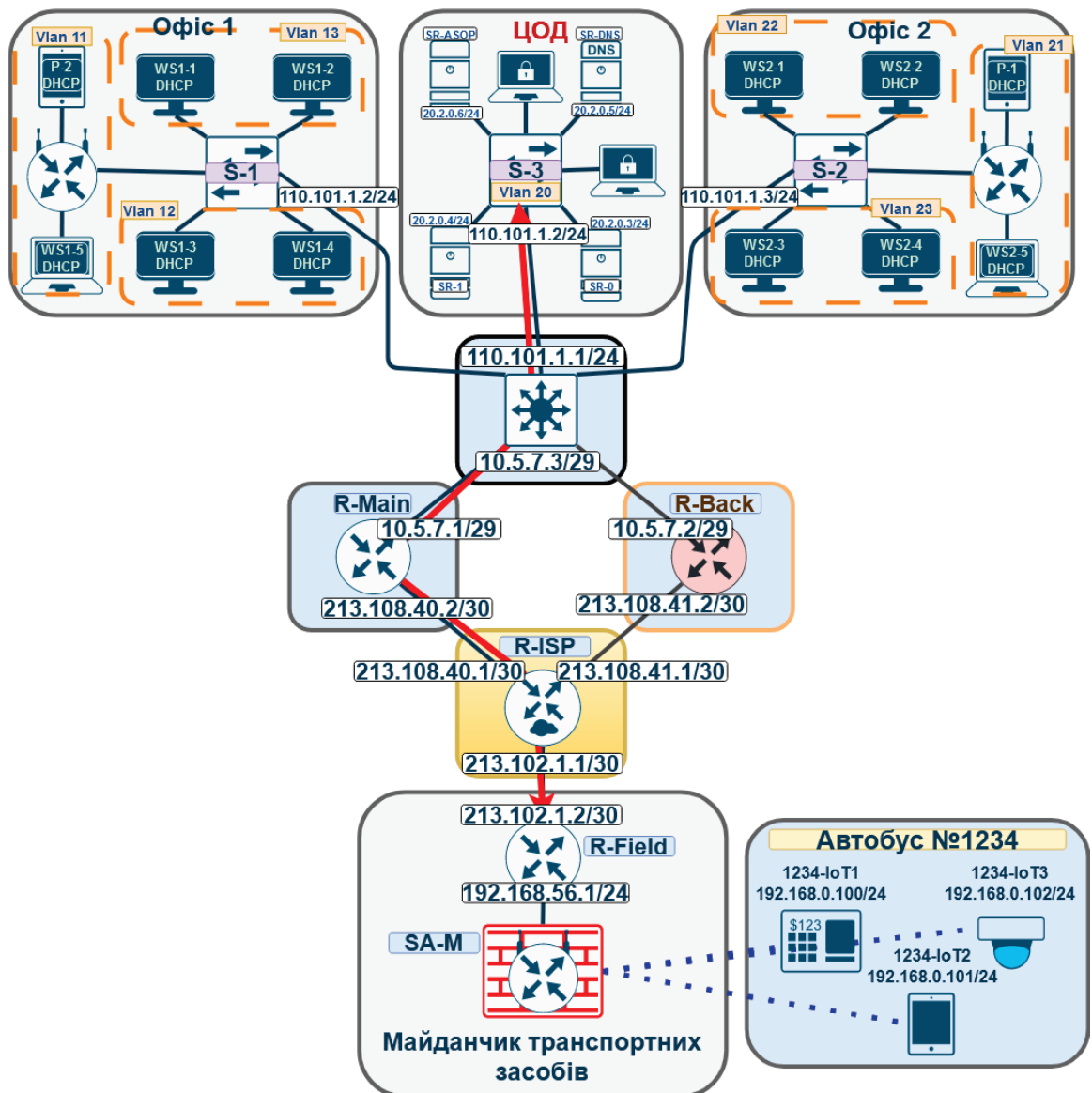


Рисунок 2.15 – Функціональна схема мережі проєкту

Для забезпечення оптимального функціонування топології мережі організації, у першу чергу, був проведений обрахунок параметрів IP-адресації. Під час цього розрахунку було зосереджене акцентування питання на

раціональному використанню IP-адрес, а також забезпеченню безпечної передачі трафіку з віддаленою мережею [40]. Адресація внутрішньої мережі, яка включає офіси та майданчик транспортних засобів, буде встановлена шляхом використання протоколу динамічного налаштування вузла DHCP. З метою полегшення конфігурації та підвищення рівня безпеки внутрішньої мережі буде розділена на віртуальні локальні мережі за допомогою технології VLAN. Детальну топологію з'єднань та параметри адресації мережі представлені у додатках А-В.

Висновки до розділу 2

В цьому розділі була виконана робота над розробкою проекту для підвищення безпеки системи обміну даними з громадським транспортом. Проведено аналіз різних шаблонів проектування, визначено їх переваги та недоліки. Окрема увага була приділена методу екранованої підмережі, і було прийнято рішення використовувати саме цей шаблон.

Проведено аналіз наявних технічних та програмних засобів для реалізації проекту, приведені особливості та характеристики обладнання на прикладі компанії Cisco.

Було вирішено використовувати технології VPN, після того як було проведено аналіз і порівняння переваг і недоліків різних відомих протоколів захисту трафіку. У результаті цього порівняння протокол IPSec було обрано як найбільш оптимальний варіант.

Представлено структурну схему та діаграму активності проекту. Проведено аналіз потенційних загроз витоку даних та представлено ефективні методи їх уникнення. Крім того, розроблено функціональну схему системи захисту, включаючи проектування топології мережі.

РОЗДІЛ 3. ПРАКТИЧНА ПОБУДОВА ТА ПЕРЕВІРКА ПРАЦЕЗДАТНОСТІ ПРОЄКТУ СИСТЕМИ

3.1. Створення практичної моделі проєкту, підготовка обладнання

У цьому розділі розглянуті основні налаштування пристроїв в мережі підприємства. З метою забезпечення зручності конфігурування та перевірки зв'язку між пристроями за їхніми іменами, замінимо назви хостів на більш доречні (рис. 3.1).

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R-Field
```

Рисунок 3.1 – Налаштування hostname на маршрутизаторі R-Field

Налаштуємо для серверного та маршрутизуючого обладнання статичну адресацію. За цими адресами, кожен пристрій зможе обмінюватись даними з іншими всередині мережі.

В локальних мережах зазвичай використовуються IP-адреси, призначені для використання в приватних мережах. Для підключення до мережі використовуються так звані 'білі' IP-адреси, названі так через те, що такі адреси ніколи не повторюються. Нижче зображено призначення саме такої адреси інтерфейсу маршрутизатора.

```
R-ISP(config)#interface GigabitEthernet0/0/0
R-ISP(config-if)#ip add 213.108.40.1 255.255.255.252
R-ISP(config-if)#no shut

R-ISP(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up
```

Рисунок 3.2 – Налаштування статичної IP-адреси на маршрутизаторі R-ISP

Далі приведемо призначення статичної адреси одному із серверів у нашій мережі.

☐ DHCP	☒ Static
IPv4 Address	20.2.0.6
Subnet Mask	255.255.255.0
Default Gateway	20.2.0.1
DNS Server	20.2.0.5

Рисунок 3.3 – Конфігурація статичної адреси для сервера SR-ASOP

Зімітуємо вихід до глобальної мережі через інтерфейс «loopback». На рисунку нижче зображено детальний процес налаштування через командний рядок маршрутизатора R-ISP (рис. 3.4).

```
R-ISP(config)#int loopback 1

R-ISP(config-if)#
%LINK-5-CHANGED: Interface Loopback1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback1, changed state to up

R-ISP(config-if)#ip add 172.16.0.1 255.255.255.252
```

Рисунок 3.4 – Налаштування інтерфесу Loopback1

Крім того, статичні IP-адреси застосовуються на комутаторах рівня L2 та L3. Це спрощує їх конфігурацію та аудит, не говорячи про віддалений доступ. Далі наведено процес налаштування Vlan5 із застосуванням статичної адреси, в подальшому даний VLAN ми застосуємо для протоколу маршрутизації HSRP.

```
S-LAN(config)#
S-LAN(config)#vlan 5
S-LAN(config-vlan)#name HSRP-PROTO
S-LAN(config-vlan)#ex
S-LAN(config)#int vlan 5
S-LAN(config-if)#
%LINK-5-CHANGED: Interface Vlan5, changed state to up

S-LAN(config-if)#ip add 10.5.7.3 255.255.255.248
```

Рисунок 3.5 – Закріплення інтерфейсу vlan 5 за статичною IP-адресою

Для розмеження доступу до пристроїв мережі всередині організації, та спрощення роботи системним адміністраторам, внутрішня мережа також буде розділена на декілька віртуальних локальних мереж.

Використання VLAN дозволяє полегшити управління мережею, покращити безпеку та ефективність ресурсів. Комутатори у мережі можуть

визначати, до якого VLAN належить конкретний мережевий порт, і таким чином обмежити трафік між різними VLAN.

Це особливо корисно в ситуаціях, коли потрібно групувати пристрої в мережі за функціональністю, відділами або іншими критеріями, щоб забезпечити кращу організацію та безпеку. Далі призначимо новостворений VLAN портам комутатора (рис. 3.6).

```
S-LAN(config)#int range g1/0/1-2
S-LAN(config-if-range)#switchport mode access
S-LAN(config-if-range)#switchport access vlan 5
S-LAN(config-if-range)#ex
S-LAN(config)#
```

Рисунок 3.6 – Налаштування vlan 5 на порти комутатора S-LAN

Щоб зробити можливим обмін інформації між різними VLAN та доступ до глобальної мережі, необхідно створити транкові канали потоку трафіку. Такі канали дозволяють зазначеним VLAN обмінюватись пакетами даних. Нижче наведено детальний приклад такого налаштування.

```
S-LAN(config-if)#switchport trunk allowed vlan add 1
S-LAN(config-if)#switchport trunk allowed vlan add 11
S-LAN(config-if)#switchport trunk allowed vlan add 12
S-LAN(config-if)#switchport trunk allowed vlan add 13
S-LAN(config-if)#exi
S-LAN(config)#ex
S-LAN#
%SYS-5-CONFIG_I: Configured from console by console

S-LAN#
S-LAN#sh int sw
S-LAN#sh int switchport
Name: Gig1/0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
```

Рисунок 3.7 – Створення транкового каналу на комутаторі S-LAN

Наступним етапом буде встановлення IP-адрес для кінцевих пристроїв, з генерацією яких нам допоможе протокол DHCP [42]. Цей протокол забезпечує автоматичне присвоєння всіх необхідних мережевих налаштувань для кінцевих пристроїв, таких як IP-адреса, маска підмережі, шлюз за замовченням, DNS та ім'я домену підмережі. Розгорнемо даний протокол на комутаторі S-LAN. Не варто забувати про можливі конфлікти з вже налаштованими статичними IP-адресами, тому такі адреса треба обов'язково додати у винятки.

```

S-LAN(config)#ip dhcp excluded-address 10.10.1.1 10.10.1.2
S-LAN(config)#ip dhcp excluded-address 10.20.2.1 10.20.2.2
S-LAN(config)#ip dhcp excluded-address 10.30.3.1 10.30.3.2
S-LAN(config)#ip dhcp excluded-address 20.10.1.1 20.10.1.2
S-LAN(config)#ip dhcp excluded-address 20.20.2.1 20.20.2.2
S-LAN(config)#ip dhcp excluded-address 20.2.0.1 20.2.0.4
S-LAN(config)#ip dhcp excluded-address 20.30.3.1 20.30.3.2
S-LAN(config)#ip dhcp excluded-address 20.2.0.1 20.2.0.6

```

Рисунок 3.8 – Додавання у вийнятки зарезервованих адрес на комутаторі S-LAN

Ми додали необхідні IP-адреси у вийнятки, тепер можливо переходити до налаштування DHCP-протоколу (рис. 3.9).

```

S-LAN(config)#ip dhcp pool WLAN1
S-LAN(dhcp-config)# network 10.10.1.0 255.255.255.0
S-LAN(dhcp-config)# default-router 10.10.1.1
S-LAN(dhcp-config)# dns-server 20.2.0.5
S-LAN(dhcp-config)# domain-name wlan1.com

```

Рисунок 3.9 – Процес конфігурації DHCP на комутаторі S-LAN

Комутатори L2 також були налаштовані для підтримки транкових каналів передачі трафіку, аналогічні до вищепроведених, окрім методу інкапсуляції – на цих комутаторах є лише 802.1Q.

Додатково, було проведено налаштування підтримки транкових каналів на комутаторах L2, окрім методу інкапсуляції.

Розглянемо процес налаштування Inter-VLAN маршрутизації. Inter-VLAN routing (маршрутизація між VLAN) - це процес обміну трафіку між різними віртуальними локальними мережами (VLAN) за допомогою маршрутизатора чи Layer 3-комутатора. Inter-VLAN routing є важливим елементом для ефективного управління трафіком та забезпечення безпеки в мережах, де використовуються VLAN [43].

При налаштуванні inter-VLAN, комутатори Cisco Catalyst використовують спеціальні інтерфейси – Switch Virtual Interfaces.

```

S-LAN(config)#
S-LAN(config)#ip routing
S-LAN(config)#

```

Рисунок 3.10 – Активація inter-VLAN маршрутизації на комутаторі S-LAN

Також необхідно налаштувати протокол динамічної маршрутизації для маршрутизаторів рівня ядра.

```

R-Back(config)#router ospf 1
R-Back(config-router)# log-adjacency-changes
R-Back(config-router)# network 213.108.41.0 0.0.0.3 area 0
R-Back(config-router)# network 10.5.7.0 0.0.0.7 area 0
R-Back(config-router)#ex
R-Back(config)#

```

Рисунок 3.11 – Процес конфігурації протоколу OSPF на маршрутизаторі R-Back

Тепер необхідно створити VPN-тунель з маршрутизатором віддаленої мережі. Система має бути побудована таким чином, щоб кожне IoT-обладнання, встановлене на транспортному засобі, мало змогу підключитись по бездротовому зв'язку до маршрутизатора та вивантажити усі дані на сервери через захищений канал зв'язку.

Нижче наведено покрокове налаштування маршрутизатора R-Field. Для цього проведемо налаштування протоколу IPSec на кожному з маршрутизаторів, між якими буде створено VPN-тунель. Зробимо необхідні конфігурації на маршрутизаторах R-Field та R-Main, проте спершу треба переконатись, що обладнання має активовану securityk9 ліцензію. Це легко зробити, під'єднавшись до командного рядка пристрою, необхідно виконати команду show version, а далі відшукати пункт щодо переліку доступних та активних (або неактивних) ліцензій (рис. 3.12).

Technology Package License Information:

Technology	Technology-package Current	Type	Technology-package Next reboot
appxk9	None	None	None
uck9	None	None	None
securityk9	securityk9	Permanent	securityk9
ipbase	ipbasek9	Permanent	ipbasek9
security	securityk9	Permanent	securityk9
ipbase	ipbasek9	Permanent	ipbasek9

Рисунок 3.12 – Команда sh version з інформацією про ліцензії маршрутизатора

Як можна побачити, ліцензія securityk9 присутня та активна. Якщо ж ліцензія не активна, необхідно її активувати командою license boot module N technology-package securityk9, де N – відповідна серія маршрутизатора.

Налаштуємо конфігурацію політик ISAKMP на маршрутизаторі віддаленої мережі R-Field:

```

R-Field(config)#crypto isakmp policy 10
R-Field(config-isakmp)# encr aes 256
R-Field(config-isakmp)# authentication pre-share
R-Field(config-isakmp)# group 5
R-Field(config-isakmp)#

```

Рисунок 3.13 – Конфігурація політики ISAKMP Phase 1

Призначимо спільний ключ для автентифікації з маршрутизатором R-Main:

```

R-Field(config)#crypto isakmp key myuniquekey address 213.108.40.2
R-Field(config)#

```

Рисунок 3.14 – Створення спільного ключа ISAKMP

Також ми маємо додати access-list, набір перетворення IPsec та Crypto Map.

Нижче наведено створення списків доступу та призначено дозволені IP-адреси для VPN-підключення (рис. 3.15).

```

R-Field(config)#access-list 110 permit ip 192.168.56.0 0.0.0.255 10.5.7.0 0.0.0.7
R-Field(config)#access-list 110 permit ip 192.168.56.0 0.0.0.255 20.2.0.0 0.0.0.7
R-Field(config)#

```

Рисунок 3.15 – Процес створення списків доступу на маршрутизаторі R-Field

Далі створимо набір перетворення, так званий Transform Set, який використаємо для підвищення безпеки даних. Якості методу шифрування виступає – esp-aes, тоді як алгоритмом шифрування було обрано – sha.

```

R-Field(config)#crypto ipsec transform-set sectunnel esp-aes 256 esp-sha-hmac
R-Field(config)#

```

Рисунок 3.16 – Набір перетворення, створений на маршрутизаторі R-Field

Останній етап це створення криптографічної карти. Тут визначаються IP-адреси маршрутизаторів, час життя підключення, вказується набір перетворення та відповідність адреси.

```

R-Field(config)#crypto map secludedmap 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
and a valid access list have been configured.
R-Field(config-crypto-map)# set peer 213.108.40.2
R-Field(config-crypto-map)# set peer 213.108.41.2
R-Field(config-crypto-map)# set pfs group5
R-Field(config-crypto-map)# set security-association lifetime seconds 86400
R-Field(config-crypto-map)# set transform-set sectunnel
R-Field(config-crypto-map)# match address 110
R-Field(config-crypto-map)#

```

Рисунок 3.17 – Створена криптографічна карта

Створену криптокарту необхідно застосувати до інтерфейсу маршрутизатора, з якого має надходити трафік. Зауважимо, що лише одна криптокарта може бути закріплена за одним інтерфейсом (рис. 3.18).

```
R-Field(config)#interface GigabitEthernet0/0/0
R-Field(config-if)# ip address 213.102.1.2 255.255.255.252
R-Field(config-if)# duplex auto
R-Field(config-if)# speed auto
R-Field(config-if)# crypto map secludedmap
*Jan  3 07:16:26.785: %CRYPTO-6-ISA_KMP_ON_OFF: ISA_KMP is ON
```

Рисунок 3.18 – Успішно застосована криптокарта до інтерфейсу Gig0/0

Таким чином, налаштування каналу VPN на маршрутизаторі R-Field завершено, аналогічний процес має бути виконаний на R-Main.

3.2. Налаштування системи та тестування на працездатність

На даному етапі завершена первинна конфігурація пристроїв мережі, тож перейдемо до більш поглибленого налаштування параметрів.

Для збереження працездатності мережі, проєкт був розроблений з урахування додаткового маршрутизатора R-Back, який виконуватиме BackUp-функцію у разі відмови R-Main. Для коректної роботи обох маршрутизаторів знадобиться протокол маршрутизації HSRP, який резервуватиме шлюз у мережі організації [44]. На рисунку нижче зображено налаштування даного протоколу.

```
R-Main(config)#interface GigabitEthernet0/0/1
R-Main(config-if)# ip address 10.5.7.1 255.255.255.248
R-Main(config-if)# duplex auto
R-Main(config-if)# speed auto
R-Main(config-if)# standby 1 ip 10.5.7.6
R-Main(config-if)# standby 1 priority 50
R-Main(config-if)# standby 1 track GigabitEthernet0/0/0
R-Main(config-if)# standby 0 timers 5 10
R-Main(config-if)#ex
R-Main(config)#|
```

Рисунок 3.19 – Налагодження HSRP на маршрутизаторі R-Main

Проведемо налаштування міжмережевих екранів Meraki. Основна відмінність у налаштуванні пристроїв даної серії є використання хмарного сервісу Cisco Meraki замість звичного командного рядка. Це робить дані пристрої більш зручними для встановлення у віддалених мережах, оскільки контроль

можливо виконувати з будь-якої точки світу, при цьому не застосовуючи технології тунелювання.

Після встановлення міжмережевого екрану, необхідно провести його первинну конфігурацію шляхом підключення до одного з портів Gigabit Ethernet на зворотній панелі. Далі відкрити браузер та перейти за адресою “setup.meraki.com”. Ми маємо побачити сторінку входу до міжмережевого екрану.

Для першого входу використаємо серійний номер пристрою, поле пароллю треба залишити порожнім.

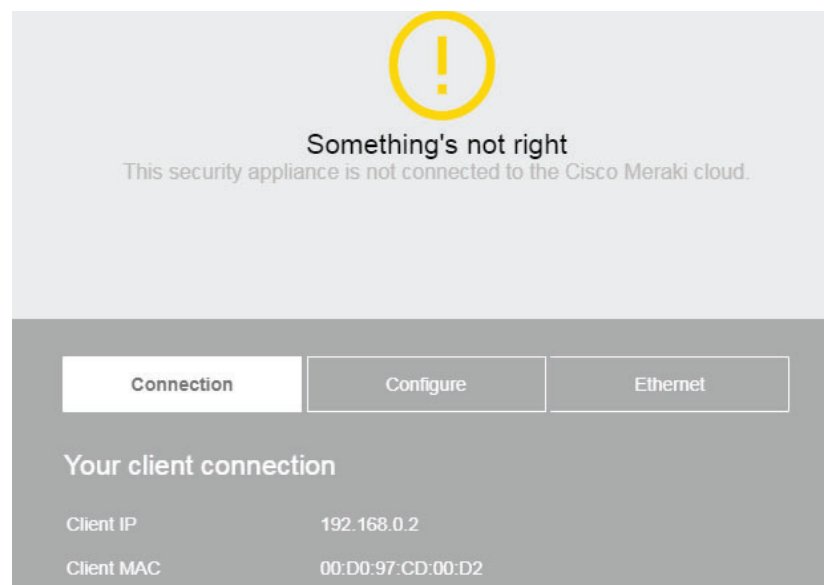


Рисунок 3.20 – Веб-інтерфейс міжмережевого екрану Meraki після авторизації

Як можна побачити, нам повідомляють, що даний пристрій не підключений до хмарного сервісу Cisco Meraki. Але спочатку треба налаштувати вихід до глобальної мережі. Для цього натиснемо на пункт меню «Configure», де можливо буде присвоїти пристрою IP-адресу вручну, або увімкнути DHCP. Для демонстрації скористаємось другим варіантом, маршрутизатор R-Field, до якого ми підключили даний міжмережевий екран, вже має відповідні налаштування на одному з портів.

Uplink configuration

Configure the uplink Internet connection on this security appliance.

Internet 1

Connection type Direct ▼

IP assignment DHCP ▼

Рисунок 3.21 – Проведено налаштування автоматичного отримання IP-адреси

Окрім цього, в базовому режимі ми також можемо викнути або увімкнути наявні інтерфейси та встановити узгодження швидкості (автоматичне за замовчуванням) (рис. 3.22).

Ethernet configuration

Use this page to configure physical link settings on the Ethernet ports.

Port Name	Enabled	Link Negotiation
Internet 1	enabled ▼	Auto (10/100/1000Mbps) ▼
Internet 2	disabled ▼	Auto (10/100/1000Mbps) ▼
GigabitEthernet 3	enabled ▼	Auto (10/100/1000Mbps) ▼
GigabitEthernet 4	enabled ▼	Auto (10/100/1000Mbps) ▼
GigabitEthernet 5	enabled ▼	Auto (10/100/1000Mbps) ▼

Рисунок 3.22 – Додаткове меню конфігурації Ethernet міжмережевого екрану

На даному етапі ми виконали початкове налаштування міжмережевого екрану Cisco Meraki. Для того щоб змінювати конфігурацію пристрою у режимі повного доступу, необхідно зареєструвати його у хмарі Cisco Meraki, перейшовши за посиланням dashboard.meraki.com та увійти в систему, якщо це Ваш перший перехід на портал, необхідно буде створити новий акаунт (рис. 3.23).

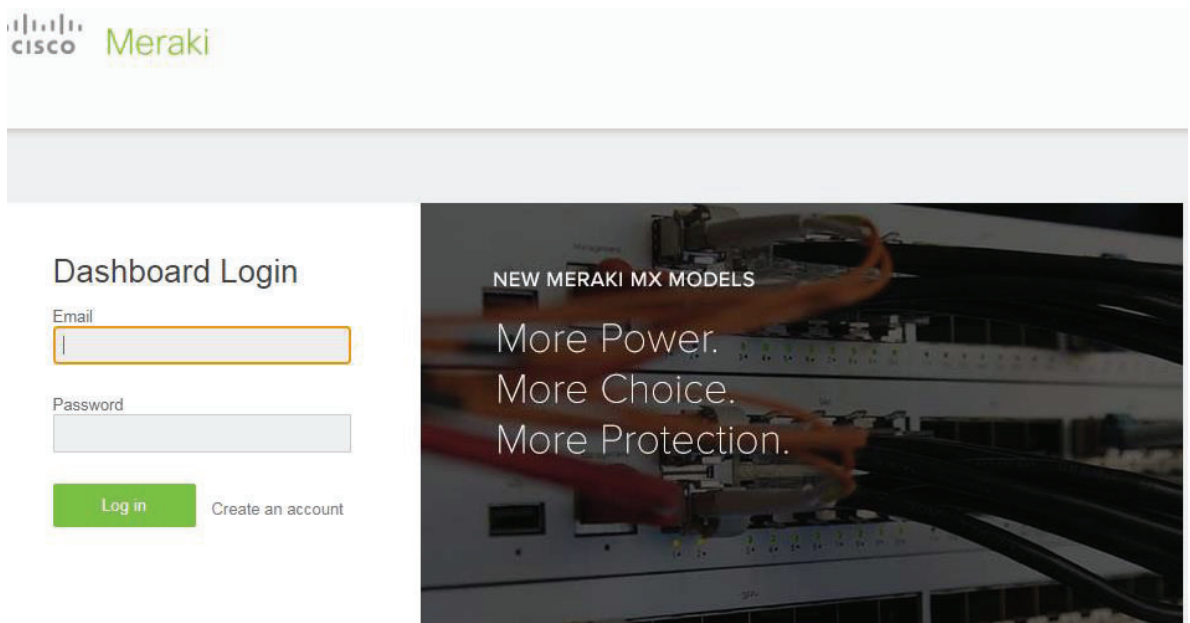


Рисунок 3.23 – Сторінка хмарного сервісу Cisco Meraki Cloud

Натиснемо на пункт “Create an account” та заповнимо форму реєстрації (рис. 3.24).

Create a new Meraki Dashboard account

Email	cisco_meraki@hotmail.com
Full Name	Michael K
Password	*****
Confirm password	*****
Company	ZSTU
Address	500 Terry A Francois Blvd
San Francisco, CA 94158
USA

Рисунок 3.24 – Форма реєстрації нового користувача Meraki Cloud

Після створення користувача, ми потрапляємо до головного меню, де зліва розташована панель навігації – тут будуть зображені усі створені мережі та додані пристрої. А перед нами буде зображено повідомлення, що на даний час ми не маємо жодного зареєстрованого пристрою Meraki.

Натиснемо на пункт «Create a network» (створити мережу), де нам запропонують ввести назву мережі та її тип. Також, на цій самій сторінці зареєструємо міжмережевий екран Meraki у відповідному вікні (рис. 3.25).

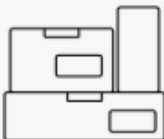
Network name: WLAN0

Network type: Security appliance

Network configuration: ☒ Default Meraki configuration

[Create network](#)

Select devices from inventory

 You have no unused devices
Add new devices or go to the inventory page to select devices that are already in networks

Add devices to inventory

Enter the individual device serial number:
7L8C-K3Q1-459I

Enter the device's model:
MX65W

Enter the device's mac address:
00:D0:97:CD:00:D2

Enter the network the device belongs to:
WLAN0

[Add devices](#) [Go to inventory](#)

Рисунок 3.25 – Сторінка створення нової мережі та реєстрації пристроїв

Мережа успішно створена, а пристрій додано до даного користувача. Перейдемо до конфігурації бездротової точки доступу, до неї будуть підключатись пристрої Інтернету речей транспортних засобів. Для цього перейдемо до меню Security Appliance -> Wireless Settings.

Зберігаємо зміни та переконаємось, що точка доступу працює (рис. 3.26).

Wireless Network Name			CH	Signal
WLAN0			1	58%

Site Information	
Wireless Mode	Infrastructure
Network Type	Mixed B/G/N
Radio Band	Auto
Security	WPA2-PSK
MAC Address	0000.0CEB.800D

[Refresh](#) [Connect](#)

Рисунок 3.26 – Підключення робочої станції #1234-IoT1 до бездротової точки доступу міжмережевого екрану Meraki

Wireless settings

SSID 1

Status	Enabled ▼
Name	WLAN0
Security	WPA2 PSK ▼
WPA key	*****
WPA encryption mode	WPA2 only ▼
Visibility	Advertise this SSID publicly ▼

Save Changes

Рисунок 3.27 – Конфігурація нової точки доступу Cisco Meraki

Налаштування міжмережевого екрану Meraki завершено. Окрім цього, необхідно увімкнути сервіси на серверах: HTTP/HTTPS, TFTP, журналювання подій SYSLOG, сервіс мережевого часу NTP, DNS та IoT [45] (рис. 3.28-3.33). Всі ці служби допоможуть слідкувати за станом мережі організації та отримувати дані від транспортних засобів кожного разу, коли вони повертаються до майданчика відпочинку у кінці зміни.

SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
M Management
Radius EAP

HTTP

HTTP

☒ On ☐ Off

HTTPS

☒ On ☐ Off

File Manager

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoptlogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

Рисунок 3.28 – Увімкнення сервісів HTTP/HTTPS на сервері SR-0

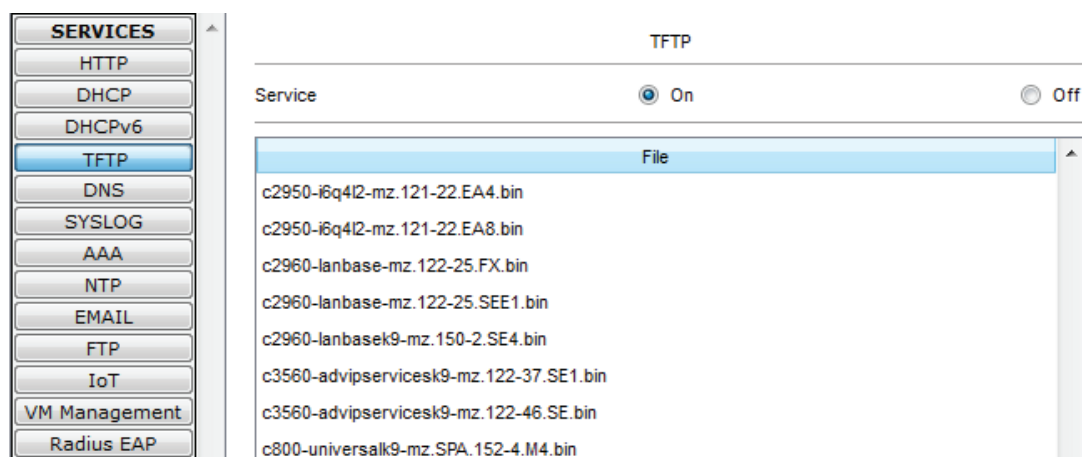


Рисунок 3.29 – Налаштований сервіс TFTP [46]

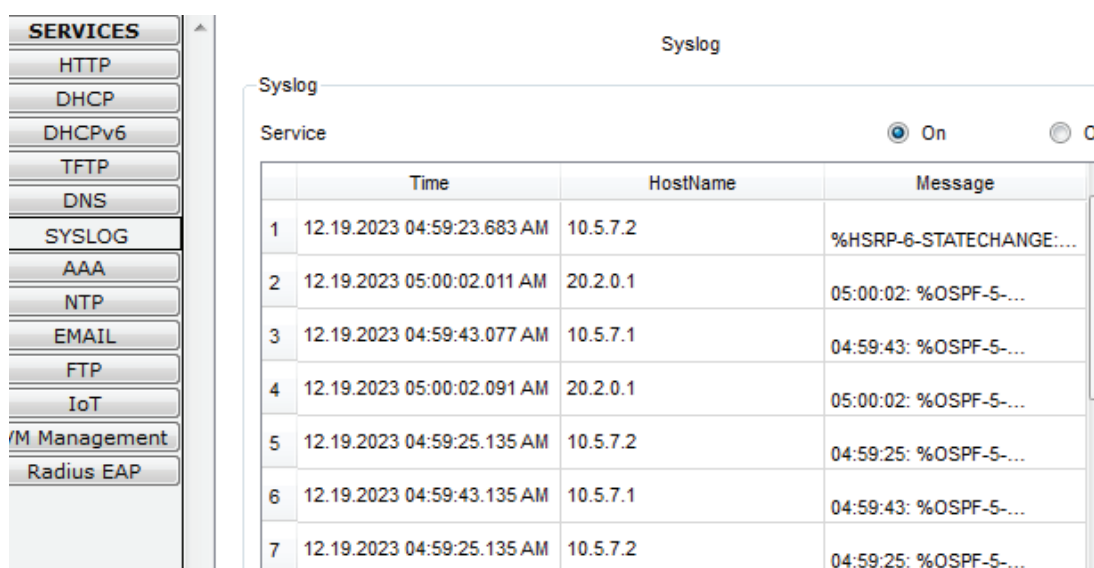


Рисунок 3.30 – Налаштований сервіс журналювання подій на сервері SR-1

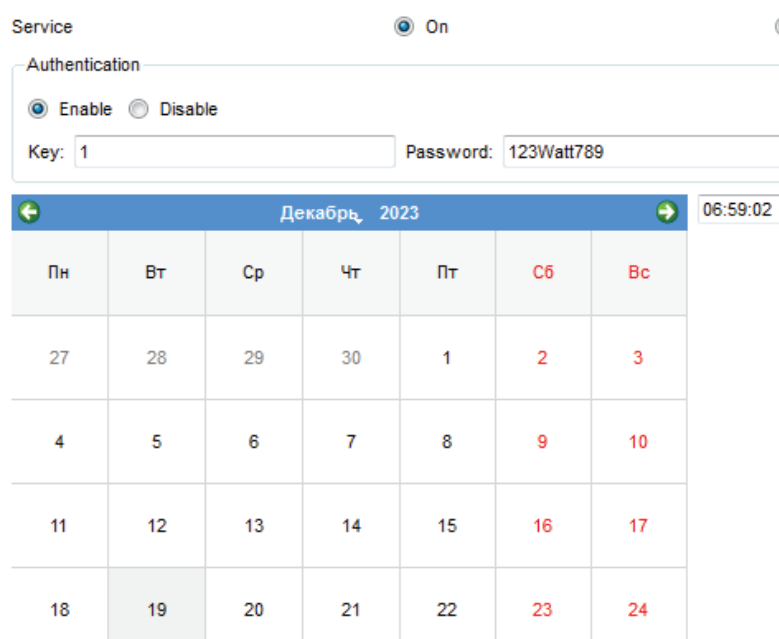


Рисунок 3.31 – Налаштований сервіс мережевого часу

DNS Service ☒ On ☐ Off

Resource Records

Name Type **A Record**

Address

No.	Name	Type	Detail
0	cisco	A Record	25.5.0.5
1	dashboard.meraki.com	A Record	20.2.0.7

Рисунок 3.32 – Налаштований сервіс DNS

Registration Server

Service ☒ On ☐ Off

	Username	Password
1	admin	admin

Рисунок 3.33 – Налаштований сервіс Інтернету речей

Перелічені сервіси також треба застосувати на пристроях нашої мережі. Протокол мережевого часу необхідний для збереження актуалізації усіх подій в мережі [47]. Для успішного застосування необхідно обрати відповідний сервер, на якому даний сервіс вже налаштовано, а також параметри часу, зокрема, часовий пояс. Синтаксис команд однаковий для усіх мережевих пристроїв (рис. 3.34).

```
R-Back(config)#ntp authenticate
R-Back(config)#ntp authentication-key 1 md5 123Watt789
R-Back(config)#ntp trusted-key 1
R-Back(config)#ntp server 20.2.0.4 key 1
R-Back(config)#ntp update-calendar
R-Back(config)#ex
R-Back#
```

Рисунок 3.34 – Застосування NTP на маршрутизаторі R-Back

Налаштування журналу подій «SYSLOG» схоже до вже застосованих конфігурацій для NTP (рис. 3.35).

```

R-ISP(config)#service timestamps log datetime msec
R-ISP(config)#service timestamps debug datetime msec
R-ISP(config)#logging on
R-ISP(config)#logging 20.2.0.4
R-ISP(config)#logging userinfo
R-ISP(config)#logging trap debugging
R-ISP(config)#logging buffered 64000
R-ISP(config)#exit
R-ISP#

```

Рисунок 3.35 – Увімкнена система журналювання подій SYSLOG на маршрутизаторі R-ISP

Підключимо пристрої транспортних засобів до внутрішньої мережі. Для цього перейдемо до реєстрації користувача на відповідному сервері IoT.

Registration Server Account Creation

Username:

Password:

Рисунок 3.36 – Реєстрація нового користувача на сервері SR-ASOP

Після процесу реєстрації ми можемо закріпити пристрої транспортних засобів за даним сервером, таким чином вся інформація буде надходити через захищений канал мережі до серверу обробки даних.

Port Status ☒ On

Bandwidth

MAC Address

SSID

Authentication

☐ Disabled ☐ WEP WEP Key
☐ WPA-PSK ☒ WPA2-PSK PSK Pass Phrase
☐ WPA ☐ WPA2 User ID
☐ 802.1X Method: Password
User Name
Password

Encryption Type

Рисунок 3.37 – Налаштування пристрою IoT #1234-Cam

Налаштування аналогічних пристроїв відбуватиметься так само. Наразі необхідно перевірити, чи працюють коректно усі вищезгадані сервіси та проведені конфігурації. Скористаємось командами перевірки сервісів за мережових підключень до пристроїв.

Організуємо перевірку на правильність розділу на віртуальні підмережі з мережних пристроїв організації. Зображення (рис. 3.38), показує, що дане розділення існує, за необхідності трафік можливо обмежити між віртуальними мережами за допомоги списків доступу.

Перевіримо раніше налаштоване розмежування VLAN для інтерфейсів. Як можна побачити, розподіл було виконано правильно, ми можемо в будь-який час заблокувати обмін даними між такими мережами, або створити додаткові із гнучким налаштуванням трафіку.

VLAN	Name	Status	Ports
1	default	active	Gig1/0/6, Gig1/0/7, Gig1/0/8, Gig1/0/9 Gig1/0/10, Gig1/0/11, Gig1/0/12, Gig1/0/14, Gig1/0/15, Gig1/0/16, Gig1/0/17, Gig1/0/18, Gig1/0/19, Gig1/0/20, Gig1/0/21, Gig1/0/22, Gig1/0/23, Gig1/0/24, Gig1/1/1 Gig1/1/2, Gig1/1/3, Gig1/1/4 Gig1/0/1, Gig1/0/2
5	HSRP-PROTO	active	
11	VLAN0011	active	
12	VLAN0012	active	
13	VLAN0013	active	
20	VLAN0020	active	
21	VLAN0021	active	
22	VLAN0022	active	
23	VLAN0023	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
5	enet	100005	1500	-	-	-	-	-	0	0
11	enet	100011	1500	-	-	-	-	-	0	0
12	enet	100012	1500	-	-	-	-	-	0	0
13	enet	100013	1500	-	-	-	-	-	0	0
20	enet	100020	1500	-	-	-	-	-	0	0
21	enet	100021	1500	-	-	-	-	-	0	0

Рисунок 3.38 – Вивід команди show vlan на комутаторі

Переконаємось що налаштування DHCP-серверу працюють:

```

S-LAN#sh ip dhcp binding
IP address      Client-ID/      Lease expiration      Type
                Hardware address
10.20.2.3       000C.8591.D277  --                     Automatic
20.2.0.8        0000.0CEB.8001  --                     Automatic
S-LAN#sh ip dhcp pool

Pool WLAN1 :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)          : 0 / 0
Total addresses                   : 254
Leased addresses                  : 0
Excluded addresses                : 9
Pending event                     : none

1 subnet is currently in the pool
Current index      IP address range      Leased/Excluded/Total
10.10.1.1         10.10.1.1 - 10.10.1.254  0 / 9 / 254

Pool L1-1 :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)          : 0 / 0
Total addresses                   : 254
Leased addresses                  : 1
Excluded addresses                : 9
Pending event                     : none

```

Рисунок 3.39 – Перевірка командами >sh ip dhcp binding та >sh ip dhcp pool

IP Configuration

☒ DHCP

☐ Static

IPv4 Address: 10.20.2.4

Subnet Mask: 255.255.255.0

Рисунок 3.40 – Перевірка DHCP на робочій станції WS3-2

Виконаємо перевірку inter-VLAN маршрутизації. Для цього скористаємось робочою станцією та командним рядком.

```

C:\>ping 20.2.0.4

Pinging 20.2.0.4 with 32 bytes of data:

Request timed out.
Reply from 20.2.0.4: bytes=32 time<1ms TTL=127
Reply from 20.2.0.4: bytes=32 time<1ms TTL=127
Reply from 20.2.0.4: bytes=32 time<1ms TTL=127

Ping statistics for 20.2.0.4:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

Рисунок 3.41 – Перевірка досяжності сусідніх будівель з WS3-2

Роботу протоколу маршрутизації HSRP можемо перевірити за командою show standby.

Перевіримо правильність роботи HSRP – виведемо діагностичні команди щодо HSRP на відповідних пристроях (рис. 3.42-3.43).

```
R-Main#sh standby
GigabitEthernet0/0/1 - Group 1
State is Active
  5 state changes, last state change 00:00:18
Virtual IP address is 10.5.7.6
Active virtual MAC address is 0000.0C07.AC01
  Local virtual MAC address is 0000.0C07.AC01 (v1 default)
Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.805 secs
Preemption disabled
Active router is local
Standby router is 10.5.7.2
Priority 50 (configured 50)
  Track interface GigabitEthernet0/0/0 state Up decrement 10
Group name is hsrp-Gig0/0/1-1 (default)
R-Main#sh standby brief
      P indicates configured to preempt.
      |
Interface    Grp  Pri P State    Active    Standby
Gig0/0/1     1   50  Active local     10.5.7.2
```

Рисунок 3.42 – Перевірка роботи протоколу HSRP на пристрої R-Main

```
R-Back#sh standby
GigabitEthernet0/0/1 - Group 1
State is Standby
  9 state changes, last state change 00:00:38
Virtual IP address is 10.5.7.6
Active virtual MAC address is 0000.0C07.AC01
  Local virtual MAC address is 0000.0C07.AC01 (v1 default)
Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.71 secs
Preemption disabled
Active router is 10.5.7.1
Standby router is local
Priority 45 (configured 45)
  Track interface GigabitEthernet0/0/0 state Up decrement 10
Group name is hsrp-Gig0/0/1-1 (default)
R-Back#sh standby brief
      P indicates configured to preempt.
      |
Interface    Grp  Pri P State    Active    Standby
Gig0/0/1     1   45  Standby 10.5.7.1  local
```

Рисунок 3.43 – Перевірка роботи протоколу HSRP на пристрої R-Back

Перевіримо роботу протоколу HTTP/S шляхом завантаження сторінки:



Рисунок 3.44 – Успішна перевірка роботи протоколу HTTP всередині мережі

Перевіримо роботу TFTP шляхом відправки дампу конфігурації мережевого пристрою.

Тепер спробуємо скопіювати стартову конфігурацію пристрою на сервер, тим самим перевіривши TFTP (рис. 3.45-3.46).

```
R-Main#copy startup-config tftp
Address or name of remote host []? 20.2.0.3
Destination filename [R-Main-config]?

Writing startup-config...!!
[OK - 2130 bytes]

2130 bytes copied in 0.024 secs (88750 bytes/sec)
R-Main#
```

Рисунок 3.45 – Успішна відправка файлу-копії config startup на TFTP сервер

Перевіримо збережені події журналу SYSLOG у базі даних:

53	12.19.2023 08:11:03.675 AM	110.101.1.2	%LINK-3-UPDOWN: Interfa...
54	12.19.2023 08:11:03.675 AM	110.101.1.2	%LINEPROTO-5-UPDOWN:...
55	12.19.2023 08:11:14.360 AM	110.101.1.2	%LINK-5-CHANGED: ...
56	12.19.2023 08:11:14.360 AM	110.101.1.2	%LINEPROTO-5-UPDOWN:...
57	12.19.2023 08:20:02.324 AM	10.5.7.1	%SYS-5-CONFIG_I: Configured from console b...
58	12.19.2023 08:21:47.309 AM	10.5.7.2	%SYS-5-CONFIG_I: Configured from console b...
59	12.19.2023 08:31:55.714 AM	10.5.7.1	%SYS-5-CONFIG_I: Configured from console b...

Рисунок 3.46 – Перевірка журналу подій SYSLOG

Перевіримо правильність роботи протоколу мережевого часу:

```
R-Back#sh ntp status
Clock is synchronized, stratum 2, reference is 20.2.0.4
nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24
reference time is E8FEEAC2.000001BA (6:59:14.442 UTC Tue Dec 19 2023)
clock offset is 0.00 msec, root delay is 1.00 msec
root dispersion is 286.90 msec, peer dispersion is -137269716642208.80 msec.
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system
poll interval is 4, last update was 15 sec ago.
R-Back#sh ntp associations

address          ref clock      st  when    poll   reach  delay    offset
disp
*~20.2.0.4       127.127.1.1    1   16      16     133    1.00     0.00
-137269716642208.69
* sys.peer, # selected, + candidate, - outlier, x falseticker, ~ configured
```

Рисунок 3.47 – Вивід діагностичних перевірки часу на пристрої

Перевіримо зв'язок з майданчиком транспортних засобів через VPN-підключення. Для цього використаємо одну з робочих станцій для процесу пінгування а також застосуємо тестові команди на маршрутизаторі.

Надішлемо команду ping з WS3-1 (рис. 3.48), а потім перевіримо чи дійсно усі запити надійшли до віддаленого хоста. Враховуючи наявність міжмережевого екрану Meraki, будь-які запити із зовнішньої мережі до пристроїв (включаючи також Meraki), що знаходяться за ним, будуть відхилені. Це обмежить доступ злоумисникам до пристроїв на транспортних засобах, навіть якщо вони потраплять до локальної мережі організації.

```
Pinging 192.168.56.1 with 32 bytes of data:
Reply from 192.168.56.1: bytes=32 time<1ms TTL=252
Reply from 192.168.56.1: bytes=32 time<1ms TTL=252
Reply from 192.168.56.1: bytes=32 time=8ms TTL=252
Reply from 192.168.56.1: bytes=32 time<1ms TTL=252

Ping statistics for 192.168.56.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 8ms, Average = 2ms
```

Рисунок 3.48 – Перевірка з'єднання з маршрутизатором R-Field

Переконаємось, що відправлений пакет дійсно був закодований (рис. 3.49):

```
local ident (addr/mask/prot/port): (192.168.56.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (20.2.0.0/255.255.255.248/0/0)
current_peer 213.108.40.2 port 500
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 72, #pkts encrypt: 72, #pkts digest: 0
#pkts decaps: 44, #pkts decrypt: 44, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

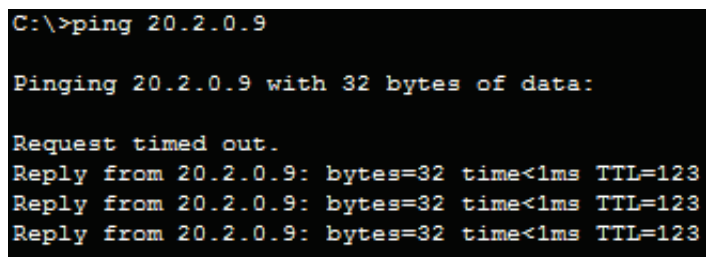
local crypto endpt.: 213.102.1.2, remote crypto endpt.:213.108.40.2
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0/0
current outbound spi: 0x938BF4E7(2475422951)

inbound esp sas:
  spi: 0x99CA1211(2580156945)
    transform: esp-aes 256 esp-sha-hmac ,
```

Рисунок 3.49 – Фрагмент виводу команди sh crypto ipsec sa

Передача даних була надійно зашифрована, так як між цими двома мережами був правильно побудований VPN-канал. На даному етапі ми успішно продемонстрували один із засобів підвищення рівня захищеності передачі трафіку з громадським транспортом.

Наостанок перевіримо, чи досяжний сервер ЦОД для пристроїв IoT транспортних засобів.



```
C:\>ping 20.2.0.9

Pinging 20.2.0.9 with 32 bytes of data:

Request timed out.
Reply from 20.2.0.9: bytes=32 time<1ms TTL=123
Reply from 20.2.0.9: bytes=32 time<1ms TTL=123
Reply from 20.2.0.9: bytes=32 time<1ms TTL=123
```

Рисунок 3.50 – Пінгування сервера ЦОД з мережі транспортного засобу

3.3. Рекомендації по застосуванню створеної моделі системи захисту

Проект системи варто рекомендувати до інтеграції з мережами транспортних компаній для подальшого вдосконалення та можливого розширення функціонального впливу.

Наразі система представлена низкою особливостей, які сприяють підвищенню рівня захищеності інформації що передається з транспортних засобів до серверів підприємства:

Клієнти (пасажери) можуть бути переконані, що їхні персональні дані захищені від можливого прослуховування трафіку та подальшого викрадення

Захищений канал передачі трафіку про поточний стан пристроїв та їх актуалізацію на транспортних засобах.

Проект системи має багато можливостей для розширення та модифікування за бажанням потенційного замовника, зокрема:

- зміна типу, характеристик, кількості тощо мережевого обладнання для захисту інформації;
- підключення сервісів моніторингу подій мережі транспортних засобів (знадобиться встановлення додаткового ПЗ на останніх).

Висновки до розділу 3

Даний розділ був представлений побудовою та подальшою перевіркою коректної роботи проекту по підвищенню рівня захищеності системи обміну

даними з громадським транспортом. Покроково зроблено аналіз кожної складової системи для захисту усієї мережі від витоку інформації з детальними прикладами налаштувань мережевого обладнання усіх трьох рівнів.

Оцінка працездатності показала непоганий результат, успішно перевірено вивантаження даних на сервер з віддаленої локальної мережі транспортного засобу, коректну роботу протоколу шифрування та стабільність VPN-тунелю в цілому. Розроблені рекомендації по підвищенню рівня захисту подібних систем.

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було досліджено актуальність теми підвищення рівня захищеності системи обміну даними з громадським транспортом. З'ясовано мету, об'єкт та предмет дослідження.

Аналіз аналогічних методів та засобів захисту довів, що питання захисту Інтернет-мереж у громадському транспорті досить актуальне на сьогоднішній день. Виробники мережевого та інформаційного обладнання пропонують низку комплексних та окремих безпекових рішень для покращення захисту мереж, пов'язаних із громадським транспортом а також більш гнучкого налаштування процесу обробки інформації пристроїв IoT.

Досліджено питання архітектури Internet of Things (IoT), розкрито та описано властивості кожного рівня моделей, представлених двома різними організаціями. Вивчено принципи використання шаблонів при проектуванні мереж, наведено приклади порівняно між собою дійсні та хибні шаблони.

За результатами дослідження трафіку від пристрою інформаційної системи доведено, що не усі виробники, так чи інакше, мають відповідний захист даних що передаються. В свою чергу, це може призвести до їх перехоплення зломисниками та подальшого використання у своїх особистих цілях. Відповідні висновки застосовано при проектуванні підсистеми підвищення рівня захищеності системи обміну даними з громадським транспортом.

Завдяки вивченню інформаційних джерел та нормативних документів та стандартів ДСТУ з технічного захисту інформації (ТЗІ), були розроблені вимоги до проєкту підвищення рівня захищеності системи обміну даними з громадським транспортом. Розроблено відповідний проєкт технічного завдання з використанням вищенаведених нормативів та стандартів.

Проаналізовано методи та засоби автентифікації та авторизації пристроїв до мереж, розглянуто можливе застосування протоколів аудиту та реєстрації.

Враховуючи здобуту інформацію, були створені:

- структурна схема проєкту підвищення рівня захищеності системи, на якій зображено основні складові проєкту мережі підприємства;

– UML-діаграма використання, яка відображає функції системи, які взаємодіють з користувачем, а також визначає ключові моменти забезпечення безпеки та контролю доступу.

Створено UML-діаграму класів, яка дозволила визначити обов'язковий функціонал під час вибору серед мережевих пристроїв. Проведено зіставлення кількісних та якісних характеристик, кількість та типи портів, наявність відповідних безпекових рішень та протоколів шифрування даних мережевого обладнання та згідно створеного технічного завдання, обрано найкращі пристрої для подальшої побудови проєкту мережі організації. Під час аналізу існуючих протоколів шифрування, була побудована UML-діаграма послідовності дій, яка детально розкриває шлях потоку даних між клієнтом та сервером.

Наведено створення проєкту підвищення рівня захищеності системи обміну даними з громадським транспортом на прикладі мережі транспортної компанії. Визначено наявність наступних складових мережі: віртуальні приватні мережі, VPN-tunneling, віддалене керування мережевими пристроями, встановлення міжмережевого екрану Meraki на шляху до локальних мереж транспортних засобів. Виконано покрокову побудову мережі проєкту з детальним описом дій на кожному з етапів. Перевірено на працездатність усі перелічені технічні та прикладні засоби для керування та захисту мережі у даному проєкті. Створену функціональну схему спроектованої мережі.

Результатом проведених етапів роботи став розгорнутий проєкт підвищення рівня захищеності системи обміну даними з громадським транспортом. Система автономно обробляє увесь вхідний та вихідний трафік, має підвищений рівень захищеності даних, які проходять процес шифрування, перш ніж потрапити на сервер.

Підсумовуючи, можна зробити висновок, що основне завдання кваліфікаційної роботи було виконане.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. JPA Yaacoub, H.N. Naura, O. Salman, A. Chebab. Ethical hacking for IoT: Security issues, challenges, solutions and recommendations. Internet of Things and Cyber-Physical Systems. Volume 3, 2023, P. 280–308.
2. Хохлов М.О., Єфіменко А.А., Вакалюк Т.А. Організація системи захищеного обміну даними транспортного підприємства із рухомим складом / Михайло Хохлов // Тези III Всеукраїнської науково-практичної Інтернет-конференції «Сучасні комп'ютерні та інформаційні системи і технології», м. Київ: Таврійський національний університет імені В. І. Вернадського, 2022. – С. 129-131.
3. Хохлов М.О., Вакалюк Т.А. Захист передачі інформації на рухомому транспорті при використанні технології LTE. / Михайло Хохлов // Тези V Всеукраїнської науково-практичної інтернет-конференції студентів, аспірантів та молодих вчених «Сучасні інформаційні системи та технології», м. Хмельницький: Херсонський національний технічний університет, 2022. – С. 167-168.
4. Директива ЄС про мережеву та інформаційну безпеку NIS EU 2016/1148 [Електронний ресурс] – Режим доступу до ресурсу: https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF (дата звернення: 05.12.2023)
5. Бурячок В. Л. Технології забезпечення безпеки мережної інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.
6. Railway-News. Cisco IoT Solution Brief – Connected Mass Transit. San Jose, CA, 95134, USA. 2018. URL: <https://railway-news.com/download/cisco-iot-solution-brief-connected-mass-transit/> (last access: 05.12.2023)
7. Sethi P., Sarangi S.R. Internet of Things: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engineering. Hindawi. 2017. P. 1-25.
8. Recommendation ITU-T Y.2060. International Telecommunication Union. Effective from 2012-06-15. 2012. 22 p.
9. McCain D. Coursey C. Implementing Cellular IoT Solutions for Digital Transformation. Packt Publishing. Birmingham. UK. 2023. 202 p.

10. Panasenko Y., Nimratz D. What's IoT edge computing: examples, benefits, and prospects for reducing costs. Yalantis Blog. URL: <https://yalantis.com/blog/edge-computing-in-iot/> (last access: 05.12.2023)

11. Закон України «Про інформацію» від 02.10.1992 № 2657-XII. [Електронний ресурс] – Режим доступу до ресурсу: https://zakononline.com.ua/documents/show/151399__591468 (дата звернення: 08.11.2023)

12. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Електронний ресурс] – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80> (дата звернення: 08.11.2023)

13. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.1999 № 1229/99 [Електронний ресурс] – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/1229/99> (дата звернення: 08.11.2023)

14. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою Кабінету Міністрів України від 29.03.2006 № 373 [Електронний ресурс] – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text> (дата звернення: 08.11.2023)

15. Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141 [Електронний ресурс] – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/z0868-99#Text> (дата звернення: 08.11.2023)

16. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс] – Режим доступу до ресурсу: https://tzi.ua/ua/nd_tz_1.1-002-99.html (дата звернення: 08.11.2023)

17. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс] – Режим доступу до ресурсу: <https://tzi.com.ua/downloads/2.5-004-99.pdf> (дата звернення: 08.11.2023)

18. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Електронний ресурс] – Режим доступу до ресурсу: <https://tzi.ua/assets/files/НД-ТЗІ-2.5-005--99.pdf> (дата звернення: 08.11.2023)

19. НД ТЗІ 2.7-009-09 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу [Електронний ресурс] – Режим доступу до ресурсу: <https://tzi.com.ua/downloads/2.7-009-09.pdf> (дата звернення: 08.11.2023)

20. НД ТЗІ 2.7-010-09 Методичні вказівки з оцінювання рівня гарантій коректності реалізації функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу [Електронний ресурс] – Режим доступу до ресурсу: <https://tzi.com.ua/downloads/2.7-010-09.pdf> (дата звернення: 08.11.2023)

21. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу [Електронний ресурс] – Режим доступу до ресурсу: <https://tzi.com.ua/downloads/3.6-001-2000.pdf> (дата звернення: 08.11.2023)

22. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі [Електронний ресурс] – Режим доступу до ресурсу: <https://tzi.com.ua/downloads/3.7-001-99.pdf> (дата звернення: 08.11.2023)

23. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі [Електронний ресурс] – Режим доступу до ресурсу: <https://tzi.com.ua/downloads/3.7-003-2005.pdf> (дата звернення: 08.11.2023)

24. ДБН А.2.2-2-96 Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та проектної документації для будівництва, затверджені наказом Держкоммістобудування України від 02.09.1996 № 156 [Електронний ресурс] – Режим доступу до ресурсу: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=5065 (дата звернення: 08.11.2023)

25. Vo N-S., Vien Q-T., Hoang V-P. Industrial Networks and Intelligent Systems. 7th EAI International Conference, INISCOM 2021, Hanoi, Vietnam, April 22-23, 2021. 514 p.
26. IEEE 802.1X. Effective from 2020-02-28. Official edition. 2020. URL: <https://standards.ieee.org/ieee/802.1X/7345/> (last access: 28.11.2023)
27. Приходько С. Віртуальні локальні мережі VLAN методичні вказівки до лабораторних, практичних занять і самостійної роботи з дисциплін : навч. посіб. / С.І. Приходько, О.С. Жученко, М.А. Штомпель, С.В. Сколота. Харків, 2018. 42 с.
28. Маршрутизатор Cisco ISR800, опис та характеристики. [Електронний ресурс] – Режим доступу до ресурсу: <https://stack-systems.com.ua/marshrutizator-cisco-881-k9> (дата звернення: 07.11.2023)
29. Комутатор Cisco Catalyst 3650. [Електронний ресурс] – Режим доступу до ресурсу: <https://lantorg.com/products/kommutator-cisco-catalyst-3650-24ts-sws-c3650-24ts-s> (дата звернення: 08.11.2023)
30. Cisco Catalyst 2960-X. Cisco Systems. [Електронний ресурс] – Режим доступу до ресурсу: <https://www.cisco.com/c/en/us/support/switches/catalyst-2960-x-series-switches/series.html/> (дата звернення: 08.11.2023)
31. Маршрутизатор Cisco ISR4331. [Електронний ресурс] – Режим доступу до ресурсу: <https://itel.ua/isr4331-seck9> (дата звернення: 04.12.2023)
32. Cisco Meraki MX65W-HW. URL: <https://inetworks.com.ua/prod17978-cisco-meraki-mx65w-hw.html> (дата звернення: 08.11.2023)
33. Cisco Training Events CCIE #29071. Skvorchevsky A. New WiFi abilities. App Hosting, User Defined Network. Cisco, 2021. 43 p.
34. Cisco Catalyst 2960 Series. Cisco E-catalog. URL: <https://www.cisco.com/c/en/us/support/switches/catalyst-2960-series-switches-/series.html> (last access: 09.11.2023)
35. Hongil Kim, Jiho Lee, Eunkyoo Lee, Yongdae Kim. Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane. Korea Advanced Institute of Science and Technology, Korea, 2019. 16 p.
36. Недашківський О.Л. Технології та протоколи Інфокомунікаційних мереж (частина друга) / О.Л. Недашківський. – К.:ДУТ, 2018. [Електронний ресурс] – Режим

доступу до ресурсу: https://dut.edu.ua/uploads/l_1799_38438908.pdf (дата звернення: 10.12.2023)

37. Cryptology and Network Security. 16th International Conference, CANS 2017, Hong Kong, China, November 30—December 2, 2017, Revised Selected Papers. 2018. 548 p.

38. Young-Jin Kim, Vladimir Kolesnikov, Hongseok Kim, Marina Thottan. SSTP: a Scalable and Secure Transport Protocol for Smart Grid Data Collection. Bell Labs, Alcatel-Lucent, Murray Hill, NJ, USA, 2011.

39. Dan Harkins, Charlie Kaufman, Radia Perlman. Overview of IKEv2. Fifty-second internet engineering task force, USA, 9-14 December 2001. 16 p. URL: <https://www.ietf.org/proceedings/52/slides/ipsec-10.pdf> (last access: 13.11.2023)

40. Helali S. Systems and Network Infrastructure Integration. Wiley. Hoboken, NJ 07030, USA. – 2020. 208 p.

41. Nefkens P-J. Transforming Campus Networks to Intent-Based Networking. Pearson Education. 2019. 320 p.

42. Feature Overview and Configuration Guide. DHCP. Allied Telesis, 2018. 19 p. URL: https://www.alliedtelesis.com/sites/default/files/documents/feature_guides/dhcp_feature_overview_guide.pdf (last access: 15.11.2023)

43. Cisco Configuration Examples and TechNotes. Configure InterVLAN Routing on Layer 3 Switches. 2023. URL: <https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/41860-howto-L3-intervlanrouting.html> (last access: 15.11.2023)

44. Приходько С. І., Жученко О. С., Штомпель М. А., Лисечко В. П. ПІДВИЩЕННЯ НАДІЙНОСТІ ШЛЮЗУ. ПРОТОКОЛ HSRP: навч. посіб. / С. І. Приходько. Харків : УДАЗТ, 2018. 42 с.

45. Mendel Rosenblum. CS142 Lecture Notes. HTTP. 2011. URL: <https://web.stanford.edu/class/cs142/lectures/HTTP.pdf> (last access: 18.11.2023)

46. IBM i Version 7.2. NTFTP. 2013. P.3-8. URL: https://www.ibm.com/docs/en/ssw_ibm_i_72/rzal5/rzal5pdf.pdf (last access 19.11.2023)

47. RFC-1119. Network Time Protocol (Version 2). Specification and Implementation. Effective from 1989-19-11. Official edition. 1989. URL: <https://www.rfc-editor.org/rfc/rfc1119.pdf> (last access 22.11.2023)

48. Mario Čagalj. The Secure Shell (SSH) Protocol. University of Split, FESB, 2019. URL: http://marjan.fesb.hr/~mcagalj/CNS/Lectures/SSH_protocol.pdf (last access 25.11.2023)

ДОДАТКИ

Топологія мережі

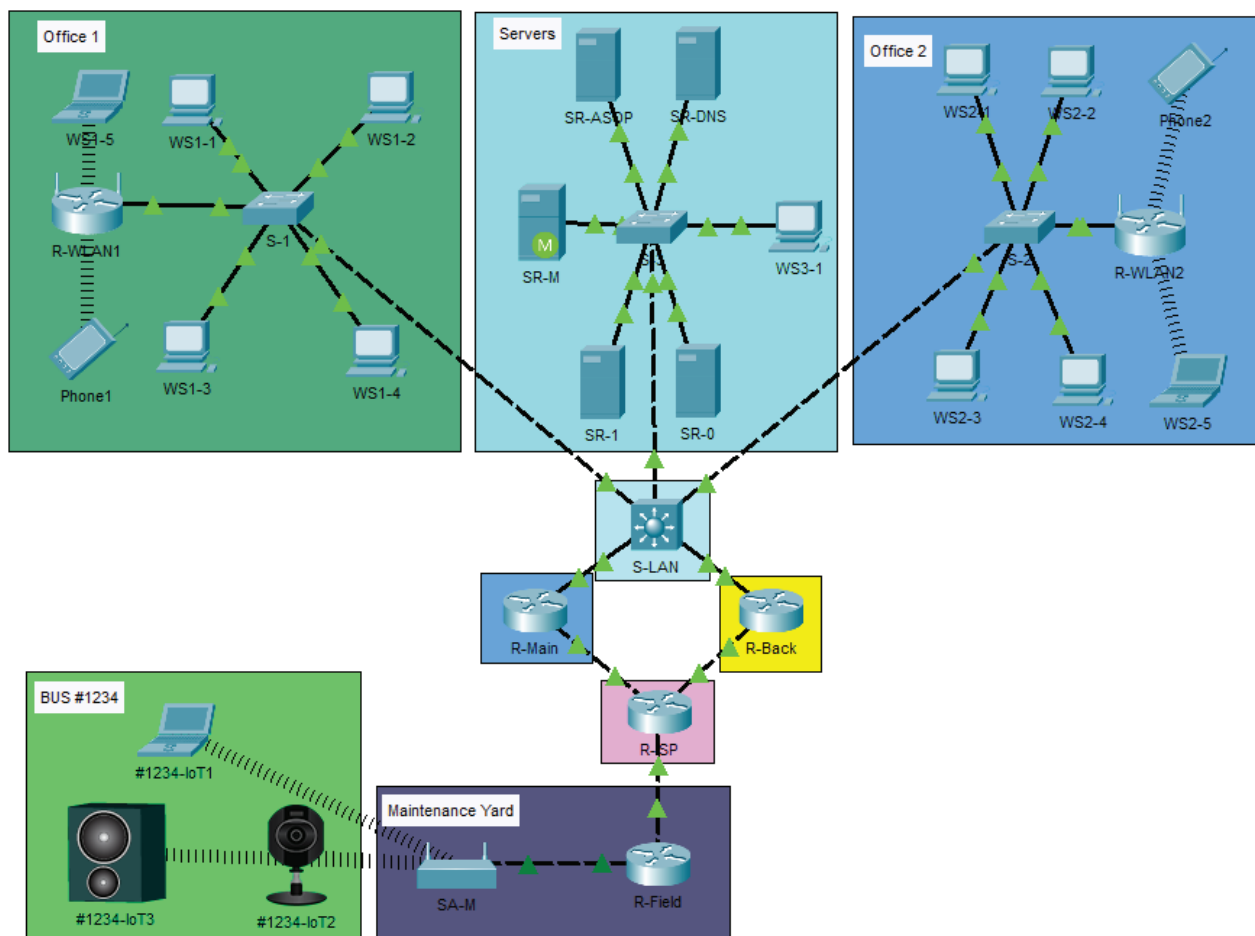


Рисунок А.1 – Топологія мережі

Параметри інтерфейсів пристроїв мережі

Таблиця Б.1 – Параметри інтерфейсів пристроїв мережі

Пристрій	Інтерфейси	Підключення до пристрою	Підключення до інтерфейсів
Маршрутизатор R-ISP	Gi0/0/0	Маршрутизатор R-Main	Gi0/0/0
	Gi0/0/1	Маршрутизатор R-Back	Gi0/0/0
	Gi0/0/2	Маршрутизатор R-Field	Gi0/0/0
Маршрутизатор R-Main	Gi0/0/0	Маршрутизатор R-ISP	Gi0/0/0
	Gi0/0/1	Комутатор S-LAN	Gi1/0/1
Маршрутизатор R-Back	Gi0/0/0	Маршрутизатор R-ISP	Gi0/0/1
	Gi0/0/1	Комутатор S-LAN	Gi1/0/2
Маршрутизатор R-Field	Gi0/0/0	Маршрутизатор R-ISP	Gi0/0/2
	Gi0/0/1	Міжмережевий екран SA-M	Internet 1
Комутатор S-LAN	Gi1/0/1	Маршрутизатор R-Main	Gi0/0/1
	Gi1/0/2	Маршрутизатор R-Back	Gi0/0/1
	Gi1/0/3	Комутатор S-1	Gi0/1
	Gi1/0/4	Комутатор S-2	Gi0/1
	Gi1/0/5	Комутатор S-3	Gi0/1
Комутатор S-1	Gi0/1	Комутатор S-LAN	Gi1/0/3
	Fa0/1	Робоча станція WS1-1	Fa0
	Fa0/2	Робоча станція WS1-2	Fa0
	Fa0/9	Робоча станція WS1-3	Fa0
	Fa0/22	Робоча станція WS1-4	Fa0
	Gi0/2	Маршрутизатор R-WLAN1	0/0
Комутатор S-2	Gi0/1	Комутатор S-LAN	Gi1/0/4
	Fa0/1	Робоча станція WS2-1	Fa0
	Fa0/2	Робоча станція WS2-2	Fa0
	Fa0/15	Робоча станція WS2-4	Fa0
	Fa0/20	Робоча станція WS2-3	Fa0
	Gi0/2	Маршрутизатор R-WLAN2	0/0

Комутатор S-3	Gi0/1	Комутатор S-LAN	Gi1/0/5
	Gi1/1	Сервер SR-0	Gi0
	Gi2/1	Сервер SR-1	Gi0
	Gi3/1	Сервер SR-ASOP	Gi0
	Gi4/1	Сервер SR-DNS	Gi0
	Gi5/1	Сервер SR-M	Gi0
	Fa6/1	Робоча станція WS3-1	Fa0
Міжмережевий екран SA-M	Internet 1	Маршрутизатор R-Field	Gi0/0/1
	Wireless	Робоча станція 1234-IoT1	Wireless
		Відеокамера 1234-IoT2	Wireless
		Динамік 1234-IoT3	Wireless
Маршрутизатор R-WLAN1	0/0	Комутатор S-1	Gi0/2
	Wireless	Телефон P-1	Wireless
		Робоча станція WS1-5	Wireless
Маршрутизатор R-WLAN2	0/0	Комутатор S-2	Gi0/2
	Wireless	Телефон P-2	Wireless
		Робоча станція WS2-5	Wireless
Робоча станція WS1-1	Fa0	Комутатор S-1	Fa0/1
Робоча станція WS1-2	Fa0	Комутатор S-1	Fa0/2
Робоча станція WS1-3	Fa0	Комутатор S-1	Fa0/23
Робоча станція WS1-4	Fa0	Комутатор S-1	Fa0/24
Робоча станція WS1-5	Wireless	Маршрутизатор R-WLAN1	Wireless
Робоча станція WS2-1	Fa0	Комутатор S-2	Fa0/1
Робоча станція WS2-2	Fa0	Комутатор S-2	Fa0/2
Робоча станція WS2-3	Fa0	Комутатор S-2	Fa0/20
Робоча станція WS2-4	Fa0	Комутатор S-2	Fa0/15
Робоча станція WS2-5	Wireless	Маршрутизатор R-WLAN2	Wireless
Робоча станція WS3-1	Fa0	Комутатор S-3	Fa6/1
Робоча станція 1234-IoT1	Wireless	Маршрутизатор R-WLAN-F	Wireless
Вебкамера 1234-IoT2	Wireless	Маршрутизатор R- WLAN-F	Wireless
Гучномовець 1234-IoT3	Wireless	Маршрутизатор R- WLAN-F	Wireless
Телефон P-1	Wireless	Маршрутизатор R-WLAN1	Wireless

Закінчення табл. Б.1

Телефон P-2	Wireless	Маршрутизатор R-WLAN2	Wireless
Сервер SR-0	Gi0	Комутатор S-3	Gi1/1
Сервер SR-1	Gi0	Комутатор S-3	Gi2/1
Сервер SR-ASOP	Gi0	Комутатор S-3	Gi3/1
Сервер SR-DNS	Gi0	Комутатор S-3	Gi4/1
Сервер SR-M	Gi0	Комутатор S-3	Gi5/1

Параметри адресації пристроїв мережі

Таблиця В.1 - Параметри адресації пристроїв мережі

Підмережа/ Пристрій	Інтерфейс/Мереж- ний адаптер/Шлюз	ІР-адреса	Маска підмережі	Префікс
Маршрутизатор R-ISP	Gi0/0/0	213.108.40.1	255.255.255.252	/30
	Gi0/0/1	213.108.41.1	255.255.255.252	/30
	Gi0/0/2	213.102.1.1	255.255.255.252	/30
Маршрутизатор R-Main	Gi0/0/0	213.108.40.2	255.255.255.252	/30
	Gi0/0/1	10.5.7.1	255.255.255.248	/29
Маршрутизатор R-Back	Gi0/0/0	213.108.41.2	255.255.255.252	/30
	Gi0/0/1	10.5.7.2	255.255.255.248	/29
Маршрутизатор R-Field	Gi0/0/0	213.102.1.2	255.255.255.252	/30
	Gi0/0/1	192.168.56.1	255.255.255.0	/24
Комутатор S-LAN	Vlan1	110.101.1.1	255.255.255.0	/24
	Vlan5	10.5.7.3	255.255.255.248	/29
	Vlan11	10.10.1.1	255.255.255.0	/24
	Vlan12	10.20.2.1	255.255.255.0	/24
	Vlan13	10.30.3.1	255.255.255.0	/24
	Vlan21	20.10.1.1	255.255.255.0	/24
	Vlan22	20.20.2.1	255.255.255.0	/24
	Vlan23	20.30.3.1	255.255.255.0	/24
	Vlan20	20.2.0.1	255.255.255.0	/24
КомутаторS-1	Vlan1	110.101.1.2	255.255.255.0	/24
	Vlan11	10.10.1.2	255.255.255.0	/24
	Vlan12	10.20.2.2	255.255.255.0	/24
	Vlan13	10.30.3.2	255.255.255.0	/24
КомутаторS-2	Vlan1	110.101.1.3	255.255.255.0	/24
	Vlan21	20.10.1.2	255.255.255.0	/24
	Vlan22	20.20.2.2	255.255.255.0	/24
	Vlan23	20.30.3.2	255.255.255.0	/24
КомутаторS-3	Vlan1	110.101.1.4	255.255.255.0	/24
	Vlan20	20.2.0.2	255.255.255.0	/24
Міжмережевий екран SA-M	Internet 1	DHCP		
	Wireless	192.168.0.1	255.255.255.0	/24
Маршрутизатор R-WLAN1	0/0	DHCP		
	Wireless	192.168.1.1	255.255.255.0	/24
Маршрутизатор R-WLAN2	0/0	DHCP		
	Wireless	192.168.2.1	255.255.255.0	/24
Робоча станція WS1-1	Fa0	DHCP		
Робоча станція WS1-2	Fa0			
Робоча станція WS1-3	Fa0			
Робоча станція WS1-4	Fa0			
Робоча станція WS1-5	Wireless			
Робоча станція WS2-1	Fa0			
Робоча станція WS2-2	Fa0			
Робоча станція WS2-3	Fa0			
Робоча станція WS2-4	Fa0			
Робоча станція WS2-5	Wireless			

Продовження табл. В.1

Підмережа/ Пристрій	Інтерфейс/Мереж- ний адаптер/Шлюз	ІР-адреса	Маска підмережі	Префікс
Робоча станція 1234-IoT1	Wireless	DHCP		
Вебкамера 1234-IoT2	Wireless			
Гучномовець 1234-IoT3	Wireless			
Телефон P-1	Wireless			
Телефон P-2	Wireless			
Сервер SR-0	Gi0	20.2.0.3	255.255.255.0	/24
Сервер SR-1	Gi0	20.2.0.4	255.255.255.0	/24
Сервер SR-DNS	Gi0	20.2.0.5	255.255.255.0	/24
Сервер SR-ASOP	Gi0	20.2.0.6	255.255.255.0	/24
Робоча станція WS3-1	Fa0	DHCP		

Лістинги конфігураційних файлів маршрутизуючого обладнання

Лістинг Г.1 – Конфігураційний файл маршрутизатора R-Main

R-Main

```

version 15.4
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
hostname R-Main
logging userinfo
login block-for 10 attempts 3 within 3
login on-failure log
login on-success log
enable secret 5
$1$mERr$Hk2hnbY8CmMl.VUj9bnT80
clock timezone EET 2
no ip cef
no ipv6 cef
username Zlinet privilege 15 secret 5
$1$mERr$Ynu1Bsv8Qb4Qcv9AnjDCXl
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 5
crypto isakmp key myuniquekey address
213.102.1.2
crypto ipsec transform-set sectunnel esp-
aes 256 esp-sha-hmac
crypto map secludedmap 10 ipsec-isakmp
  set peer 213.102.1.2
  set pfs group5
  set security-association lifetime
seconds 86400
  set transform-set sectunnel
  match address 110
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 60
ip domain-name main.it
spanning-tree mode pvst
interface GigabitEthernet0/0/0
  ip address 213.108.40.2 255.255.255.252
  duplex auto
  speed auto
  crypto map secludedmap
interface GigabitEthernet0/0/1
  ip address 10.5.7.1 255.255.255.248
  duplex auto
  speed auto
  standby 1 ip 10.5.7.6
  standby 1 priority 50
  standby 1 track GigabitEthernet0/0/0
  standby 0 timers 5 10
interface Vlan1
  no ip address
  shutdown
router ospf 1
  log-adjacency-changes
  network 213.108.40.0 0.0.0.3 area 0
  network 10.5.7.0 0.0.0.7 area 0
ip classless
ip route 20.2.0.0 255.255.255.0 10.5.7.3
ip flow-export version 9
ip access-list extended sl_def_acl
  deny tcp any any eq telnet
  deny tcp any any eq www
  deny tcp any any eq 22
  permit tcp any any eq 22
access-list 110 permit ip 20.2.0.0
0.0.0.7 192.168.56.0 0.0.0.255
no cdp run
banner motd # Connection to router R-Main
For legal users only #
logging trap debugging
logging 20.2.0.4
line con 0
  logging synchronous
  login local
line aux 0
line vty 0 4
  logging synchronous
  login local
  transport input ssh
  transport output ssh
ntp authentication-key 1 md5
08701E1D3E181103455355 7
ntp authenticate
ntp trusted-key 1
ntp server 20.2.0.4 key 1
ntp update-calendar
end

```

Лістинг Г.2 – Конфігураційний файл маршрутизатора R-ISP

R-ISP

```
version 15.4
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
hostname R-ISP
logging userinfo
login block-for 10 attempts 3 within 3
login on-failure log
login on-success log
enable secret 5
$1$mERr$Hk2hnbY8CmMl.VUj9bnT80
clock timezone EET 2
ip cef
no ipv6 cef
username Zlinet privilege 15 secret 5
$1$mERr$Ynu1Bsv8Qb4Qcv9AnjDCX1
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 60
ip domain-name internet.com
spanning-tree mode pvst
interface Loopback1
    ip address 172.16.0.1 255.255.255.252
interface GigabitEthernet0/0/0
    ip address 213.108.40.1 255.255.255.252
    duplex auto
    speed auto
interface GigabitEthernet0/0/1
    ip address 213.108.41.1 255.255.255.252
    duplex auto
    speed auto
interface GigabitEthernet0/0/2
    media-type sfp
    ip address 213.102.1.1 255.255.255.252
    duplex auto
    speed auto
interface GigabitEthernet0/1/0
    switchport mode access
    switchport nonegotiate
interface GigabitEthernet0/1/1
    switchport mode access
    switchport nonegotiate
interface GigabitEthernet0/1/2
    switchport mode access
    switchport nonegotiate
interface GigabitEthernet0/1/3
    switchport mode access
    switchport nonegotiate
interface Vlan1
    no ip address
    shutdown
router ospf 1
    log-adjacency-changes
    redistribute static
    passive-interface Loopback1
    network 213.108.40.0 0.0.0.3 area 0
    network 172.16.0.0 0.0.0.3 area 0
    network 213.102.1.0 0.0.0.3 area 0
    network 213.108.41.0 0.0.0.3 area 0
ip classless
ip route 20.2.0.0 255.255.255.0
213.108.40.2
ip route 20.2.0.0 255.255.255.0
213.108.41.2 2
ip route 0.0.0.0 0.0.0.0 Loopback1
ip flow-export version 9
ip access-list extended sl_def_acl
    deny tcp any any eq telnet
    deny tcp any any eq www
    deny tcp any any eq 22
    permit tcp any any eq 22
banner motd # Connection to router ISP
For legal users only #
logging trap debugging
logging 20.2.0.4
line con 0
    logging synchronous
    login local
line aux 0
line vty 0 4
    logging synchronous
    login local
    transport input ssh
    transport output ssh
ntp authentication-key 1 md5
08701E1D3E181103455355 7
ntp authenticate
ntp trusted-key 1
ntp server 20.2.0.4 key 1
ntp update-calendar
!
end
```

Лістинг Г.3 – Конфігураційний файл маршрутизатора R-Field

R-Field

```
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
hostname R-Field
enable secret 5
$1$mERr$Hk2hnbY8CmMl.VUj9bnT80
ip dhcp pool WLAN0
    network 192.168.56.0 255.255.255.0
    default-router 192.168.56.1
    dns-server 20.2.0.5

ip cef
no ipv6 cef
username Zlinet privilege 15 secret 5
$1$mERr$Ynu1Bsv8Qb4Qcv9AnjDCX1
crypto isakmp policy 10
    encr aes 256
    authentication pre-share
    group 5
crypto isakmp key myuniquekey address
213.108.40.2
crypto ipsec transform-set sectunnel esp-
aes 256 esp-sha-hmac
crypto map secludedmap 10 ipsec-isakmp
    set peer 213.108.40.2
    set peer 213.108.41.2
    set pfs group5
    set security-association lifetime
seconds 86400
    set transform-set sectunnel
    match address 110
spanning-tree mode pvst

interface GigabitEthernet0/0/0
    ip address 213.102.1.2 255.255.255.252
    duplex auto
    speed auto
    crypto map secludedmap
interface GigabitEthernet0/0/1
    ip address 192.168.56.1 255.255.255.0
    duplex auto
    speed auto
interface Vlan1
    no ip address
    shutdown
router ospf 110
    log-adjacency-changes
    network 213.102.1.0 0.0.0.3 area 0
    network 192.168.56.0 0.0.0.255 area 0
ip classless
ip flow-export version 9
access-list 110 permit ip 192.168.56.0
0.0.0.255 10.5.7.0 0.0.0.7
access-list 110 permit ip 192.168.56.0
0.0.0.255 20.2.0.0 0.0.0.7
line con 0
line aux 0
line vty 0 4
    login
ntp authentication-key 1 md5
08701E1D3E181103455355 7
ntp authenticate
ntp trusted-key 1
ntp server 20.2.0.4 key 1
ntp update-calendar
end
```

Лістинг Г.4 – Конфігураційний файл маршрутизатора R-Back

R-Back

```
version 15.4
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
hostname R-Back
logging userinfo
login block-for 10 attempts 3 within 3
login on-failure log
login on-success log
enable secret 5
$1$mERr$Hk2hnbY8CmMl.VUj9bnT80
clock timezone EET 2
no ip cef
no ipv6 cef
username Zlinet privilege 15 secret 5
$1$mERr$YnUlBsv8Qb4Qcv9AnjDCXl
crypto isakmp policy 10
  encr aes 256
  authentication pre-share
  group 5
crypto isakmp key myuniquekey address
213.102.1.2
crypto ipsec transform-set sectunnel esp-
aes 256 esp-sha-hmac
crypto map secludedmap 10 ipsec-isakmp
  set peer 213.102.1.2
  set pfs group5
  set security-association lifetime
seconds 86400
  set transform-set sectunnel
  match address 110
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 60
ip domain-name Rback.backup
spanning-tree mode pvst
interface GigabitEthernet0/0/0
  ip address 213.108.41.2 255.255.255.252
  duplex auto
  speed auto
  crypto map secludedmap
interface GigabitEthernet0/0/1
  ip address 10.5.7.2 255.255.255.248
  duplex auto
  speed auto
  standby 1 ip 10.5.7.6
  standby 1 priority 45
  standby 1 track GigabitEthernet0/0/0
  standby 0 timers 5 10
interface Vlan1
  no ip address
  shutdown
router ospf 1
  log-adjacency-changes
  network 213.108.41.0 0.0.0.3 area 0
  network 10.5.7.0 0.0.0.7 area 0
ip classless
ip route 20.2.0.0 255.255.255.0 10.5.7.3
ip flow-export version 9
ip access-list extended sl_def_acl
  deny tcp any any eq telnet
  deny tcp any any eq www
  deny tcp any any eq 22
  permit tcp any any eq 22
access-list 110 permit ip 10.5.7.0
0.0.0.7 192.168.56.0 0.0.0.255
access-list 110 permit ip 20.2.0.0
0.0.0.7 192.168.56.0 0.0.0.255
no cdp run
banner motd # Connection to router R-Back
For legal users only #
logging trap debugging
logging 20.2.0.4
line con 0
  logging synchronous
  login local
line aux 0
line vty 0 4
  logging synchronous
  login local
  transport input ssh
  transport output ssh
ntp authentication-key 1 md5
08701E1D3E181103455355 7
ntp authenticate
ntp trusted-key 1
ntp server 20.2.0.4 key 1
ntp update-calendar
end
```

Лістинг конфігураційних файлів комутаторів внутрішньої локальної мережі

Лістинг Д.1 – Конфігураційний файл комутатора S-LAN

```

S-LAN#sh run
Building configuration...

version 16.3.2
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
hostname S-LAN
logging userinfo
login block-for 10 attempts 3 within 3
login on-failure log
login on-success log
enable secret 5
$1$mERr$Hk2hnbY8CmMl.VUj9bnT80
ip dhcp excluded-address 10.10.1.1
10.10.1.2
ip dhcp excluded-address 10.20.2.1
10.20.2.2
ip dhcp excluded-address 10.30.3.1
10.30.3.2
ip dhcp excluded-address 20.10.1.1
20.10.1.2
ip dhcp excluded-address 20.20.2.1
20.20.2.2
ip dhcp excluded-address 20.30.3.1
20.30.3.2
ip dhcp excluded-address 20.2.0.1
20.2.0.4
ip dhcp excluded-address 20.2.0.1
20.2.0.6
ip dhcp excluded-address 20.2.0.1
20.2.0.7
ip dhcp pool WLAN1
network 10.10.1.0 255.255.255.0
default-router 10.10.1.1
dns-server 20.2.0.5
domain-name wlan1.com
ip dhcp pool L1-1
network 10.20.2.0 255.255.255.0
default-router 10.20.2.1
dns-server 20.2.0.5
domain-name lan1-1.com
ip dhcp pool L1-2
network 10.30.3.0 255.255.255.0
default-router 10.30.3.1
dns-server 20.2.0.5
domain-name lan1-2.com
ip dhcp pool WLAN2
network 20.10.1.0 255.255.255.0
default-router 20.10.1.1
dns-server 20.2.0.5
domain-name wlan2.com
ip dhcp pool L2-1
network 20.20.2.0 255.255.255.0
default-router 20.20.2.1
dns-server 20.2.0.5
domain-name l2-1.com
ip dhcp pool Servers
network 20.2.0.0 255.255.255.0
default-router 20.2.0.1
dns-server 20.2.0.5
domain-name servers.com
ip dhcp pool L2-2
network 20.30.3.0 255.255.255.0
default-router 20.30.3.1
dns-server 20.2.0.5
domain-name l2-2.com
clock timezone EET 2
no ip cef
ip routing
no ipv6 cef
username Zlinet privilege 15 secret 5
$1$mERr$YnUlBsv8Qb4Qcv9AnjDCX1
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 60
ip domain-name SMain.it
spanning-tree mode pvst
interface GigabitEthernet1/0/1
switchport access vlan 5
switchport mode access
switchport nonegotiate
interface GigabitEthernet1/0/2
switchport access vlan 5
switchport mode access
switchport nonegotiate
interface GigabitEthernet1/0/3
switchport access vlan 13
switchport mode trunk
interface GigabitEthernet1/0/4

```

```

switchport access vlan 23
switchport mode trunk
interface GigabitEthernet1/0/5
switchport access vlan 20
switchport mode trunk
interface GigabitEthernet1/0/6
...
interface GigabitEthernet1/0/24
interface GigabitEthernet1/1/1
...
interface GigabitEthernet1/1/4
interface Vlan1
ip address 110.101.1.1 255.255.255.0
interface Vlan5
mac-address 0050.0f6b.d501
ip address 10.5.7.3 255.255.255.248
interface Vlan11
mac-address 0050.0f6b.d502
ip address 10.10.1.1 255.255.255.0
interface Vlan12
mac-address 0050.0f6b.d503
ip address 10.20.2.1 255.255.255.0
interface Vlan13
mac-address 0050.0f6b.d504
ip address 10.30.3.1 255.255.255.0
interface Vlan20
mac-address 0050.0f6b.d505
ip address 20.2.0.1 255.255.255.0
interface Vlan21
mac-address 0050.0f6b.d506
ip address 20.10.1.1 255.255.255.0
interface Vlan22
mac-address 0050.0f6b.d507
ip address 20.20.2.1 255.255.255.0
interface Vlan23
mac-address 0050.0f6b.d508
ip address 20.30.3.1 255.255.255.0
router ospf 1
router-id 10.5.7.3

```

```

log-adjacency-changes
network 10.5.7.0 0.0.0.7 area 0
network 10.10.1.0 0.0.0.255 area 0
network 10.20.2.0 0.0.0.255 area 0
network 10.30.3.0 0.0.0.255 area 0
network 20.10.1.0 0.0.0.255 area 0
network 20.20.2.0 0.0.0.255 area 0
network 20.30.3.0 0.0.0.255 area 0
network 20.2.0.0 0.0.0.255 area 0
ip classless
ip route 20.2.0.0 255.255.255.0 20.2.0.2
ip route 0.0.0.0 0.0.0.0 10.5.7.1
ip route 0.0.0.0 0.0.0.0 10.5.7.2 2
ip flow-export version 9
ip access-list extended sl_def_acl
deny tcp any any eq telnet
deny tcp any any eq www
deny tcp any any eq 22
permit tcp any any eq 22
banner motd # Connection to switch S-LAN
For legal users only #
logging trap debugging
logging 20.2.0.4
line con 0
logging synchronous
login local
line aux 0
line vty 0 4
logging synchronous
login local
transport input ssh
transport output ssh
ntp authentication-key 1 md5
08701E1D3E181103455355 7
ntp authenticate
ntp trusted-key 1
ntp server 20.2.0.4 key 1
ntp update-calendar
end

```

Лістинг Д.2 – Конфігураційний файл комутатора S-1

```
S-1#sh run
Building configuration...
version 15.0
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
hostname S-1
enable secret 5
$1$mERr$Hk2hnbY8CmM1.VUj9bnT80
clock timezone EET 2
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 60
ip domain-name S1.st
username Zlinet secret 5
$1$mERr$Ynu1Bsv8Qb4Qcv9AnjDCX1
spanning-tree mode pvst
spanning-tree extend system-id
interface FastEthernet0/1
  switchport access vlan 12
  switchport mode access
interface FastEthernet0/2
  switchport access vlan 12
  switchport mode access
interface FastEthernet0/3
  switchport access vlan 12
  switchport mode access
interface FastEthernet0/4
  switchport access vlan 12
  switchport mode access
interface FastEthernet0/5
  switchport access vlan 12
  switchport mode access
interface FastEthernet0/6
  switchport access vlan 12
  switchport mode access
interface FastEthernet0/7
  switchport access vlan 12
  switchport mode access
interface FastEthernet0/8
  switchport access vlan 12
  switchport mode access
interface FastEthernet0/9
  switchport access vlan 12
  switchport mode access
interface FastEthernet0/10
  switchport access vlan 12
  switchport mode access
interface FastEthernet0/11
  switchport access vlan 12
  switchport mode access
interface FastEthernet0/12
  switchport access vlan 12
  switchport mode access
interface FastEthernet0/13
  switchport access vlan 13
  switchport mode access
interface FastEthernet0/14
  switchport access vlan 13
  switchport mode access
interface FastEthernet0/15
  switchport access vlan 13
  switchport mode access
interface FastEthernet0/16
  switchport access vlan 13
  switchport mode access
interface FastEthernet0/17
  switchport access vlan 13
  switchport mode access
interface FastEthernet0/18
  switchport access vlan 13
  switchport mode access
interface FastEthernet0/19
  switchport access vlan 13
  switchport mode access
interface FastEthernet0/20
  switchport access vlan 13
  switchport mode access
interface FastEthernet0/21
  switchport access vlan 13
  switchport mode access
interface FastEthernet0/22
  switchport access vlan 13
  switchport mode access
interface FastEthernet0/23
  switchport access vlan 13
  switchport mode access
interface FastEthernet0/24
  switchport access vlan 13
  switchport mode access
interface GigabitEthernet0/1
  switchport mode trunk
interface GigabitEthernet0/2
  switchport access vlan 11
  switchport mode access
interface Vlan1
  ip address 110.101.1.2 255.255.255.0
interface Vlan11
  ip address 10.10.1.2 255.255.255.0
interface Vlan12
  ip address 10.20.2.2 255.255.255.0
interface Vlan13
  ip address 10.30.3.2 255.255.255.0
ip default-gateway 110.101.1.1
banner motd # Connection to switch S-1
For legal users only #
logging trap debugging
logging 20.2.0.4
line con 0
  logging synchronous
  login local
line vty 0 4
  logging synchronous
  login local
  transport input ssh
  transport output ssh
line vty 5 15
  login
ntp authenticate
ntp trusted-key 1
ntp server 20.2.0.4 key 1
end
```

Лістинг Д.3 – Конфігураційний файл комутатора S-2

```
S-2#sh run
Building configuration...
version 15.0
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
hostname S-2
enable secret 5
$1$mERr$Hk2hnbY8CmM1.VUj9bnT80
clock timezone EET 2
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 60
ip domain-name S2.sd
username Zlinet secret 5
$1$mERr$Ynu1Bsv8Qb4Qcv9AnjDCX1
spanning-tree mode pvst
spanning-tree extend system-id
interface FastEthernet0/1
  switchport access vlan 22
  switchport mode access
interface FastEthernet0/2
  switchport access vlan 22
  switchport mode access
interface FastEthernet0/3
  switchport access vlan 22
  switchport mode access
interface FastEthernet0/4
  switchport access vlan 22
  switchport mode access
interface FastEthernet0/5
  switchport access vlan 22
  switchport mode access
interface FastEthernet0/6
  switchport access vlan 22
  switchport mode access
interface FastEthernet0/7
  switchport access vlan 22
  switchport mode access
interface FastEthernet0/8
  switchport access vlan 22
  switchport mode access
interface FastEthernet0/9
  switchport access vlan 22
  switchport mode access
interface FastEthernet0/10
  switchport access vlan 22
  switchport mode access
interface FastEthernet0/11
  switchport access vlan 22
  switchport mode access
interface FastEthernet0/12
  switchport access vlan 22
  switchport mode access
interface FastEthernet0/13
  switchport access vlan 23
  switchport mode access
interface FastEthernet0/14
  switchport access vlan 23
  switchport mode access
interface FastEthernet0/15
  switchport access vlan 23
  switchport mode access
interface FastEthernet0/16
  switchport access vlan 23
  switchport mode access
interface FastEthernet0/17
  switchport access vlan 23
  switchport mode access
interface FastEthernet0/18
  switchport access vlan 23
  switchport mode access
interface FastEthernet0/19
  switchport access vlan 23
  switchport mode access
interface FastEthernet0/20
  switchport access vlan 23
  switchport mode access
interface FastEthernet0/21
  switchport access vlan 23
  switchport mode access
interface FastEthernet0/22
  switchport access vlan 23
  switchport mode access
interface FastEthernet0/23
  switchport access vlan 23
  switchport mode access
interface FastEthernet0/24
  switchport access vlan 23
  switchport mode access
interface GigabitEthernet0/1
  switchport mode trunk
interface GigabitEthernet0/2
  switchport access vlan 21
  switchport mode access
interface Vlan1
  ip address 110.101.1.3 255.255.255.0
interface Vlan21
  ip address 20.10.1.2 255.255.255.0
interface Vlan22
  ip address 20.20.2.2 255.255.255.0
interface Vlan23
  ip address 20.30.3.2 255.255.255.0
ip default-gateway 110.101.1.1
banner motd # Connection to switch S-2
For legal users only #
logging trap debugging
logging 20.2.0.4
line con 0
  logging synchronous
  login local
line vty 0 4
  logging synchronous
  login local
  transport input ssh
  transport output ssh
line vty 5 15
  login
ntp authenticate
ntp trusted-key 1
ntp server 20.2.0.4 key 1
end
```

Лістинг Д.3 – Конфігураційний файл комутатора S-3

```
S-3#sh run
Building configuration...

version 12.1
service timestamps log datetime msec
service timestamps debug datetime msec
no service password-encryption
hostname S-3
enable secret 5
$1$mERr$Hk2hnbY8CmMl.VUj9bnT80
clock timezone EET 2
ip ssh version 2
ip ssh authentication-retries 5
ip ssh time-out 60
ip domain-name S3.rd
username Zlinet secret 5
$1$mERr$YnulBsv8Qb4Qcv9AnjDCX1
spanning-tree mode pvst
spanning-tree extend system-id
interface GigabitEthernet0/1
    switchport mode trunk
interface GigabitEthernet1/1
    switchport access vlan 20
    switchport mode access
interface GigabitEthernet2/1
    switchport access vlan 20
    switchport mode access
interface GigabitEthernet3/1
    switchport access vlan 20
    switchport mode access
interface GigabitEthernet4/1
    switchport access vlan 20
    switchport mode access
interface GigabitEthernet5/1
    switchport access vlan 20
    switchport mode access
interface FastEthernet6/1
    switchport access vlan 20
    switchport mode access
interface FastEthernet7/1
    switchport access vlan 20
    switchport mode access
interface Vlan1
    ip address 110.101.1.4 255.255.255.0
interface Vlan20
    ip address 20.2.0.2 255.255.255.0
banner motd # Connection to switch S-3
For legal users only #
logging trap debugging
logging 20.2.0.4
line con 0
    logging synchronous
    login local
line vty 0 4
    logging synchronous
    login local
    transport input ssh
    transport output ssh
line vty 5 15
    login
ntp authenticate
ntp trusted-key 1
ntp server 20.2.0.4 key 1
end
```