Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: *Сервіси безпеки та віддаленого доступу до ресурсів системи управління підприємством*

Виконала: студентка *IV* курсу, групи *СІс-43*
спеціальності *123 «Комп'ютерна інженерія»*
(шифр і назва спеціальності)

(підпис) *Іваночко Н.А.* (прізвище та ініціали)

Керівник (підпис) *Яцишин В.В.* (прізвище та ініціали)

Нормоконтроль (підпис) *Тиш Є.В.* (прізвище та ініціали)

Завідувач кафедри (підпис) *Осухівська Г.М.* (прізвище та ініціали)

Рецензент (підпис) *Марценко С.В.* (прізвище та ініціали)

Тернопіль
2022

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет *комп'ютерно-інформаційних систем і програмної інженерії*
(повна назва факультету)

Кафедра *комп'ютерних систем та мереж*
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ *Осухівська Г.М.*
(підпис) (прізвище та ініціали)
« ___ » _____ 2022 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня *бакалавр*
(назва освітнього ступеня)

за спеціальністю *123 «Комп'ютерна інженерія»*
(шифр і назва спеціальності)

студентці *Іваночко Назар Андрійович*
(прізвище, ім'я, по батькові)

1. Тема роботи *Сервіси безпеки та віддаленого доступу до ресурсів системи управління підприємством*

Керівник роботи *Яцишин Василь Володимирович, к.т.н., доцент*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*23*» *березня* 2022 року № *4.7-180*

2. Термін подання студентом завершеної роботи *22.06.2022 р.*

3. Вихідні дані до роботи *план будівлі, кількість автоматизованих робочих місць, характеристики комутаційного обладнання, тип ресурсів та сервера для управління підприємством*

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1 аналіз технічного завдання та можливих рішень щодо реалізації сервісів безпеки та віддаленого доступу до інформаційних ресурсів підприємства 2. Проектування та аналіз структури компонентів комп'ютерної мережі. 3. Налаштування сервісів безпеки та віддаленого доступу до ресурсів управління підприємством 4. Безпека життєдіяльності, основи охорони праці. Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. *Фізична топологія комп'ютерної мережі (1 поверх).*
2. *Фізична топологія комп'ютерної мережі (2 поверх).*
3. *Фізична топологія комп'ютерної мережі (3 поверх).*
4. *Логічна топологія мережі*
5. *Схема IP-адресації.*
6. *Схема з'єднань комп'ютерної мережі.*

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності,	*Лазарюк В.В., к.т.н., доц. каф. МТ*		
основи охорони праці			

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	*Розробка і затвердження технічного завдання*	*23.03-28.03.2022*	
2	*Аналіз технічного завдання*	*28.03-02.04.2022*	
3	*Визначення вимог до апаратного та програмного забезпечення комп'ютерної мережі*	*03.04-18.04.2022*	
4	*Проектування схеми організації сервісів безпеки та віддаленого доступу*	*19.04-04.05.2022*	
5	*Налаштування сервісів безпеки та віддаленого доступу до ресурсів управління підприємством*	*04.05-12.05.2022*	
6	*Розробка інструкцій із встановлення та налаштування параметрів комп'ютерної мережі і відповідних сервісів*	*12.05-29.05.2022*	
7	*Безпека життєдіяльності, основи охорони праці*	*01.06-08.06.2022*	
8	*Оформлення кваліфікаційної роботи*	*09.06-18.06.2022*	
9	*Попередній захист кваліфікаційної роботи*	*18.06-22.06.2022*	
10	*Захист кваліфікаційної роботи*	*22.06.2022*	

Студент _____ *Іваночко Назар Андрійович*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Яцишин Василь Володимирович*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Сервіси безпеки та віддаленого доступу до ресурсів системи управління підприємством // Кваліфікаційна робота на здобуття освітнього ступеня бакалавр // Іваночко Назар Андрійович // ТНТУ, спеціальність 123 «Комп'ютерна інженерія»// Тернопіль, 2022 // с.– 93 , рис. – 48 , табл. – 25, аркушів А1 – 6, бібліогр. – 14.

Ключові слова: сервіс, безпека, віддалений доступ, комп'ютерна мережа, система управління.

У даній кваліфікаційній роботі на здобуття освітнього ступеня бакалавра спроектовано комп'ютерну мережу підприємства, що знаходиться у трьохповерховій будівлі. На основі технологій IPsec та L2TP організовано сервіси безпечного віддаленого доступу та налаштовано параметри FireWall.

При налаштуванні параметрів безпеки встановлено групи користувачів та визначено дозволи щодо використання ресурсів підприємства, зокрема, в контексті віддаленого доступу до системи відеоспостереження та фінансової звітності й обліку підприємства.

Налаштування сервісів безпеки та віддаленого доступу виконано на основі MikroTik hEX (RB750Gr3), повністю налаштовано його FireWall, реалізовано запропоновані рішення щодо сегментації локальної комп'ютерної мережі та логічної топології.

В якості комутаторів використано комутатори другого рівня, зокрема один TL-SL5428E і два HP ProCurve 1700 – 24, які розташовано у стійках 19". Кабельна інфраструктура побудована на основі вимог і рекомендацій стандартів структурованих кабельних систем.

ABSTRACT

Security and remote access services to enterprise management system resources // Bachelor’s thesis // Ivanochko Nazar Andriiovych // TNTU, speciality 123 «Computer engineering»// Ternopil, 2022 // p.– 93 , fig. – 48 , tab. – 25, posters A1 – 6, ref. – 14.

Keywords: service, security, remote access, computer network, manage,ent system.

The qualification work is devoted to design of the computer network of an enterprise located in a three-story building. Based on IPsec and L2TP technologies, secure remote access services are organized and FireWall settings are configured.

When configuring security settings, user groups are set and permissions for the use of enterprise resources are defined, in particular, in the context of remote access to the video surveillance system and financial reporting and accounting of the enterprise.

Configuration of security and remote access services is based on MikroTik hEX (RB750Gr3), its FireWall is fully configured, the proposed solutions for local computer network segmentation and logical topology are implemented.

Second-level switches were used as switches, including one TL-SL5428E and two HP ProCurve 1700-24, which are located in 19 ”racks. Cable infrastructure is based on the requirements and recommendations of the standards of structured cabling systems.

ЗМІСТ

ПЕРЕЛІК ОСНОВНИХ УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ І СКОРОЧЕНЬ8

ВСТУП 9

РОЗДІЛ 1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ ТА МОЖЛИВИХ РІШЕНЬ ЩОДО РЕАЛІЗАЦІЇ СЕРВІСІВ БЕЗПЕКИ ТА ВІДДАЛЕНОГО ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ ПІДПРИЄМСТВА 11

1.1 Аналіз завдання щодо призначення та налаштування сервісів безпеки та віддаленого доступу до ресурсів підприємства 11

1.2 Аналіз основних понять і принципів організації сервісів безпеки та віддаленого доступу 17

1.2.1 Принцип організації безпечного віддаленого доступу 17

1.2.2 Аналіз технологій віддаленого доступу 19

1.2.3 Переваги віддаленого доступу до ресурсів 20

РОЗДІЛ 2 ПРОЕКТУВАННЯ ТА АНАЛІЗ СТРУКТУРИ КОМПОНЕНТІВ КОМП'ЮТЕРНОЇ МЕРЕЖІ 22

2.1 Аналіз фізичної структури організації комп'ютерної мережі з сервісами безпеки та віддаленого доступу 22

2.2 Обґрунтування технічних рішень при проектуванні фізичної і логічної топологій комп'ютерної мережі 24

2.3 Побудова та обґрунтування логічної топології комп'ютерної мережі 29

2.4 Обґрунтування вибору комутаційного обладнання 30

2.5 Логічна адресація робочих станцій та серверів 39

2.6 Комутація з'єднань комп'ютерної мережі 44

РОЗДІЛ 3 НАЛАШТУВАННЯ СЕРВІСІВ БЕЗПЕКИ ТА ВІДДАЛЕНОГО ДОСТУПУ ДО РЕСУРСІВ УПРАВЛІННЯ ПІДПРИЄМСТВОМ 49
3.1 Базові налаштування MikroTik RB750Gr3 49
3.2 Формування VLAN та налаштування сервісу безпеки 54
3.2.1 Налаштування VLAN 54
3.2.2 Налаштування сервісу безпеки 62
3.3 Організація безпечного віддаленого доступу до ресурсів управління підприємством 66
РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ. 73
4.1 Організація служби охорони праці на підприємстві 73
4.2 Заходи, які забезпечують створення оптимальних метеорологічних умов у приміщеннях з використанням ПК 76
ВИСНОВКИ 80
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 81
Додаток А. Технічне завдання

ПЕРЕЛІК ОСНОВНИХ УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ І СКОРОЧЕНЬ

БД	База даних
КС	Комп’ютерна система
ПЗ	Програмне забезпечення
КМ	Комп’ютерна мережа
UML	Unified Modelling Language

ВСТУП

Сучасний розвиток галузей народного господарства вимагає від керівників підприємств, не важливо від форми власності, ефективного застосування інформаційних технологій для забезпечення успіху бізнес проектів та існуючих бізнес систем. Тому актуальним з точки зору збору, опрацювання та управління ресурсами підприємства є проектування інформаційних інфраструктур, які б давали змогу автоматизувати процеси передачі даних, їх централізованого зберігання т безпечного використання.

Важливість розробки інформаційної інфраструктури на базі комп'ютерних мереж, враховуючи функціональні можливості щодо організації віддаленого доступу і безпеки, пов'язана, насамперед, із здатністю забезпечити облік наданих послуг, розширити сферу діяльності підприємства, підтримувати актуальність даних і їх цілісність.

Враховуючи останні тенденції щодо поширення пандемії COVID-19, а також ведення військових дій на території України все більше уваги підприємства приділяють організації дистанційної роботи працівників. Це в свою чергу, вимагає впровадження сервісів віддаленого доступу до робочого місця та забезпечення безпеки ресурсів системи управління підприємством. Тому актуальною задачею на сьогодні є проектування, реалізація та налаштування комунікаційної частини інфраструктури підприємства для забезпечення ефективності роботи підприємства.

Організація сервісів безпеки та віддаленого доступу до ресурсів системи управління підприємством передбачає розв'язання ряду взаємопов'язаних задач, зокрема:

– аналізу організаційної структуру підприємства для визначення інформаційних потоків даних взаємодії між структурними підрозділами;

– аналіз архітектурних планів приміщень для проектування або модернізації фізичної топології мережі;

– обґрунтування техніко-економічних показників проектування комп’ютерної мережі;

– обґрунтування вибору мережевого комутаційного обладнання комп’ютерної мережі, робочих станцій та серверів;

– моделювання логічної схеми роботи мережі;

– розробку IP-адресної схеми та схеми комутації для забезпечення ефективності обміну даними;

– забезпечення захисту та контролю над інформаційними ресурсами даного підприємства;

– організацію віддаленого доступу до робочих місць працівників.

РОЗДІЛ 1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ ТА МОЖЛИВИХ РІШЕНЬ ЩОДО РЕАЛІЗАЦІЇ СЕРВІСІВ БЕЗПЕКИ ТА ВІДДАЛЕНОГО ДОСТУПУ ДО ІНФОРМАЦІЙНИХ РЕСУРСІВ ПІДПРИЄМСТВА

1.1 Аналіз завдання щодо призначення та налаштування сервісів безпеки та віддаленого доступу до ресурсів підприємства

Сервіси безпеки та віддаленого доступу до ресурсів системи управління підприємством функціонують на основі комунікаційної складової інформаційної системи підприємства. Основне призначення таких сервісів полягає у забезпеченні захисту та авторизованого доступу до наявних інформаційних ресурсів, а також забезпечення віддаленого доступу до бухгалтерських документів і звітності, доступу до камер відеоспостереження, які наявні на підприємстві.

Такі сервіси повинні забезпечувати логічну і фізичну стійкість при доступі до ресурсів, а також забезпечувати локальний авторизований доступ до програмного та інформаційного забезпечення. Наявність сервісів безпеки та віддаленого доступу повинні сприяти підвищенню ефективності функціонування підприємства, запобігти витокам інформації, а також чітко розподілити права і ролі користувачів при опрацюванні даних та забезпечити захист інформації.

Мета реалізації та налаштування сервісів безпеки та віддаленого доступу до інформаційних ресурсів управління підприємством полягає у підвищенні безпекового і захисного потенціалу при автоматизації бізнес-процесів фірми, а також забезпечення гнучкості і доступу з віддаленого географічного розташування визначених груп користувачів.

До переліку основних задач, які повинні реалізовувати сервіси безпеки та віддаленого доступу належать:

– автоматизація процесу аутентифікованого доступу до ресурсів управління підприємством;

– здатність налаштування дозволів для визначених груп користувачів;

– здатність логувати та зберігати інформацію про доступ до ресурсів управління підприємством з фіксацією дати і часу;

– можливість аналізу логів звернення до інформаційних ресурсів;

– можливість визначення групи IP-адрес в межах пісочниці інтернет-провайдера;

– можливість трансляції відеопотоку із встановлених відеокамер;

– забезпечення можливості управління інформаційними та відеопотоками;

– здатність захищеного входу/виходу користувачів з локальної мережі в інтернет-простір;

– здатність до взаємодії з довіреними зовнішніми програмними та інформаційними ресурсами;

– забезпечення віддаленого доступу з використанням двохфакторної авторизації користувачів.

Найбільш важливими функціями і задачами, які покликані розв’язати сервіси безпеки і віддаленого доступу до інформаційних ресурсів є здатність гнучко та надійно проводити аутентифікацію користувачів, надавати можливість віддаленого використання інформаційних ресурсів та ресурсів управління бухгалтерським обліком підприємства, а також організації доступу до комунікаційної частини інфраструктури в контексті відеоспостереження.

Реалізація таких сервісів дозволить адміністратору проводити моніторинг використання інформаційних ресурсів, фіксувати дату і час їхньої зміни, а також проводити додаткові заходи щодо підвищення ефективності процесів кіберзахисту із застосування сучасних технологій, зокрема штучного інтелекту, в контексті розпізнавання шахраїв.

Досягнення цілі відносно реалізації сервісів віддаленого доступу і безпеки передбачає виконання ряду задач. Серед найбільш важливих серед них є аналіз існуючої комунікаційної інфраструктури, визначення груп користувачів з відповідними правами і дозволами доступу до ресурсів, проектування фізичної і логічної топологій комунікаційної мережі та системи відеоспостереження, параметризація доступу до ресурсів глобальної мережі Інтернет, обміну даними у локальній комп'ютерній мережі.

Важливою задачею також є організація віртуальних мереж, що дозволяють відобразити концептуально подібні групи користувачів. Це забезпечує можливість спільно, в авторизованому режимі, використовувати інформаційні ресурси.

Безпека у комп'ютерній мережі передбачає налаштування на логічному та фізичному рівні методів аутентифікованого доступу за різними рівнями. Система логування дозволяє проводити аналіз даних щодо використання інформації користувачами, віддалений доступ до інформації управління підприємством, зокрема, 1С Бухгалтерія.

Сервіси безпеки і віддаленого доступу до ресурсів управління підприємства, що функціонують на основі комунікаційної складової інформаційної системи повинні надавати дозвіл доступу до необхідних даних у межах визначених організаційних структур підприємства і як наслідок забезпечити ефективність функціонування всього підприємства. Для цього необхідно передбачити та реалізувати права доступу і дозволи для визначених груп користувачів. Використання ресурсів управління підприємством повинно бути визначеним на основі аналізу авторизаційних даних користувачів, відноситись до однієї з груп чи правил захищеності даних, а також повинні бути відсутні втрати зв'язку. Для кожного користувача комунікаційної мережі, на основі встановлених правил і дозволів, повинна бути передбачена можливість доступу та використання ресурсів мережі Internet. Передача даних у середовищі комунікаційної мережі повинна становити не менше, ніж 100 Мб/с.

Структура комунікаційної мережі, а також відповідних сервісів віддаленого доступу до ресурсів і безпеки системи включає:

– архітектуру об’єднання комп’ютерів в межах кожного окремого відділу, до складу яких входять:

- інженерно-технічний відділ – 4 комп’ютери;
- аналітичний відділ – 2 комп’ютери;
- адміністративний підрозділ – 4 комп’ютери;
- сукупність робочих місць в орендованих приміщеннях – 15 комп’ютерів;
- комутаційна кімната – 1 комп’ютерів;

– схему організації доступу і модель зв’язків для з’єднання з мережею Internet;

– схему допоміжної та резервної взаємодії з структурними організаційними елементами підприємства;

Зазвичай, логічна топологія комунікаційних зв’язків повинна бути орієнтована на відображення організаційної взаємодії між відділами підприємства, а також модель реалізації доступу до Internet.

До функціональних та нефункціональних вимог щодо організації комп’ютерної мережі з сервісами віддаленого доступу і безпеки належать :

– стійкість і безвідмовність функціонування активних та пасивних вузлів інформаційної системи;

– швидкість обміну інформацією на рівні не менше 100 Мб/с;

– напрацювання на відмови і безперебійна передача даних у рамках визначеного часового діапазону;

– забезпечення авторизованого доступу на фізичному та логічному рівнях;

– зручність монтажу та модернізаці;

– час відгуку та реакції компонентів системи в межах не більше 2 с.;

– розширюваність і масштабованість вузлів мережі в межах 6 робочих місць.

При організації комп'ютерної мережі необхідно передбачити забезпечення зв'язку між її вузлами, що використовує як кабельні структуровані систем, так і технологію безпровідного середовища WiFi. Основні комунікаційні інтерфейси та параметри передачі даних налаштовуються як на рівні операційних систем, так і на основі системного програмного забезпечення активного комутаційних вузлів.

Діагностування комп'ютерної мережі з відповідними сервісами безпеки та віддаленого управління ресурсів управління підприємством відбувається у відповідності до графіку обслуговування. Розрізняють два режими експлуатації та функціонування системи, зокрема її складових у вигляді сервісів безпеки та віддаленого доступу: нормальний та аварійний. У випадку функціонування сервісів у штатному режимі (нормальний режим) передбачається висока ефективність і безвідмовність усіх вузлів та елементів інформаційної системи. У випадку настання і переходу системи в аварійний режим може спостерігатися часткова втрата швидкості передачі даних та перехід на резервні канали зв'язку.

Фізичний доступ до компонентів комп'ютерної мережі з сервісами безпеки і віддаленого доступу повинен бути захищеним від несанкціонованого доступу та механічних пошкоджень. Через це повинні бути передбачені засоби захисту коробів, комутаційних вузлів, активного і пасивного комутаційного обладнання і т.д.

Окрім обмеження фізичного доступу, компоненти комп'ютетрної системи повинні бути захищеними на рівні системного та прикладного програмного забезпечення інформаційної системи.

Важливою вимогою, що є підхарактерситикою надійності комунікаційної мережі, є здатність до відновлення працездатності при збоях елементів мережі на різних рівнях.

Функціональними вимогами, які висуваються до комп'ютерної мережі та сервісів безпеки і віддаленого доступу до інформаційних ресурсів є наступні:

– централізоване та водночас гнучке управління бізнес-процесами і даними;

– забезпечення доступності до ресурсів мережі Internet;

– організація системи аутентифікації користувачів на прикладному і програмних рівнях;

– організація моніторингу використання ресурсів мережі;

– швидкість передачі даних у локальній мережі на рівні не нижче, ніж 100 Мб/с, а вхідного/вихідного трафіку у глобальну мережу не нижче 60 Мб/с на одного користувача;

– узгодженість монтажу вузлів комп'ютерної мережі стандартам проектування структурованих кабельних систем.

Мінімальні вимоги до серверного обладнання:

– процесор з тактовою частотою не нижче, ніж 2,1 ГГц/ ядро;

– кількість фізичних ядер – не менше 8;

– обсяг оперативної пам'яті – на рівні 16 ГБ;

– об'єм жорсткого диску - не менше 20 ТБ.

Мінімальні вимоги до користувацьких машин:

– тактова частота процесора на рівні 2,0 ГГц/ядро;

– кількість фізичних ядер – мінімум 2;

– обсяг оперативної пам'яті - не менше 8 ГБ;

– об'єм жорсткого диску - не менше 500 Гб.

Мережеве обладнання:

– комутатори – 4 шт.;

– маршрутизатори – 1 шт.

Периферійні пристрої:

– принтер звичайний – 4 шт.

– мережевий принтер – 1 шт.

– багатофункціональний пристрій – 2 шт.

Програмне забезпечення робочих станцій – Windows 10, Windows 7, або UNIX-подібні ОС та прикладне програмне забезпечення, зокрема 1С. Бухгалтерія, веб-оглядач та ін.

1.2 Аналіз основних понять і принципів організації сервісів безпеки та віддаленого доступу

Безпечний віддалений доступ — це комбінація процесів або рішень безпеки, які призначені для запобігання несанкціонованому доступу до цифрових активів організації та запобігання втрати конфіденційних даних.

Безпечний віддалений доступ може охоплювати ряд методологій, таких як VPN, багатофакторна аутентифікація та захист кінцевої точки. Швидко змінний «ландшафт» загроз і збільшення кількості віддалених працівників через пандемію Covid зробили безпечний віддалений доступ критичним елементом сучасного IT-середовища. Успіх вимагає навчання користувачів, посилення політики кібербезпеки та розробки найкращих практик гігієни безпеки.

1.2.1 Принцип організації безпечного віддаленого доступу

Захист кінцевих точок для всіх віддалених користувачів та їхніх пристроїв. Захист кінцевих точок у центрах опрацювання даних є досить простим у порівнянні із захистом кінцевих точок для віддалених користувачів, які часто використовують декілька пристроїв протягом робочого дня. Антивірусне програмне забезпечення має бути встановлено на всіх кінцевих пристроях, будь то ПК з операційними системами Mac, Linux, iOS або Android. Політика безпеки повинна вимагати, щоб усі співробітники підтримували поточний захист, якщо вони хочуть отримати доступ до корпоративних ресурсів. Якщо необхідно, співробітникам надаються вказівки та допомогу з метою встановлення безпечного доступу до ресурсів організації.

Уникнення використання віддаленого доступу із зростанням загроз – налаштування віддаленого доступу може становити ризики для організації. Зокрема, атаки програм-вимагачів часто сканують сервери протоколу віддаленого робочого столу (RDP) і отримують доступ з будь-якого доступного порту. Аналогічно, потрібно утриматися від відкриття портів віддаленого доступу, якщо брандмауери не налаштовані на відповідь лише для відомих IP-адрес системних адміністраторів.

Використання багатофакторної автентифікації. Двофакторна автентифікація (2FA) вимагає від користувачів надати «щось, що вони знають і те, що вони мають», наприклад, пароль і маркер автентифікації, які можуть бути згенеровані пристроєм або програмою для смартфона, наприклад DUO. Це може гарантувати, що лише перевіреним користувачам буде дозволений доступ до корпоративних ресурсів.

Використання віртуальних приватних мереж (VPN) – багато віддалених користувачів захочуть підключитися через незахищений Wi-Fi або інші ненадійні мережеві з'єднання. VPN можуть усунути цей ризик, однак програмне забезпечення кінцевої точки VPN також має оновлюватися, щоб уникнути вразливостей, які можуть виникнути через старі версії програмного клієнта.

Нормалізація журналів та відстеження інформації про безпеку.

Існуючі інструменти безпеки та керування подіями (SIEM), які реєструють трафік із клієнтських пристроїв, можуть раптово вважати користувачами, які входять зі своїх домашніх IP-адрес як аномалію, тому можуть знадобитися налаштування як SIEM, так і геозони або функції геоблокування в брандмауерах, щоб гарантувати, що співробітники можуть входити звідки б вони не працювали.

Пандемія Covid призвела до створення низки нових кіберзагроз і фішингових атак, які нібито пов'язані з вірусом. У рамках навчання з питань безпеки та відповідності всім співробітникам та іншим особам, які мають доступ до корпоративних ресурсів, слід нагадати, що вони не повинні відкривати будь-які небажані листи або посилання в них.

Оновлення політики для віддалених користувачів полягає в тому, щоб переконатися, що політики прийнятного використання включають домашні комп'ютерні засоби співробітника, якими можуть бути комп'ютер, ноутбук, планшет і смартфон, включаючи оновлення антивірусного та VPN-програм, які можуть бути встановлені на пристроях, що належать працівникам.

1.2.2 Аналіз технологій віддаленого доступу

Безпечний віддалений доступ — це не одна технологія, а скоріше сукупність технологій, які разом забезпечують безпеку, необхідну організаціям, коли користувачі працюють вдома чи в інших віддалених місцях. До технологій безпечного віддаленого доступу належить безпека кінцевої точки, що представляє собою програмне забезпечення, зокрема антивірус для кінцевих машин, а також політики, які визначають, як віддалені пристрої мають використовуватися в системах організації. Це може включати керування виправленнями та запобігання завантаженню або кешування критично важливої для бізнесу інформації на віддалені пристрої.

Віртуальна приватна мережа (VPN) – надзвичайно популярна технологія для віддаленого доступу, оскільки дозволяє віддаленим користувачам, підключеним через незахищений віддалений Wi-Fi підключатися до приватної мережі через зашифрований тунель.

Доступ до мережі з нульовою довірою (ZTNA) – як випливає з назви, рішення ZTNA не роблять жодних припущень щодо безпеки з'єднання і вимагають повторної аутентифікації перед кожною транзакцією. Це забезпечує вищий рівень безпеки для даних і програм організації.

Контроль доступу до мережі (NAC) – доступом до мережі керують за допомогою комбінації таких інструментів, як двофакторна аутентифікація (2FA), інструментів безпеки кінцевих точок, а також навчання та застосування політики.

Єдиний вхід (SSO) – за допомогою SSO користувачам потрібен лише один набір облікових даних для доступу до всіх своїх програм і ресурсів.

1.2.3 Переваги віддаленого доступу до ресурсів

До 2020 року кількість віддалених працівників зросла, а пандемія Covid швидко прискорила потребу користувачів у доступі до корпоративних мереж із кількох віддалених місць. Для багатьох організацій переважна більшість вхідних з'єднань тепер виникають у домашніх мережах їхніх співробітників, що посилює ризики як для мереж організації, так і для самих співробітників. Як наслідок, старі, застарілі заходи безпеки не відповідають вимогам віддаленої, переважно мобільної бази користувачів. Новий базовий рівень безпеки вимагає підтримки для кожного користувача, з кожного пристрою, який він використовує, з будь-якої мережі, з якої вони підключаються.

Стратегія безпечного віддаленого доступу має кілька переваг. Серед них: Безпечний доступ будь-де з будь-якого пристрою – користувачі можуть використовувати той самий рівень високого захищеного доступу, який вони використовувати раніше на робочому місці. Контроль доступу може надавати доступ до конкретних програм і даних для кожного користувача на основі його ролей та обов'язків. Оскільки багато співробітників працюватимуть з дому навіть після того, як криза Covid пройде, це найважливіша перевага стратегії безпечного віддаленого доступу.

Надійний захист кінцевої точки – безпечний віддалений доступ не має значення, якщо кінцеві точки також не захищені. Оскільки користувачі все більше покладаються на кілька пристроїв для виконання своєї роботи, захист ноутбуків, планшетів і смартфонів є важливим. Крім того, пристроям, що належать співробітникам, слід пропонувати ті ж можливості безпеки кінцевої точки, що й ті, які надаються організацією.

Безпечний доступ до Інтернету – організації покладаються на багато веб-додатків та програм, орієнтованих на Інтернет, як частину свого IT-середовища. У результаті користувачі потребують захисту щоразу, коли вони підключені до Інтернету, а не лише коли вони підключені до локальних ресурсів організації. Безпечний віддалений доступ включає захист користувачів від загроз

зловмисного програмного забезпечення, таких як програми-вимагачі та фішингові атаки.

Підвищення обізнаності з проблемами безпеки – все більш мобільні працівники створюють багато нових проблем безпеки, і для багатьох з них освіта є найкращими «ліками». Підтримуючи та впроваджуючи політику безпеки та передовий досвід, IT-організації та організації з безпеки можуть постійно посилювати важливість належної гігієни кібербезпеки.

РОЗДІЛ 2 ПРОЕКТУВАННЯ ТА АНАЛІЗ СТРУКТУРИ КОМПОНЕНТІВ КОМП'ЮТЕРНОЇ МЕРЕЖІ

2.1 Аналіз фізичної структури організації комп'ютерної мережі з сервісами безпеки та віддаленого доступу

Для вирішення поставлених у роботі завдань необхідно провести аналіз структури та фактичного і потенційного розташування об'єктів комп'ютерної мережі у приміщенні, де вони знаходяться. Приміщення організації, для якої необхідно розробити сервіси безпеки та віддаленого доступу до ресурсів управління підприємством, розташовано у трьохповерховій будівлі.

На першому поверсі розміщено устаткування підприємства, що займається вогне- та біозахистом. Важливими компонентами інформаційної інфраструктури даної організації є робочі станції працівників та сервер для ведення бухгалтерського обліку.

На другому і третьому поверхах розташовано офіси та приміщення окремих організацій, які перебувають в оренді.

У таблиці 1.1 наведено характеристику площ та кількості робочих станцій, які знаходяться на першому поверсі триповерхової будівлі..

Таблиця 1.1 – Характеристика приміщень з АРМ (1 поверх)

№ приміщення	Кількість робочих станцій, шт.	Розміри, м	Площа, кв. м
1	3	9.94*2.74	27.28
2	4	7.25*6.44	46.66
3	1	2.43*5.52	13.42
5	3	8.62*2.80	24.13

У таблиці 1.2 наведено розміри та обчислено площі приміщень 2-го поверху будівлі для якої розробляються та налаштовуються сервіси безпеки і віддаленого доступу.

Таблиця 1.2 – Характеристика приміщень з АРМ (2 поверх)

№ приміщення	Кількість робочих станцій, шт.	Розміри, м	Площа, кв. м
201	1	5.6*5.74	32.14
202	1	2.8*5.74	16.07
206	6	5.46*5.74	31.34
207	1	2.87*5.74	16.47
215	6	3.8*8.6	64.05

У таблиці 1.3 наведено розміри та обчислено площі приміщень 3-го поверху для формування інформаційної інфраструктури у приміщеннях триповерхової будівлі.

Таблиця 1.3 – Характеристика приміщень з АРМ (3 поверх)

№ приміщення	Кількість робочих станцій, шт.	Розміри, м	Площа, кв. м
301	3	4.2*6.44	27.05
303	6	5.88*6.44	37.87
304	1	2.80*6.44	18.03
305	2	2.80*6.44	18.03
306	6	6.16*6.44	39.67

Для фізичного та логічного з’єднання компонентів комп’ютерної мережі при реалізації сервісів безпеки та віддаленого доступу до ресурсів управління підприємством запропоновано використовувати маршрутизатори та комутатори фірми TP-Link, Hewlett Packard та Mikrotik.

Перевагами даного класу комутаторів є відносно невисока ціна та надійність. Крім того, ці пристрої характеризуються підтримкою стандартів обміну інформацією IEEE 802.3 10Base-T Ethernet, IEEE 802.3u 100Base-TX Fast Ethernet, автоузгодження з ANSI/IEEE 802.3 Nway, керування потоком IEEE 802.3x. Швидкість обміну і передачі даних при реалізації мережі типу Ethernet:

– 10Мбіт/с (напівдуплекс);
– 20Мбіт/с (повний дуплекс).

Швидкість передачі даних при реалізації мережі типу Fast Ethernet:

– 100Мбіт/с (напівдуплекс);
– 200Мбіт/с (напівдуплекс).

Виходячи з організаційної структури та вимог з охорони праці щодо кількості робочих місць на відведену площу (6 м^2), спроектовано фізичну топологію комп'ютерної мережі. Автоматизовані робочі місця, відведена на них площа та конкретні кабінети наведені у таблицях 1.1 –1.3. У графічному матеріалі до роботи наведено схеми фізичних топологій усіх поверхів. При проектуванні фізичної топології використано підхід до проектування комп'ютерних мереж з використанням стандартів структурованих кабельних систем.

2.2 Обґрунтування технічних рішень при проектуванні фізичної і логічної топологій комп'ютерної мережі

Обґрунтування технічних рішень при проектуванні комп'ютерних мереж включає в себе аналіз фізичної та логічної топології мережі, обґрунтування вибору технології проектування, аналіз стандартів і середовищ передачі даних. Тому для забезпечення ефективної працездатності комп'ютерної мережі та відповідно реалізації сервісів безпеки і віддаленого доступу на основі аналізу фізичного розміщення та організаційної структури даної організації проведемо дослідження найбільш оптимальних фізичних та логічних архітектур.

Забезпечення ефективності управління підприємства в еру технічного прогресу та інтенсивного впровадження інформаційних технологій забезпечується надійною, гнучкою та багатофункціональною комунікаційною складовою, тобто комп'ютерною мережею. Це дає змогу ефективно об'єднувати у спільний інформаційний простір автоматизовані робочі місця та підтримувати актуальність і достовірність даних, які безпосередньо впливають на здатність приймати стратегічні управлінські рішення. Комунікаційна складова інформаційної інфраструктури, окрім безпосередньої передачі даних, повинна забезпечувати сервіси безпеки. В умовах пандемії COVID-19, а також військових дій на території України, працівники більшості підприємств повинні мати можливість віддаленого доступу до ресурсів підприємства, що також реалізується на основі віддаленого доступу до комунікаційної мережі.

Найпростіша комп'ютерна мережа може бути реалізована з використанням двох ПК, які з'єднуються за допомогою послідовних чи паралельних портів та використовують мережевий адаптер.

Варто відмітити, що під фізичною топологією комп'ютерної мережі, зазвичай, розуміють безпосереднє фізичне підключення каналів передачі даних з врахуванням особливостей підключення клієнтів комунікаційної складової інформаційної інфраструктури підприємства.

На сьогодні найбільш поширеними та використовуваними на практиці топологіями комп'ютерних мереж є:

– шинна топологія;
– зіркоподібна топологія;
– топологія кільця.

Використання тієї чи іншої топології диктується функціональним призначення комп'ютерної мережі, а відповідно до цього, кожен з видів організації комунікаційної мережі володіє певним спектром переваг і недоліків.

Шинна топологія організації комп'ютерної мережі передбачає безпосереднє підключення клієнтів до центральної магістралі передачі даних і відноситься до найбільш дешевих способів реалізації комунікаційної складової інформаційної інфраструктури.

Екземплярами організації КМ на основі топології шина можуть бути як «товстий Ethernet», так і «тонкий Ethernet» На рисунку 2.1 показано приклад організації мережі на основі шинної топології.

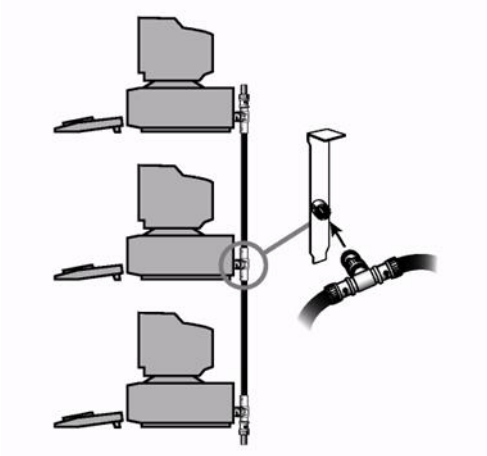

Рисунок 2.1 – Приклад організації мережі на основі шинної топології

Усі клієнти, при організації мережі на основі топології шини, повинні бути підключені до одного і того ж магістрального кабелю. При цьому перший і останній клієнт мають бути «розв'язані». У якості так званої «розв'язки» може використовуватися звичайний резистор, основна функція якого полягає у «гасінні» сигналу при проходженні до крайньої точки мережі і запобігає утворенню завад [1].

До основного недоліку шинної топології належить фактор і властивість надійності, що полягає у високій імовірності виникнення проблем з передачею даних при пошкодженні центрального магістрального кабелю.

Виявлення несправності у кабелі передбачає декомпозицію сегментів мережі на два блоки до тих пір, поки не буде виявлено обрив у лінії передачі даних. Така діагностика може займати тривалий час і негативно позначається на функціональності мережі. Застосування топології шини може ефективно використовуватися при проектуванні невеликих комунікаційних мереж, які не вимагають дотримання суворих вимог надійності, а кабельна інфраструктура є легкодоступною для виявлення і виправлення несправностей.

З точки зору забезпечення надійності і функціональності комп'ютерних мереж найбільш ефективною є організація мережі на основі топології зірки. Завдяки тому, що кожен клієнт підключається за допомогою окремого кабеля до комутатора, значно знижується імовірність виникнення обриву та (або) усунення цього фактору. Кожен клієнт підключається до окремого порту повторювача, який може виконувати функції комутатора або концентратора. На рисунку 2.2 показано приклад організації мережі на основі топології зірка.

Рисунок 2.2 – Організація мережі на основі топології «зірка»

Коли складається ситуація виходу з ладу самого комутатора, то обмін і передача даних між клієнтами, які до нього підключені, втрачається. У такому випадку необхідно виконати його заміну на ідентичний або кращий за технічними характеристиками пристрій. Доцільним при проектуванні комп'ютерної мережі є використання однорідного мережевого обладнання, що дає змогу ефективно реагувати на вихід з ладу окремих ланок мережі. Сьогодні у більшості випадків використовують інтелектуальні комутатори, які підтримують протокол SNMP та ряд інших, які дають змогу віддалено виконувати його налаштування та одержувати доступ до ресурсів локальної комп'ютерної мережі.

Фірма IBM використовує топологію кільця для організації комунікації на основі естафетного доступу. Схема та структура організації мережі на основі такої топології схожа до топології «зірка», а приклад її візуалізації показано на

рисунку 2.3. У даному випадку, клієнти взаємодіють з пристроєм множинного доступу, а не до комутатора. Multiple Access Unit відповідає за логічну комунікацію комп'ютерів у кільце.

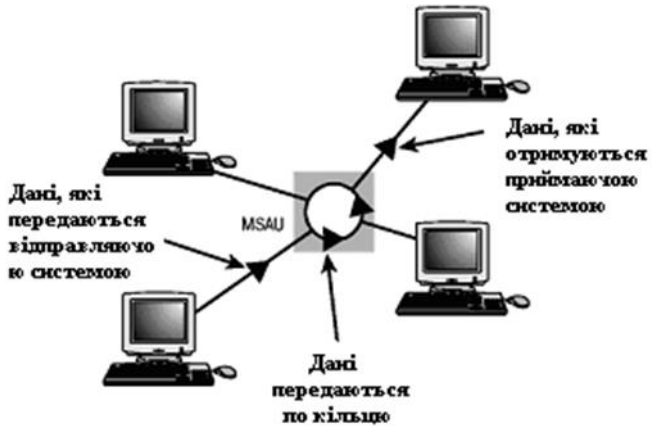

Рисунок 2.3 - Організація мережі на основі топології кільця

Характерною особливістю топологій зірка та кільце є те, що спосіб їхньої фізичної організації ідентичний, тому обидві вони володіють такими ж перевагами відносно шинної топології. Слабким місцем, як і у випадку топології зірки, є пристрій комутації, тобто найбільш часто на надійність і функціональність мережі впливає пристрій, який виконує функції Multiple Access Unit.

При організації комп’ютерних мереж сьогодні використовують різні канали передачі даних, кабельні на основі електричного струму (вита пара, коаксіальний кабель), оптоволоконні лінії зв’язку, а також безпровідні технології – супутникові канали передачі даних, радіоканали і т.п.

Модель комп’ютерної мережі з сервісами безпеки та віддаленого доступу до ресурсів управління підприємством повинна реалізовувати підхід, що базується на використанні технології Fast Ethernet. Крім того, моделлю локальної комп’ютерної мережі, з врахуванням обміну документацією, може бути організаційна структура підприємства. Виходячи з такого підходу необхідно визначити «логіку» взаємодії між структурними відділами

підприємства, що при реалізації зменшить ймовірність виникнення колізій і збільшить швидкодію передачі даних.

2.3 Побудова та обґрунтування логічної топології комп'ютерної мережі

У даному підрозділі описано структуру локальної комп'ютерної мережі та виконано розрахунок кількості дозволених комп'ютерів в кожній з кімнат.

Проаналізувавши плани будівлі, було вирішено обрати топологію розширеної зірки, яка будується на основі топології "зірка". Принцип формування даної топології полягає в об'єднанні трьох сегментів мережі з врахуванням того фактору, що сам сегменти також утворюють топологією "зірка". Зв'язок між сегментами створюється між центральним маршрутизатором та комутаторами, які розташовані на кожному поверсі будівлі. Маршрутизатор є центральним керуючим вузлом (MDF), що забезпечує доступ до ресурсів локальної мережі та доступу до мережі Інтернет. Комутатори, розташовані на кожному з поверхів, є додатковими (IDF) і під'єднуються до центрального.

Локальна комп'ютерна мережа, що розробляється має займати три поверхи будівлі. Центральний маршрутизатор розташований в серверній кімнаті на третьому поверсі будівлі, до якого з першого та другого поверхів під'єднуються комутатори. Відповідно до цих комутаторів під'єднуються кінцеві пристрої. Сервери розташовані в одній кімнаті з центральним маршрутизатором. Для визначення кількості розеток в кожній з кімнат бралась до уваги площа кімнати, та тип групи користувачів, які знаходяться в даній кімнаті (табл. 2.1 - табл. 2.3). Для одного комп'ютера виділено шість квадратних метрів, з урахуванням того, що висота стелі дорівнює 3,3 м^2.

При проектуванні комп'ютерної мережі адміністративної будівлі доцільно скористатися стандартом TIA/EIA-568-B, що сформований на основі трьох інших стандартів, що затвердженні асоціацією телекомунікаційної промисловості Сполучених Штатів Америки. TIA/EIA-568-B є розвитком

стандарту TIA/EIA-568-A [5]. Цей стандарт описує способи побудови структурованої кабельної системи в будівлях та з’єднання між корпусами.

У ньому описані різні типи кабелів, з'єднувальні компоненти, архітектури кабельних систем, методи їх тестування і так далі

Даний стандарт описує топологію, яка використовується, для проектування визначеної комп’ютерної мережі. Для горизонтального та вертикального кабелювання, в комп’ютерній мережі, що розробляється, обрано виту пару [3], що складається з 4-х пар скручених між собою провідників, покритих пластиковою оболонкою. При реалізації обраної топології (розширена зірка) з’єднання між центральним маршрутизатором (MDF), серверами та допоміжними маршрутизаторами, які керується віддаленим доступом, виконувалось за допомогою кабелю витої пари категорії 5е. При цьому в кабелі задіяно чотири пари провідників, що говорить про те що швидкість передачі даних між маршрутизатором та комутаторами буде досягати одного гігабіта за секунду. З’єднання комутаторів між собою відбувалось аналогічно, де теж використовується вита пара категорії 5е із задіяними чотирма парами провідників. З’єднання робочих станцій до комутаторів, дещо відрізняється від інших з’єднань, так як при цьому використано лише дві пари провідників кабелі витої пари категорії 5е, що вказує на те, що швидкість передачі даних між робочими станціями та комутатором буде досягати 100 Мбіт/с. Логічну топологію комп’ютерної мережі з сервісами безпеки та віддаленого доступу наведено у графічному матеріалі до кваліфікаційної роботи.

2.4 Обґрунтування вибору комутаційного обладнання

При розробці проекту комп’ютерної мережі з сервісами безпеки та віддаленого доступу до ресурсів управління підприємством було обрано наступне мережеве обладнання:

– маршрутизатор – «MikroTik hEX (RB750Gr3)»;

– комутатор другого рівня TL-SL5428E;

– комутатори с.

Маршрутизатор RB750Gr3 показано на рисунку 2.4. Він надає масштабоване управління у міру зміни потреб.

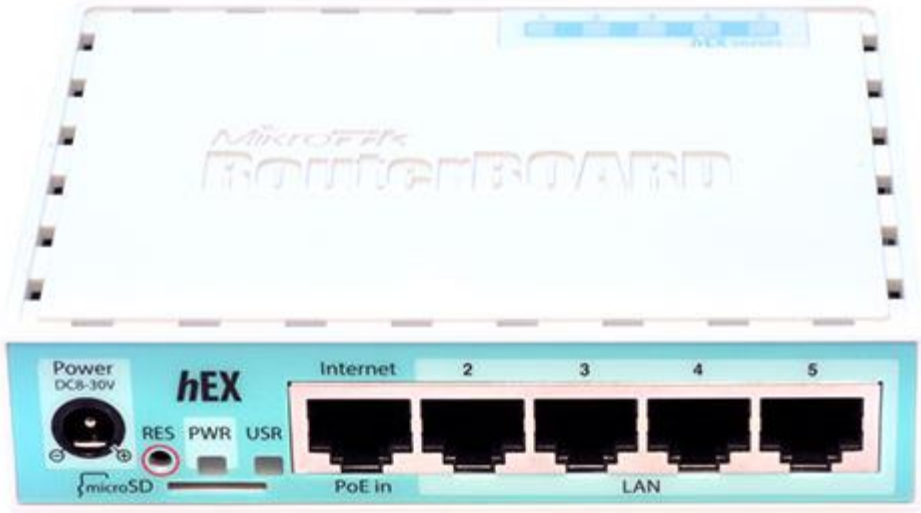

Рисунок 2.4 – MikroTik hEX RB750Gr3

MikroTik hEX представляє собою маршрутизатор з підтримкою апаратного шифрування IPsec. Даний пристрій містить п'ять мережевих портів з підтримкою швидкості передачі даних на рівні 1 Гбіт/с. Окрім цього, наявний порт USB 2.0 (повнорозмірний), що дає можливість підключати модеми з підтримкою технологій 3G/4G , а також зовнішніх flash-носіїв. Також існує можливість використання microSD.

В якості пристрою керування пристроєм використовується процесор з тактовою частотою 880 МГц з двома фізичними ядрами, що працює у чотири потоки. У випадку застосування алгоритму шифрування AES-128 з розміром пакетів 1,4 Кбайт досягається швидкість обміну даними до 472 Мбіт/с.

MikroTik hEX володіє оперативною пам'яттю в об’ємі 256 Мб, дозволяє живити і віддалено звертатися до нього за допомогою технології POE. У базовій комплектацій відсутній POE інжектор.

MikroTik RB750Gr3 на рівні системного програмного забезпечення використовує операційну систему RouterOS Level4, що володіє потужними функціональними можливостями щодо налаштування.

До основних функціональних можливостей маршрутизатора MikroTik RB750Gr3 належать:

– обмеження швидкості передачі даних для користувачів;

– налаштування заборони доступу до соцмереж та/або торентів;

– можливість налаштування HotSpot з перенаправленням на рекламну сторінку;

– організація віддаленого захищеного підключення та можливістю організації VPN і т.п.;

– підтримка «The Dude Server», що дозволяє проводити моніторинг у мережі різних пристроїв і сервісів, а також встановлення комунікації між ними та оповіщення при виникненні збоїв.

Структурна схеми та інтерфейси MikroTik RB750Gr3 показано на рис. 2.5.

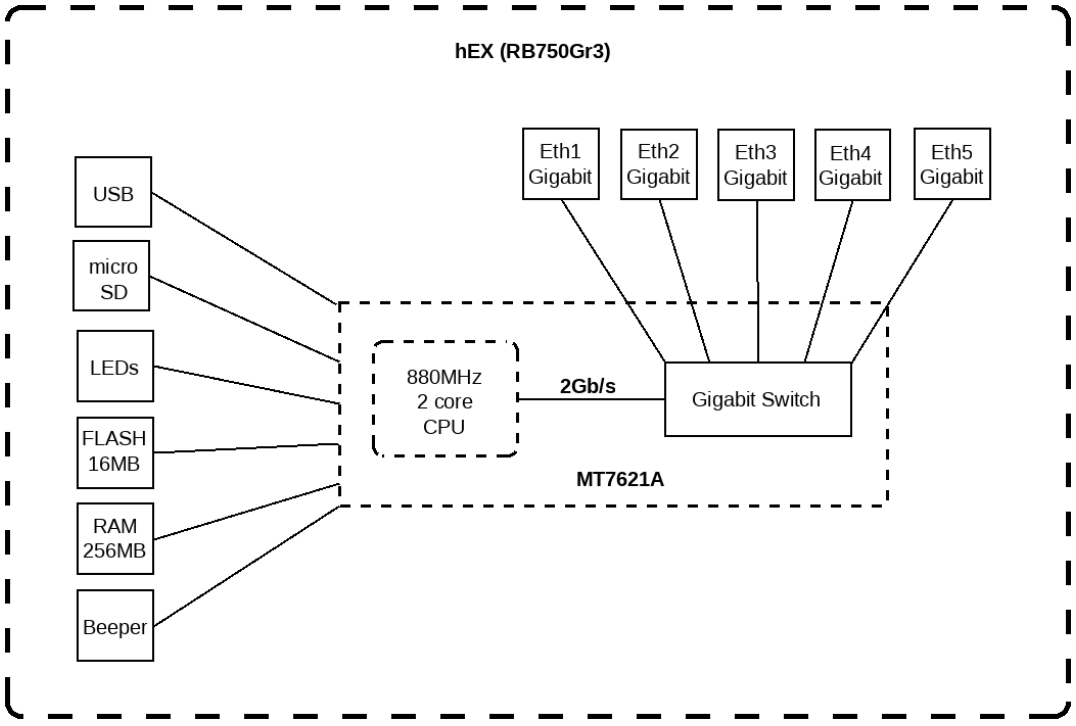

Рисунок 2.5 – Блок схема MikroTik RB750Gr3

Основні технічні характеристики маршрутизатора MikroTik RB750Gr3 показано у таблиці 2.4.

Таблиця 2.4 – Основні технічні характеристики MikroTik RB750Gr3

Характеристика	Значення
Процессор:	MT7621A 880 МГц, 2 ядра і 4 потоки
RAM:	256 MB
Flash:	16 MB
Порти	5 × 10/100/1000 Mbit/s Ethernet RJ45 1 × USB 2.0 1 × microSD slot
Операційна система	MikroTik RouterOS Level4
Електроживлення	PoE: 8..30 V DC on Ethernet port1 jack**:**8..30 V DC
Споживана потужність	до 5 Вт

Комутатором третього поверху є TP-Link TL-SL5428E, що представляє собою керований комутатор другого рівня і призначений для побудови мереж ETTX, FTTX та Enterprise ринку.

Даний комутатор можна монтувати у стійку 19”, а його висота становить 1U. TP-Link TL-SL5428E має інтегровані двадцять чотири порти Fast Ethernet, а також чотири комбінованих гігабітних/SFP-порти. Характерною особливістю SFP-портів є забезпечення швидкості передачі даних на рівні не більше 4 Гбіт/с і здатність до підтримки архітектури подвійного кільця.

З точки зору надійності, TL-SL5428E містить захисний механізм від ураження блискавкою до 6 кВ. Основними показниками забезпечення ефективності використання даного виду комутатора є:

– висока продуктивність,
– пріоритезація трафіку на рівні підприємства,
– наявність розширених функцій безпеки

– наявність широкого набору функцій управління другого рівня та Metro Ethernet.

До основних функцій щодо налаштування та забезпечення безпеки належать:

– функції прив'язки за IP-адресами;

– функції прив’язки за MAC-адресою;

– функції прив’язки за портами і VID;

– захист від заміни IP-адреси, DHCP Snooping, портів;

– обмеження швидкості;

– захисту від широкомовних мережевих штормів, ARP-атак;

– здатність розпізнавання типових DoS-атак;

– функція списку контролю доступу дозволяє обмежувати доступ до критичних ресурсів мережі, забороняючи передачу пакетів на основі фільтрації MAC- та IP-адрес, TCP/UDP-портів та призначення та VLAN ID.

– підтримка аутентифікації 802.1X, яка використовується разом з RADIUS/TACACS+-сервером для запиту інформації з аутентифікації до надання доступу до мережі.

На рисунку 2.6 показано зовнішній вигляд підключеного комутатора TL-SL5428E.

Рисунок 2.6 – Зовнішній вигляд TP-LINK TL-SL5428E

Розширення функціональних можливостей комутатора другого рівня TL-SL5428E передбачає імплементацію таких функція як:

– здатність налаштування VLAN на портах комутатора (802/1Q);

– дзеркалювання портів;

– підтримка протоколу LACP і здатності моніторингу потоків 802.3x.

Відносно розширеності можливостей моніторингу стану, у якому перебуває мережа, комутатор може:

– виявляти петлі;

– діагностувати обриви кабелів;

– виявляти однонаправлений канал обміну даними та IGMP/MLD Snooping.

IGMP/MLD snooping функціонально визначає «розумну передачу» multicast-потоку лише визначеним користувачам. Налаштування обмежень та фільтрації IGMP дають змогу накладати обмеження для наявних користувачів на рівні порту, що забезпечують і запобігають неавторизованому multicast-доступу.

Для вирішення задачі об’єднання передачі голосової, мультимедійної та іншої інформації, TL-SL5428E володіє потужними можливостями щодо налаштування пріоритету (QoS).

На системного адміністратора покладаються функції розподілу пріоритетності трафіку за визначеними категоріями, що може включати IP чи MAC-адреси, тип (TCP, UDP) порту і його номер з метою забезпечення якості передачі голосових чи мультимедійних повідомлень.

Особливістю комутатора TL-SL5428E є зручність у використанні та простота налаштування. До зручних та інтуїтивно зрозумілих можливостей належать:

– орієнтований на користувача графічний інтерфейс;

– наявність командної стрічки для advanced адміністраторів;

– можливість шифрування даних за допомогою SSL або SSH;

– наявність підтримки протоколу LLDP дозволяє швидко виявити нове мережеве обладнання;

– можливість побудови топології на основі системи керування мережею;

– підтримка SNMP (v1/2/3) та RMON забезпечує формування запитів щодо стану мережевих клієнтів і відправлення повідомлень при виникненні критичного стану;

– наявність механізму гнучкого формування IP-адрес з використанням DHCP;

– здатність до кластеризації IP-адрес, що значно підвищує ефективність процесу управління за рахунок налаштовування, контролю та забезпечення функціональності наявних комутаторів з будь-якого ПК з наявним веб-браузером та унікальну IP-адресою.

При організації комп'ютерної мережі першого і другого поверхів використано комутатори HP ProCurve 1700. На рисунку 2.7 показано зовнішній вигляд даного комутатора.

Рисунок 2.7 – Комутатор HP ProCurve 1700-24

До складу комутатора HP ProCurve 1700 – 24 входить два безвентиляторних комутатори, які підтримують веб управління та швидкість передачі даних 10/100 Мб/с. Даний вид комутаційних пристроїв широко використовуються в офісах різних компаній, зокрема тих, де необхідно забезпечити тишу і забезпечити перехід від некерованих КМ до керованих.

Загалом комутатор HP ProCurve 1700-24 представляє собою 24-портовий мережевий пристрій, який включає 22 порти 10/100 Мб/с та два порти Dual-Personality. У таблиці 2.5 наведено основні технічні та експлуатаційні характеристики комутатора HP ProCurve 1700-24.

Таблиця 2.5 – Основні характеристики комутатора HP ProCurve 1700-24

Характеристика	Значення характеристики
Рівень комутатора	Керований другого рівня
Кількість RJ45 портів	24 порти
Підтримка POE	Відсутня
Формфактор	Монтаж в стойку
Зовнішні порти вводу/виводу	22 порти з автовизначенням 10/100 (протокол: IEEE 802.3, тип: 10Base-T, протокол IEEE 802.3u, тип 100Base-TX); Дуплексний режим: повно- або напівдуплексний; Тип носія: ProCurve Auto-MDIX; 2 порти подвійного призначення: кожен порт може використовуватися як порт RJ-45 з автовизначенням 10/100/1000 (протокол IEEE 802.3, тип 10Base-T; протокол IEEE 802.3u, тип 100Base-TX; протокол IEEE 802.3ab, 1000Base-T Gigabit Ethernet) або як вільний слот mini-GBIC (для використання з трансиверами mini-GBIC)
Монтаж	Монтується в стандартну для EIA 19-дюймову стійку Telco або шафу для електроживлення
Пам’ять і процесор	Флеш-пам’ять 2 Мб Об’єм RAM/ROM 2 Кб Розмір пакетного буфера: 500 Кб
Час затримки	100 Мб: <4,7 мкс (розмір пакету 64 байти); 1000 Мб: <3,0 мкс (розмір пакету 64 байти)
Розмір таблиці адрес	8 000 елементов
Продуктивність маршрутизації /комутації	8,4 Гбіт/с

Продовження таблиці 2.5

Характеристика	Значення характеристики
Функції керування	ProCurve Manager; Web-браузер
Протоколи зв’язку	Загальні протоколи: Пріоритетність за протоколом IEEE 802.1p; IEEE 802.1Q VLAN; IEEE 802.3ad Link Aggregation; Control Protocol (LACP); IEEE 802.3x Flow Control; Управління мережею: Протокол IEEE 802.1AB Link Layer; Discovery Protocol (LLDP)
Вимоги до живлення	100-127 / 200-240 В змінного струму; 50/60 Гц
Загальна потужність	0,75 А /0,4 А
Споживана потужність	24 Вт
Умови експлуатації:	
Безпека	CSA 22.2 No. 60950; EN 60950/IEC 60950; UL 60950
Електромагнітна сумісність	Правила FCC, частина 15, підрозділ B, клас A; EN55022; VCCI; ICES-003 (Канада)
Діапазон температур при експлуатації	від 0° до 40° С
Вологість при експлуатації	від 15 до 95% відносної вологості

2.5 Логічна адресація робочих станцій та серверів

У результаті аналізу фізичної топології та інформаційних потоків, притаманних об’єкту проектування, спроектовано логічну топологію комп’ютерної мережі, яка показана на рисунку 2.8.

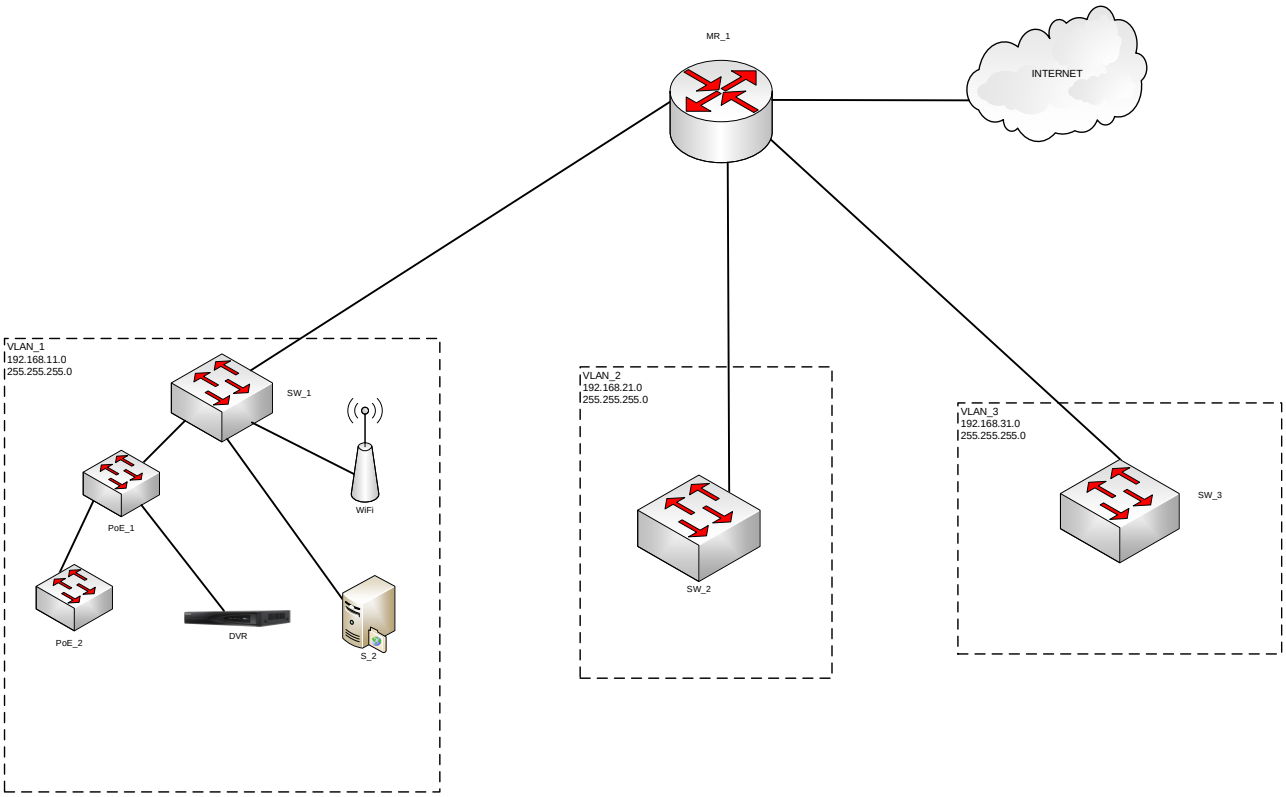

Рисунок 2.8 – Логічна топологія комп’ютерної мережі з сервісами безпеки та віддаленого доступу

Як видно з рисунку 2.8, комп’ютерну мережу з сервісами безпеки та віддаленого доступу до ресурсів підприємства сегментовано на три частини, відповідно створено 3 VLAN.

VLAN_1 налаштовано для робочих станцій, які знаходяться на першому поверсі будівлі. Окрім робочих станцій працівників, для цієї локації характерним є підключення відеокамер спостереження та відповідного апаратного і програмного забезпечення для управління IP-камерами. Окрім цього, для надання гостьового доступу використовується WIFI-маршрутизатор фірми Netis, що працює в режимі Access Point. У таблиці 2.6 наведено IP-

адресну схему робочих станцій і компонентів відеоспостереження першого поверху будівлі.

Таблиця 2.6 – IP-адресна схема робочих станцій першого поверху

Позначення робочої станції	IP-адреса	Адреса підмережі	Маска підмережі	IDVlan
IP_10	192.168.11.1	192.168.11.0	255.255.255.0	1
IP_11	192.168.11.2	192.168.11.0	255.255.255.0	1
IP_12	192.168.11.3	192.168.11.0	255.255.255.0	1
IP_21	192.168.11.4	192.168.11.0	255.255.255.0	1
IP_22	192.168.11.5	192.168.11.0	255.255.255.0	1
IP_23	192.168.11.6	192.168.11.0	255.255.255.0	1
IP_24	192.168.11.7	192.168.11.0	255.255.255.0	1
IP_31	192.168.11.8	192.168.11.0	255.255.255.0	1
IP_51	192.168.11.9	192.168.11.0	255.255.255.0	1
IP_52	192.168.11.10	192.168.11.0	255.255.255.0	1
IP_53	192.168.11.11	192.168.11.0	255.255.255.0	1

У таблиці 2.7 наведено IP-адресну схему робочих станцій другого поверху комп’ютерної мережі з сервісами безпеки і віддаленого доступу.

Таблиця 2.7 - IP-адресна схема робочих станцій другого поверху

Позначення робочої станції	IP-адреса	Адреса підмережі	Маска підмережі	IDVlan
IP_2010	192.168.21.1	192.168.21.0	255.255.255.0	2
IP_2020	192.168.21.2	192.168.21.0	255.255.255.0	2
IP_2060	192.168.21.3	192.168.21.0	255.255.255.0	2
IP_2061	192.168.21.4	192.168.21.0	255.255.255.0	2

Продовження таблиці 2.7

Позначення робочої станції	IP-адреса	Адреса підмережі	Маска підмережі	IDVlan
IP_2062	192.168.21.5	192.168.21.0	255.255.255.0	2
IP_2063	192.168.21.6	192.168.21.0	255.255.255.0	2
IP_2070	192.168.21.7	192.168.21.0	255.255.255.0	2
IP_2150	192.168.21.8	192.168.21.0	255.255.255.0	2
IP_2151	192.168.21.9	192.168.21.0	255.255.255.0	2
IP_2152	192.168.21.10	192.168.21.0	255.255.255.0	2
IP_2153	192.168.21.11	192.168.21.0	255.255.255.0	2
IP_2154	192.168.21.12	192.168.21.0	255.255.255.0	2
IP_2155	192.168.21.13	192.168.21.0	255.255.255.0	2

У таблиці 2.8 наведено IP-адресну схему третього поверху комп’ютерної мережі.

Таблиця 2.8 – IP-адресна схема робочих станцій третього поверху

Позначення робочої станції	IP-адреса	Адреса підмережі	Маска підмережі	IDVlan
IP_3010	192.168.31.1	192.168.31.0	255.255.255.0	3
IP_3011	192.168.31.2	192.168.31.0	255.255.255.0	3
IP_3012	192.168.31.3	192.168.31.0	255.255.255.0	3
IP_3030	192.168.31.4	192.168.31.0	255.255.255.0	3
IP_3031	192.168.31.5	192.168.31.0	255.255.255.0	3
IP_3032	192.168.31.6	192.168.31.0	255.255.255.0	3
IP_3033	192.168.31.7	192.168.31.0	255.255.255.0	3
IP_3034	192.168.31.8	192.168.31.0	255.255.255.0	3
IP_3035	192.168.31.9	192.168.31.0	255.255.255.0	3
IP_3040	192.168.31.10	192.168.31.0	255.255.255.0	3
IP_3050	192.168.31.11	192.168.31.0	255.255.255.0	3

Продовження таблиці 2.8

Позначення робочої станції	IP-адреса	Адреса підмережі	Маска підмережі	IDVlan
IP_3051	192.168.31.12	192.168.31.0	255.255.255.0	3
IP_3060	192.168.31.13	192.168.31.0	255.255.255.0	3
IP_3061	192.168.31.14	192.168.31.0	255.255.255.0	3
IP_3062	192.168.31.15	192.168.31.0	255.255.255.0	3
IP_3063	192.168.31.16	192.168.31.0	255.255.255.0	3
IP_3064	192.168.31.17	192.168.31.0	255.255.255.0	3
IP_3065	192.168.31.18	192.168.31.0	255.255.255.0	3
IP_3170	192.168.31.19	192.168.31.0	255.255.255.0	3
IP_3171	192.168.31.20	192.168.31.0	255.255.255.0	3
IP_3172	192.168.31.21	192.168.31.0	255.255.255.0	3

До складу VLAN_1 входять також 14 IP-камер, адресація яких показана у таблиці 2.9.

Таблиця 2.9 – Адресація IP-камер

Мітка IP-камери	IP-адреса	Адреса підмережі	Маска підмережі	IDVlan
IP_CAM_1	192.168.21.202	192.168.21.0	255.255.255.0	1
IP_CAM_2	192.168.21.203	192.168.21.0	255.255.255.0	1
IP_CAM_3	192.168.21.204	192.168.21.0	255.255.255.0	1
IP_CAM_4	192.168.21.205	192.168.21.0	255.255.255.0	1
IP_CAM_5	192.168.21.206	192.168.21.0	255.255.255.0	1
IP_CAM_6	192.168.21.207	192.168.21.0	255.255.255.0	1
IP_CAM_7	192.168.21.208	192.168.21.0	255.255.255.0	1
IP_CAM_8	192.168.21.209	192.168.21.0	255.255.255.0	1
IP_CAM_9	192.168.21.210	192.168.21.0	255.255.255.0	1
IP_CAM_10	192.168.21.211	192.168.21.0	255.255.255.0	1

Продовження таблиці 2.9

Мітка IP-камери	IP-адреса	Адреса підмережі	Маска підмережі	IDVlan
IP_CAM_11	192.168.21.212	192.168.21.0	255.255.255.0	1
IP_CAM_12	192.168.21.213	192.168.21.0	255.255.255.0	1
IP_CAM_13	192.168.21.214	192.168.21.0	255.255.255.0	1
IP_CAM_14	192.168.21.215	192.168.21.0	255.255.255.0	1
DVR	192.168.21.201	192.168.21.0	255.255.255.0	1

IP-адресація пристроїв комутації і маршрутизації показана у таблиці 2.10.

Таблиця 2.10 – IP-адресація пристроїв комутації і маршрутизації

Мережевий пристрій	Інтерфейс (№ порта)	IP-адреса	Адреса підмережі	Маска підмережі	ID VLan
MR_1	5	192.168.11.0	192.168.11.0	255.255.255.0	1
	4	192.168.21.0	192.168.21.0	255.255.255.0	2
	3	192.168.31.0	192.168.31.0	255.255.255.0	3
	Інтернет	31.14x.1xx.1xx			
	bridge	192.168.88.1	192.168.21.0	255.255.255.0	local
SW_1	LAN	192.168.11.200	192.168.11.0	255.255.255.0	1
SW_2	LAN	192.168.21.200	192.168.21.0	255.255.255.0	2
SW_3	LAN	192.168.31.250	192.168.21.0	255.255.255.0	3
AP	LAN	192.168.11.199	192.168.11.0	255.255.255.0	1

Таким чином, у результаті проведеного розбиття на підмережі на основі створення Virtual Local Area Network , забезпечено логічний та фізичний розподіл прав доступу до ресурсів у комп’ютерній мережі, що є одним з аспектів організації сервісу безпеки.

2.6 Комутація з’єднань комп’ютерної мережі

Для того, щоб забезпечити зручність та ефективність обслуговування комп’ютерної мережі кожен кабель, який з’єднує робочу станцію з комутуючим обладнанням промарковано і розроблено схеми комутаційних з’єднань, які наведено у таблицях 2.11 –2.14.

Таблиця 2.11 – Схема комутації з’єднань комп’ютерної мережі (1-ий поверх)

Комутаційний пристрій	Інтерфейс кінцевого пристрою	Інтерфейс патч-панелі	Розетка/ інтерфейс
SW_1	FE0/1	FE0/1	IP_10
	FE0/2	FE0/2	IP_11
	FE0/3	FE0/3	IP_12
	FE0/4	FE0/4	IP_21
	FE0/5	FE0/5	IP_22
	FE0/6	FE0/6	IP_23
	FE0/7	FE0/7	IP_24
	FE0/8	FE0/8	IP_31
	FE0/9	FE0/9	IP_51
	FE0/10	FE0/10	IP_52
	FE0/11	FE0/11	IP_53
	FE0/12	FE0/12	AP
	FE0/13	FE0/13	-
	FE0/14	FE0/14	-
	FE0/15	FE0/15	-
	FE0/16	FE0/16	-
	FE0/17	FE0/17	-
	FE0/18	FE0/18	-
	FE0/19	FE0/19	-

Продовження таблиці 2.11

Комутаційний пристрій	Інтерфейс кінцевого пристрою	Інтерфейс патч-панелі	Розетка/ інтерфейс
SW_1	FE0/20	FE0/20	-
	FE0/21	FE0/21	POE_1
	FE0/22	FE0/22	-
	FE0/23	FE0/23	-
	FE0/24	FE0/24	MR_1

У таблиці 2.12 наведено комутацію з’єднань робочих станцій та мережевого обладнання другого поверху.

Таблиця 2.12 – Схема комутації з’єднань комп’ютерної мережі (2-ий поверх)

Комутаційний пристрій	Інтерфейс кінцевого пристрою	Інтерфейс патч-панелі	Розетка/ інтерфейс
SW_2	FE0/1	FE0/1	IP_2010
	FE0/2	FE0/2	IP_2020
	FE0/3	FE0/3	IP_2060
	FE0/4	FE0/4	IP_2061
	FE0/5	FE0/5	IP_2062
	FE0/6	FE0/6	IP_2063
	FE0/7	FE0/7	IP_2070
	FE0/8	FE0/8	IP_2150
	FE0/9	FE0/9	IP_2151
	FE0/10	FE0/10	IP_2152
	FE0/11	FE0/11	IP_2153
	FE0/12	FE0/12	IP_2154
	FE0/13	FE0/13	IP_2155

Продовження таблиці 2.12

Комутаційний пристрій	Інтерфейс кінцевого пристрою	Інтерфейс патч-панелі	Розетка/ інтерфейс
SW_2	FE0/14	FE0/14	-
	FE0/15	FE0/15	-
	FE0/16	FE0/16	-
	FE0/17	FE0/17	-
	FE0/18	FE0/18	-
	FE0/19	FE0/19	-
	FE0/20	FE0/20	-
	FE0/21	FE0/21	-
	FE0/22	FE0/22	-
	FE0/23	FE0/23	-
	FE0/24	FE0/24	MR_1

У таблиці 2.13 наведено комутацію з’єднань на третьому поверсі будівлі.

Таблиця 2.13 – Схема комутації з’єднань комп’ютерної мережі будівлі (3-ий поверх)

Комутаційний пристрій	Інтерфейс кінцевого пристрою	Інтерфейс патч-панелі	Розетка/ інтерфейс
SW_3	FE0/1	FE0/1	IP_3010
	FE0/2	FE0/2	IP_3011
	FE0/3	FE0/3	IP_3012
	FE0/4	FE0/4	IP_3030
	FE0/5	FE0/5	IP_3031
	FE0/6	FE0/6	IP_3032
	FE0/7	FE0/7	IP_3033

Продовження таблиці 2.13

Комутаційний пристрій	Інтерфейс кінцевого пристрою	Інтерфейс патч-панелі	Розетка/ інтерфейс
SW_3	FE0/8	FE0/8	IP_3034
	FE0/9	FE0/9	IP_3035
	FE0/10	FE0/10	IP_3040
	FE0/11	FE0/11	IP_3050
	FE0/12	FE0/12	IP_3051
	FE0/13	FE0/13	IP_3060
	FE0/14	FE0/14	IP_3061
	FE0/15	FE0/15	IP_3062
	FE0/16	FE0/16	IP_3063
	FE0/17	FE0/17	IP_3064
	FE0/18	FE0/18	IP_3065
	FE0/19	FE0/19	IP_3170
	FE0/20	FE0/20	IP_3171
	FE0/21	FE0/21	IP_3172
	FE0/22	FE0/22	-
	FE0/23	FE0/23	-
	FE0/24	FE0/24	-
	FE0/25	FE0/25	-
	FE0/26	FE0/26	-
	FE0/27	FE0/27	-
	FE0/28	FE0/28	MR_1

У таблиці 2.14 наведено комутацію з’єднання за портами MikroTik RB750Gr3.

Таблиця 2.14 – Комутація портів MikroTik RB750Gr3

Комутаційний пристрій	Інтерфейс MR_1	Інтерфейс кінцевого пристрою
MR_1	FE0/1(Internet)	Internet provider
	FE0/2	-
	FE0/3	SW_3
	FE0/4	SW_2
	FE0/5	SW_1

Таким чином при проектуванні комутаційних з’єднань комп’ютерної мережі враховано усі заходи щодо організації підтримки в процесі її експлуатації.

РОЗДІЛ 3 НАЛАШТУВАННЯ СЕРВІСІВ БЕЗПЕКИ ТА ВІДДАЛЕНОГО ДОСТУПУ ДО РЕСУРСІВ УПРАВЛІННЯ ПІДПРИЄМСТВОМ

3.1 Базові налаштування MikroTik RB750Gr3

У кваліфікаційній роботі запропоновано реалізувати сервіси безпеки і віддаленого доступу до ресурсів управління підприємством на основі налаштувань маршрутизатора MikroTik RB750Gr3, оскільки за технічними і функціональними характеристиками він відповідає критеріям економічної доцільності та надійності при забезпеченні авторизованого доступу в тому числі і віддаленого.

Для того, щоб провести налаштування маршрутизатора MikroTik RB750Gr3 перш за все необхідно мати сам пристрій, можливість підключення до інтернет-провайдера та ПК або ноутбук. Схема підключення роутера MikroTik показана на рисунку 3.1.

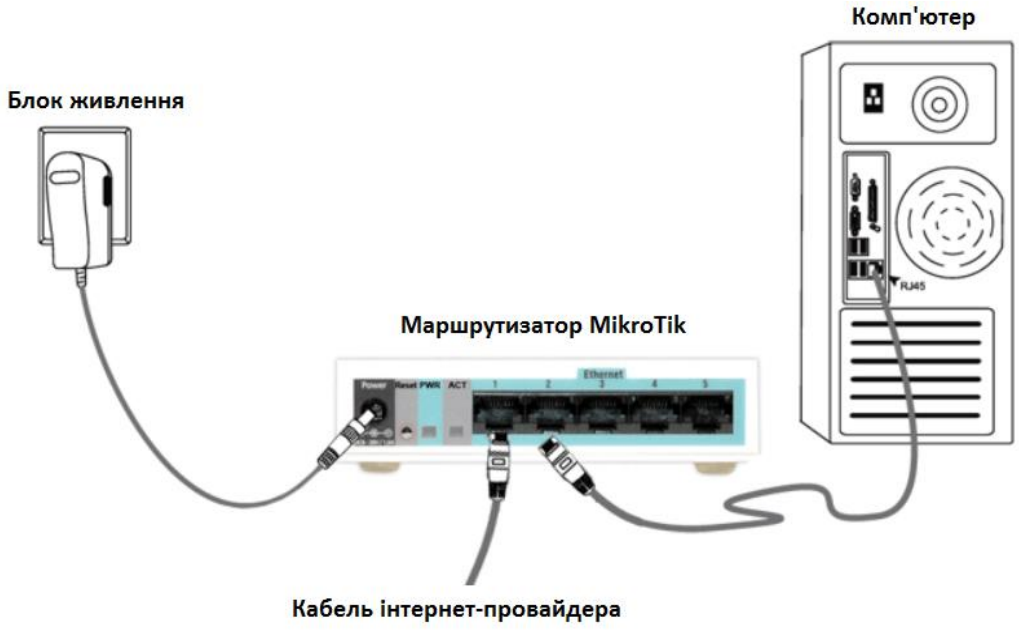

Рисунок 3.1 – Схема підключення маршрутизатора для базового налаштування

Як видно з рисунку 3.1, кабель інтернет-провайдера підключається до першого порту маршрутизатора MikroTik RB750Gr3, ноутбук або ПК підключається до будь-якого з вільних LAN-портів, а блок живлення у відповідний порт-роз'єм "Power".

Після підключення мережевого пристрою необхідно забезпечити можливість комунікації ПК з маршрутизатором. Для цього потрібно налаштувати мережеву плату в режимі одержання автоматичних налаштувань (рис. 3.2 і рис. 3.3).

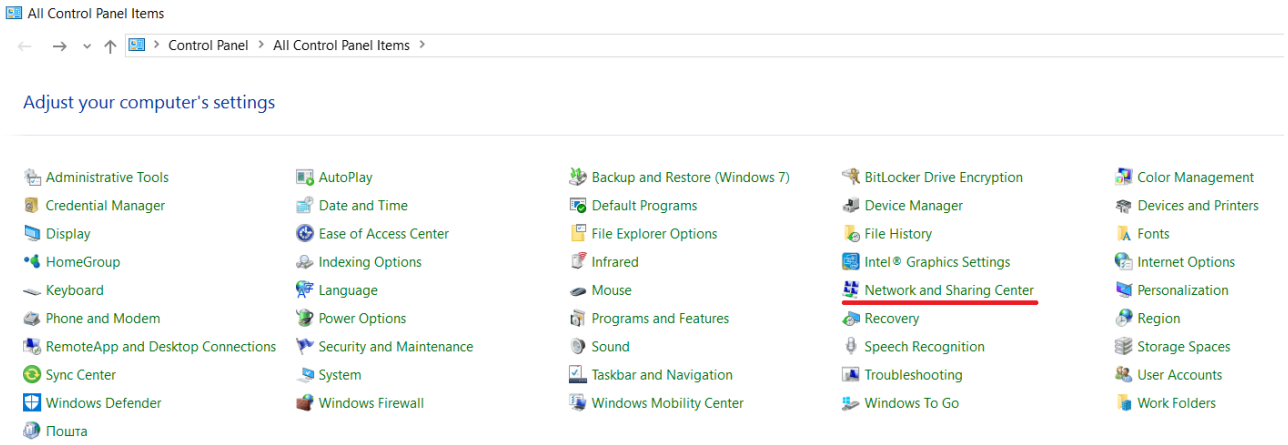

Рисунок 3.2 – Меню управління мережами

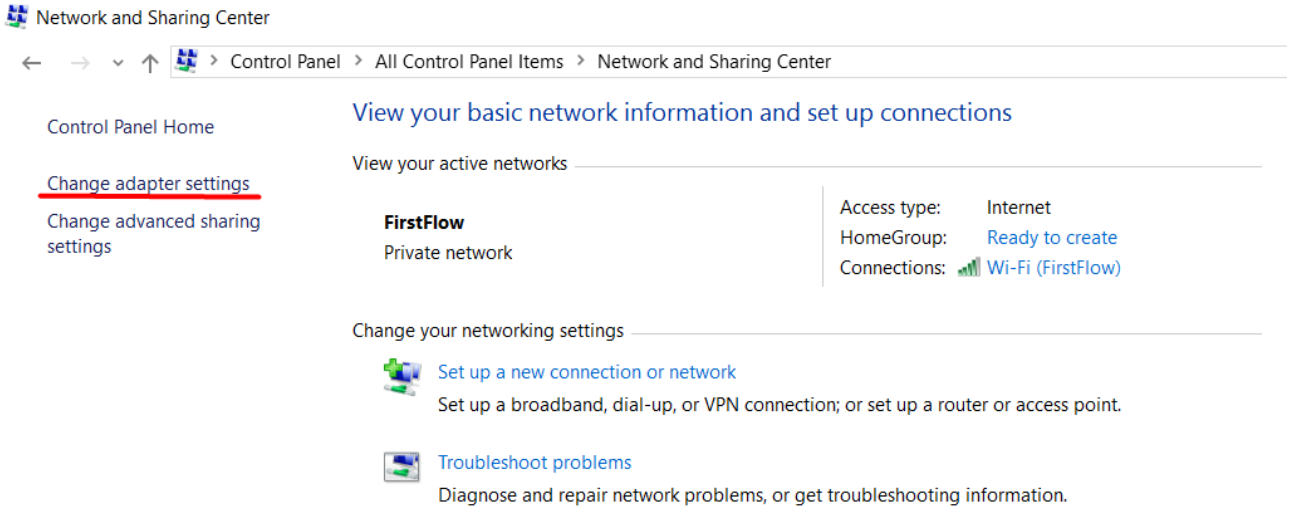

Рисунок 3.3 – Зміна параметрів мережевого адаптера

Після цього потрібно правою клавішею миші натиснути на «Ethernet» та обрати «Properties», як показано на рисунку 3.4.

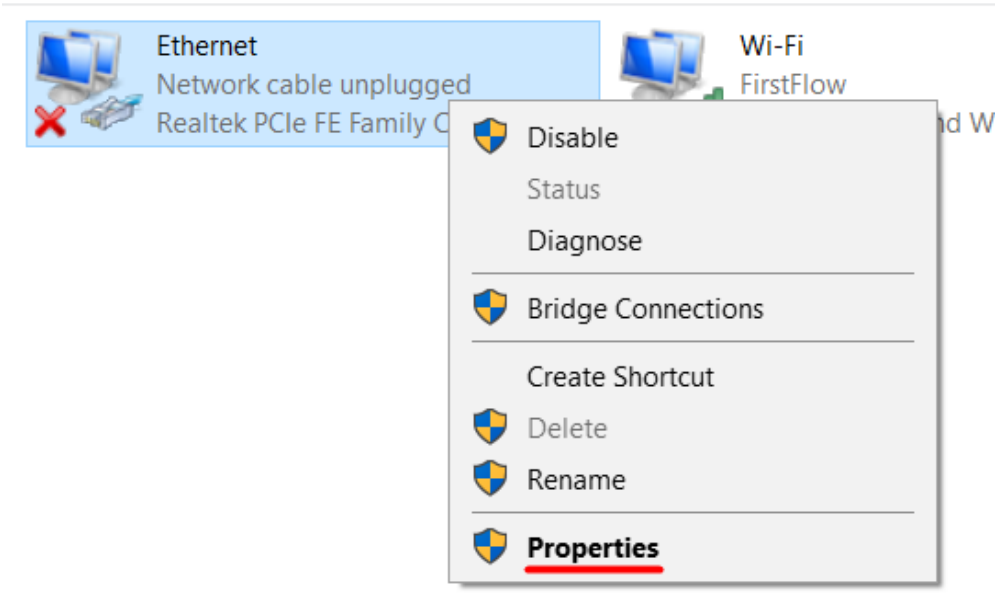

Рисунок 3.4 – Налаштування параметрів мережевого адаптера

Наступний крок полягає у налаштуванні «Internet Protocol Version 4 (TCP/IPv4)». Для цього потрібно відкрити одноіменний пункт меню та у вікні, що з'явилось вказати «Obtain an IP address automatically», як показано на рисунку 3.5.

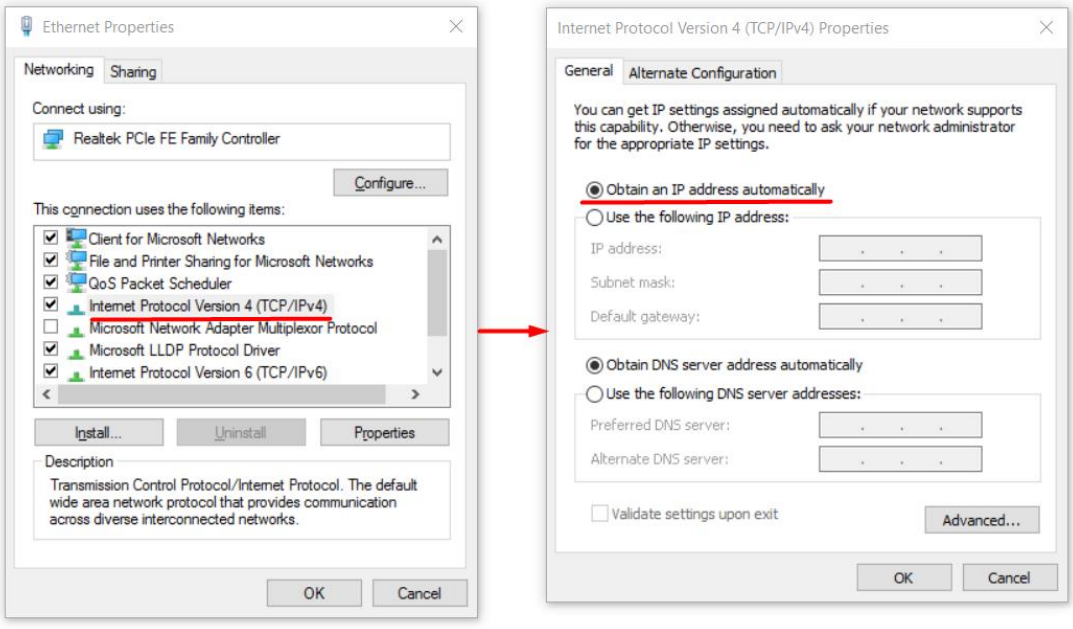

Рисунок 3.5 – Встановлення параметра «Obtain an IP address automatically»

Налаштування маршрутизатора MikroTik можна виконувати кількома способами:

– з використанням WinBox для ОС Windows;

– з використанням веб-браузера, перейшовши за адресою за замовчуванням «192.168.88.1»;

– з використанням Telnet.

Найбільш простим та інтуїтивно зрозумілим способом у даному випадку є використання WinBox. Запустивши дану програму і перейшовши на вкладку «Neighbors» можна побачити маршрутизатор, до якого потрібно виконати підключення. Зовнішній вигляд цього вікна показано на рисунку 3.6.

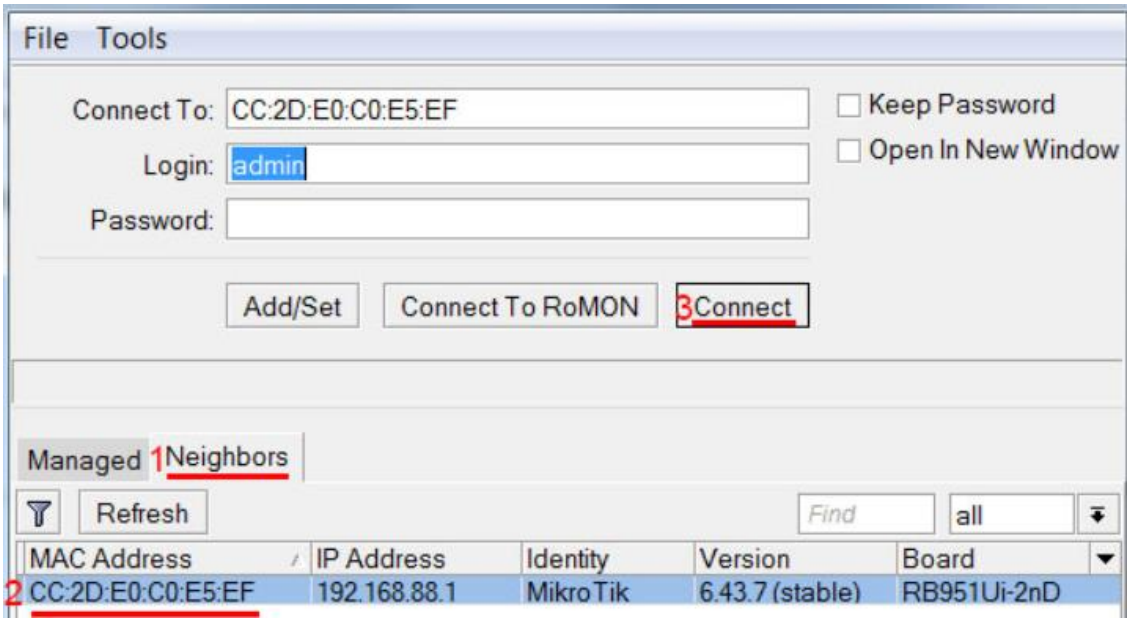

Рисунок 3.6 – Вкладка «Neighbors»

Після виконання наведених вище операцій, потрібно на лівою клавішею миші настиснути на MAC-адресі маршрутизатора і настиснути «Connect». За замовчуванням login=admin без паролю. Задавши пароль і перейшовши на першу вкладку «Managed» одержимо результат, як показано на рисунку 3.7.

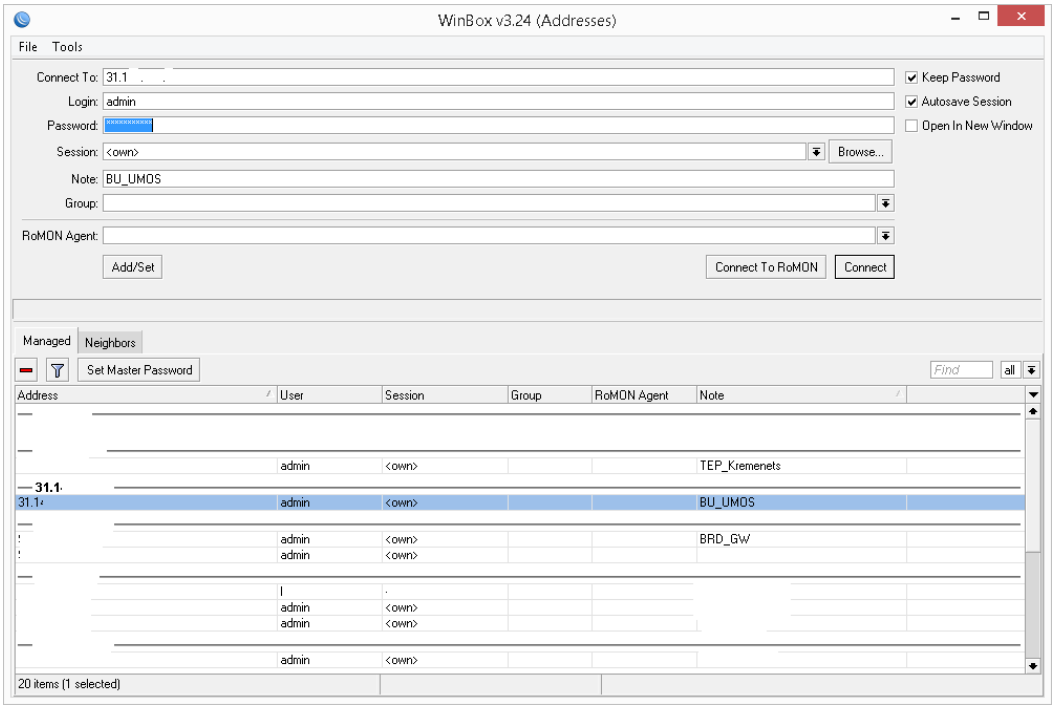

Рисунок 3.7 – Вікно управління та налаштування параметрів маршрутизатора

Після того, як встановлено з'єднання з MikroTik RB750Gr3, можна переходити до безпосереднього налаштування запропонованих рішень щодо декомпозиції на VLAN, формування адресного простору, налаштування правил безпеки та віддаленого доступу, які в комплексі утворюють відповідні сервіси. На рисунку 3.8 показано вікно з меню щодо налаштування параметрів роутера.

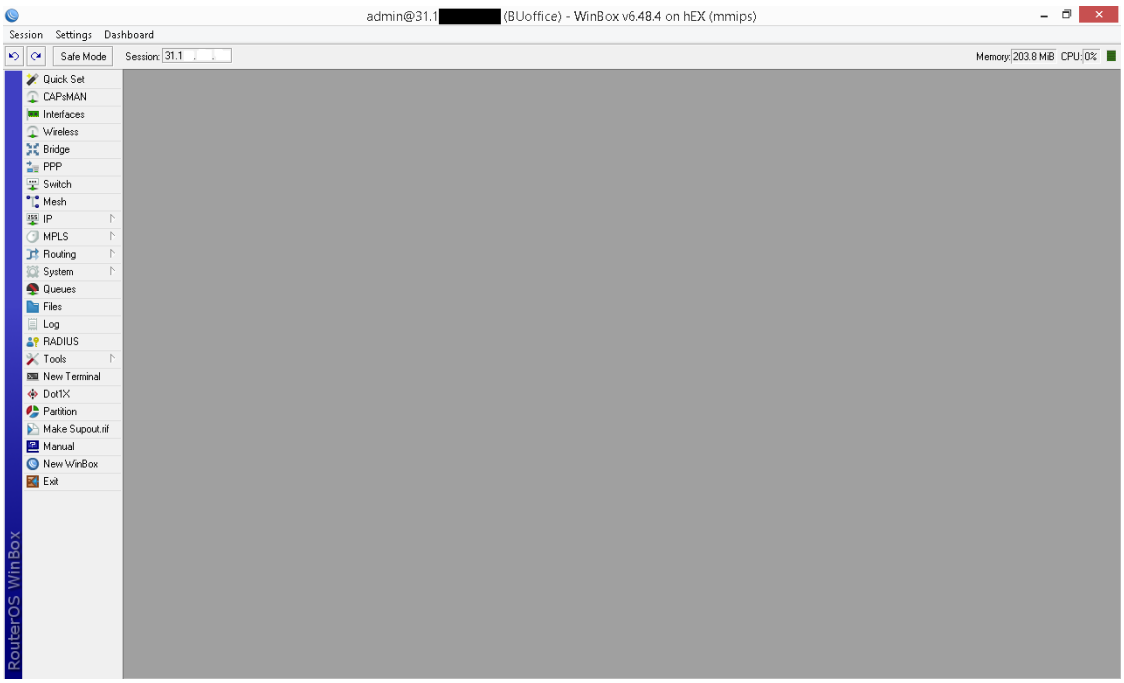

Рисунок 3.8 – Вікно налаштувань MikroTik RB750Gr3

3.2 Формування VLAN та налаштування сервісу безпеки

3.2.1 Налаштування VLAN

Перш за все для формування різноманітних правил щодо функціонування маршрутизатора і задання логіки забезпечення безпеки і віддаленого доступу необхідно володіти інформацією щодо типу маршрутизатора та його особливостей. Обравши «RouterBOARD» у меню «System» можна побачити коротку технічну інформацію про нього, як показано на рисунку 3.9.

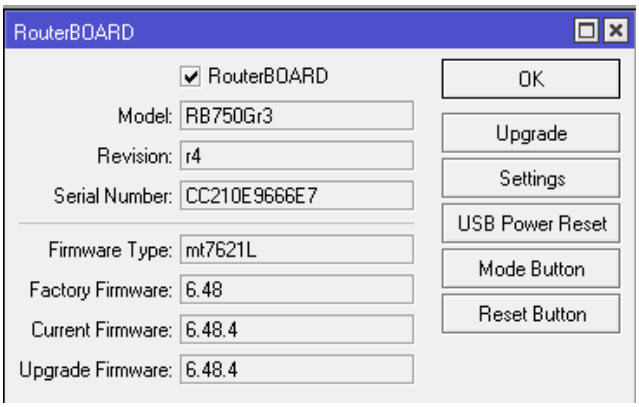

Рисунок 3.9 – Вікно «RouterBOARD»

Файли з резервними копіями налаштувань MikroTik RB750Gr3 можна подивитись у меню «Files->File List», як показано на рисуноку 3.10.

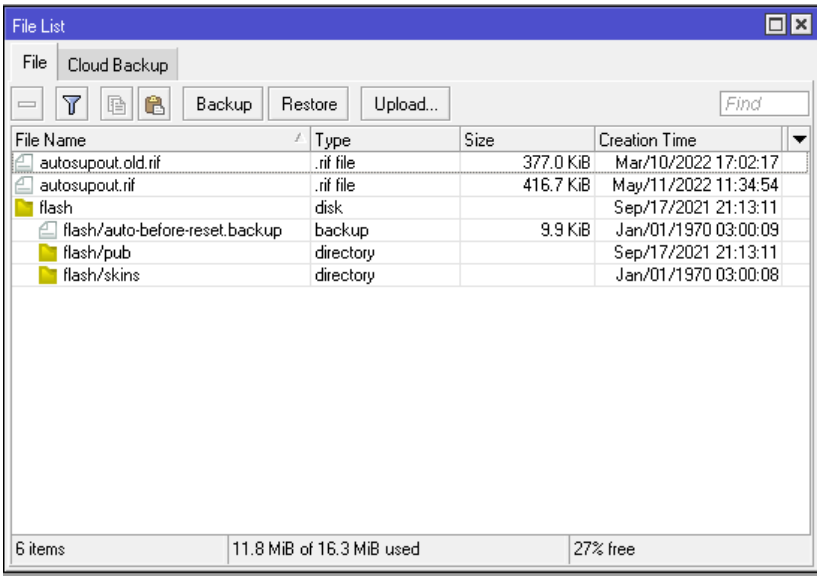

Рисунок 3.10 – BackUp файли налаштувань MikroTik RB750Gr3

Наступний крок полягає у налаштуванні типу доступу до маршрутизатора із вказання списку дозволеного IP-адресного простору. У даному випадку дозволено доступ з використанням WinBox та SSH, а всі інші методи доступу є заблокованими. Простори IP-адрес, доступ з яких дозволено, визначено наступним чином:

– 192.168.88.0/24 – IP-адреси з простору управління та налаштування маршрутизатора, шляхом фізичного безпосереднього підключення до нього

– 192.168.11.0/24 – IP-адреси локальної комп'ютерної мережі першого поверху будівлі

– 91. . .0/24 – IP-адреси, яким дозволений доступ до ресурсів ззовні.

На рисунку 3.11 показано налаштування доступу до маршрутизатора та відповідно ресурсів управління підприємством.

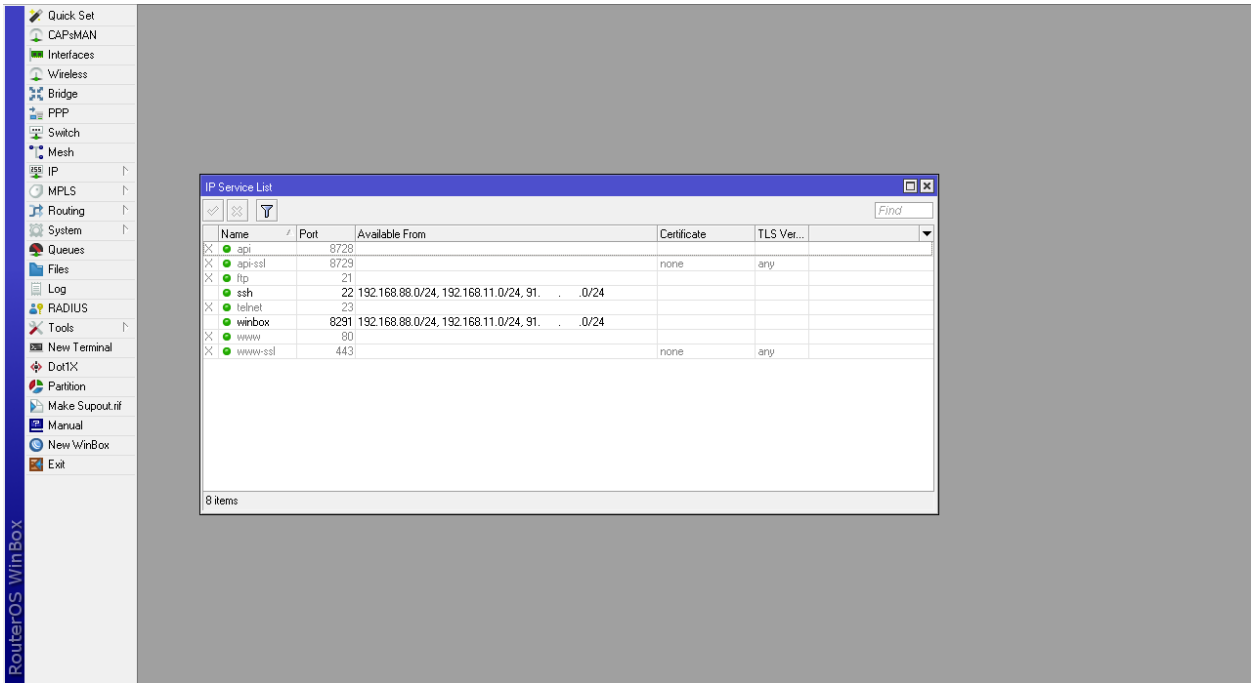

Рисунок 3.11 – Налаштування «IP Service List»

Налаштування VLAN за портами MikroTik RB750Gr3 наведено у лістингу 3.1, а результат налаштування показано на рисунку 3.12.

Лістинг 3.1 – Налаштування VLAN

```
/ip address
add    address=192.168.88.1/24    comment="My    IP,    bridge,
LAN_default" interface=\
    bridge network=192.168.88.0
add    address=192.168.11.254/24    comment="My    IP,    ether5,
LAN_floor1" interface=\
    ether5 network=192.168.11.0
add    address=192.168.21.254/24    comment="My    IP,    ether4,
LAN_floor2" interface=\
    ether4 network=192.168.21.0
add    address=192.168.31.254/24    comment="My    IP,    ether3,
LAN_floor3" interface=\
    ether3 network=192.168.31.0
```

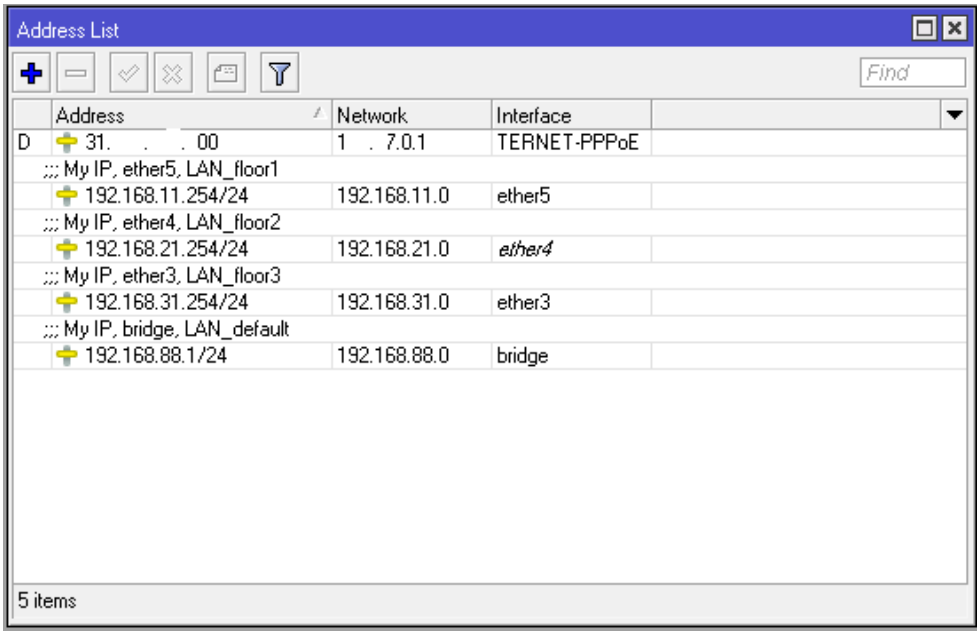

Рисунок 3.12 – Налаштування VLAN

Варто відмітити, що налаштування підмереж повністю відповідає запропонованій схемі IP-адресації і спроектованій логічній топології комп'ютерної мережі. Порт 1 маршрутизатора використовується для підключення до інтернет-провайдера, 2-ий порт – вільний, 3-ий – підмережа 3-го поверху, 4-ий порт – підмережа другого поверху, 5-ий порт – підмережа

першого поверху. Список доступних та використовуваних інтерфейсів показано на рисунку 3.13.

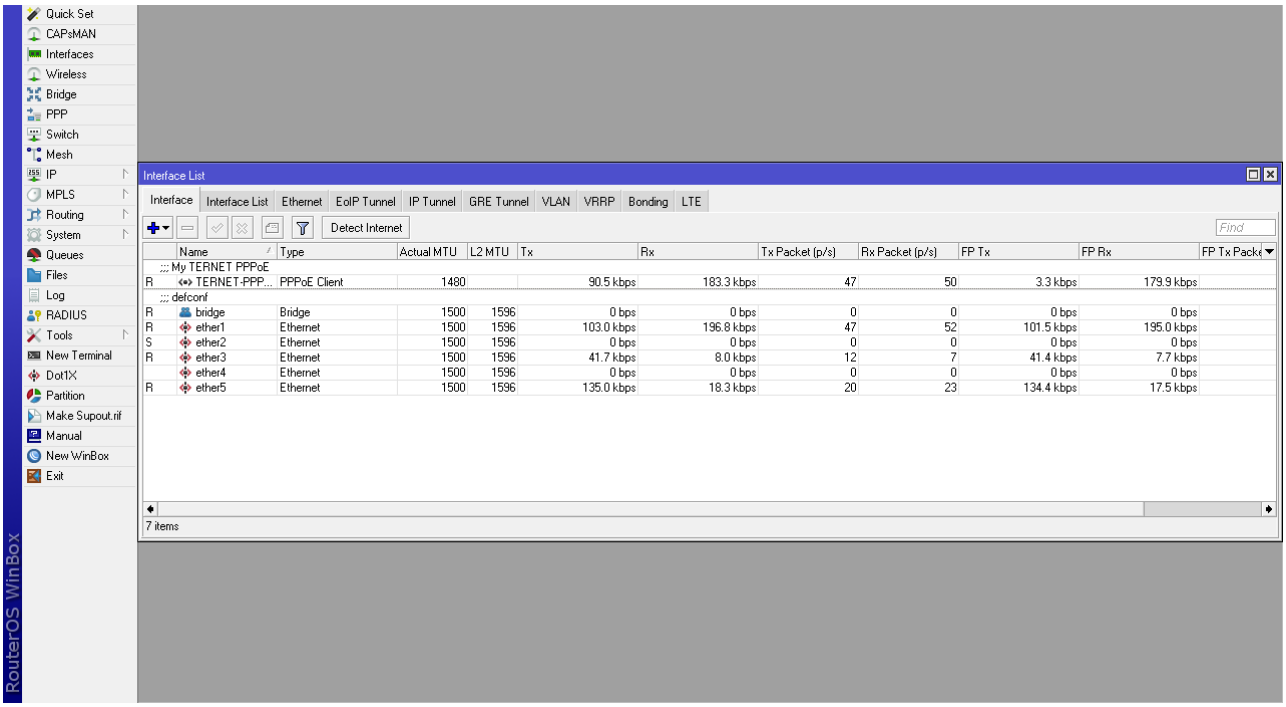

Рисунок 3.13 – «Interface List»

Як видно з рисунку 3.13 з’єднання з інтернет-провайдером відбувається за технологією PPPOE. Налаштування з’єднання з інтернет-провайдером наведено у лістингу 3.2.

Лістинг 3.2 – Налаштування PPPOE

```
/interface pppoe-client
add add-default-route=yes comment="My TERNET PPPoE" disabled=no
interface=\
    ether1 name=TERNET-PPPoE password=[redacted] user=[redacted]
/interface list
add comment=defconf name=WAN
add comment=defconf name=LAN
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
```

Налаштування правил та обмежень на множину IP-адресного простору за поверхами будівлі, в якій експлуатується комп'ютерна мережа, а також DHCP показано у лістингу 3.3.

Лістинг 3.3 – Налаштування правил та обмежень IP-адресного простору

```
/ip pool
add comment="My IP pool LAN_default" name=LAN_default-pool
ranges=\
    192.168.88.10-192.168.88.254
add comment="My IP pool LAN_floor1" name=LAN_floor1-pool
ranges=\
    192.168.11.50-192.168.11.99
add comment="My IP pool LAN_floor2" name=LAN_floor2-pool
ranges=\
    192.168.21.101-192.168.21.240
add comment="My IP pool LAN_floor3" name=LAN_floor3-pool
ranges=\
    192.168.31.101-192.168.31.240
add comment="My IP pool L2TP VPN" name=L2TP_VPN-pool ranges=\
    192.168.19.241-192.168.19.251
/ip dhcp-server
add address-pool=LAN_default-pool disabled=no interface=bridge
name=\
    DHCP_defconf
add address-pool=LAN_floor1-pool disabled=no interface=ether5
name=\
    DHCP_SRV-LAN_floor1
add address-pool=LAN_floor2-pool disabled=no interface=ether4
name=\
    DHCP_SRV-LAN_floor2
add address-pool=LAN_floor3-pool disabled=no interface=ether3
name=\
    DHCP_SRV-LAN_floor3
```

На рисунку 3.14 показано таблицю маршрутизації з доступними і налаштованими списками маршрутів, які обслуговує маршрутизатор.

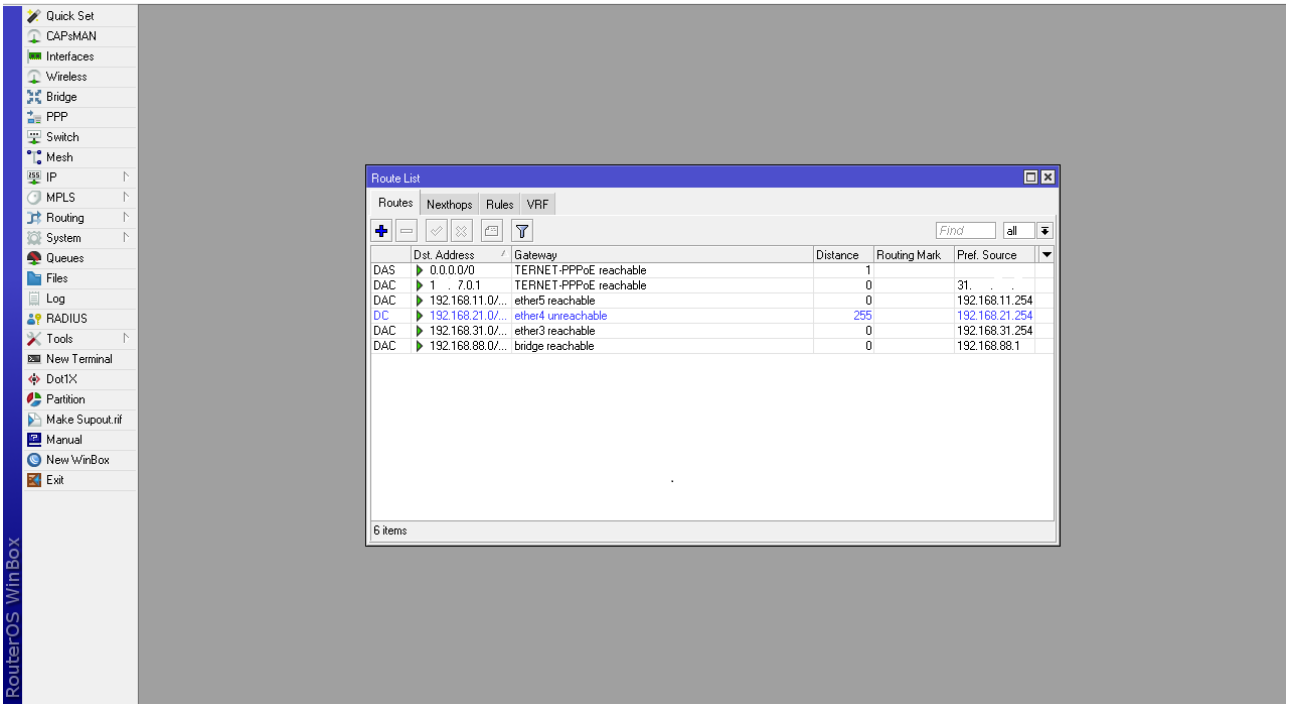

Рисунок 3.14 – Створена таблиця маршрутизації

На рисунку 3.15 – 3.16 візуалізовано налаштування DHCP сервера, що функціонує на базі маршрутизатора.

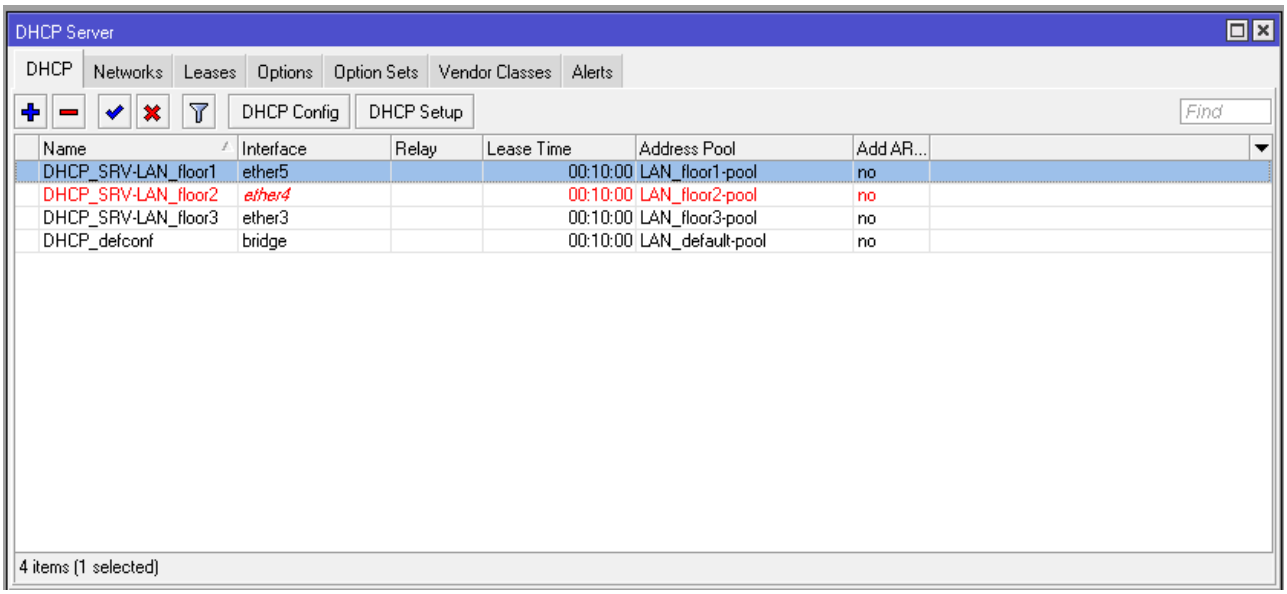

Рисунок 3.15 – Результат налаштування DHCP

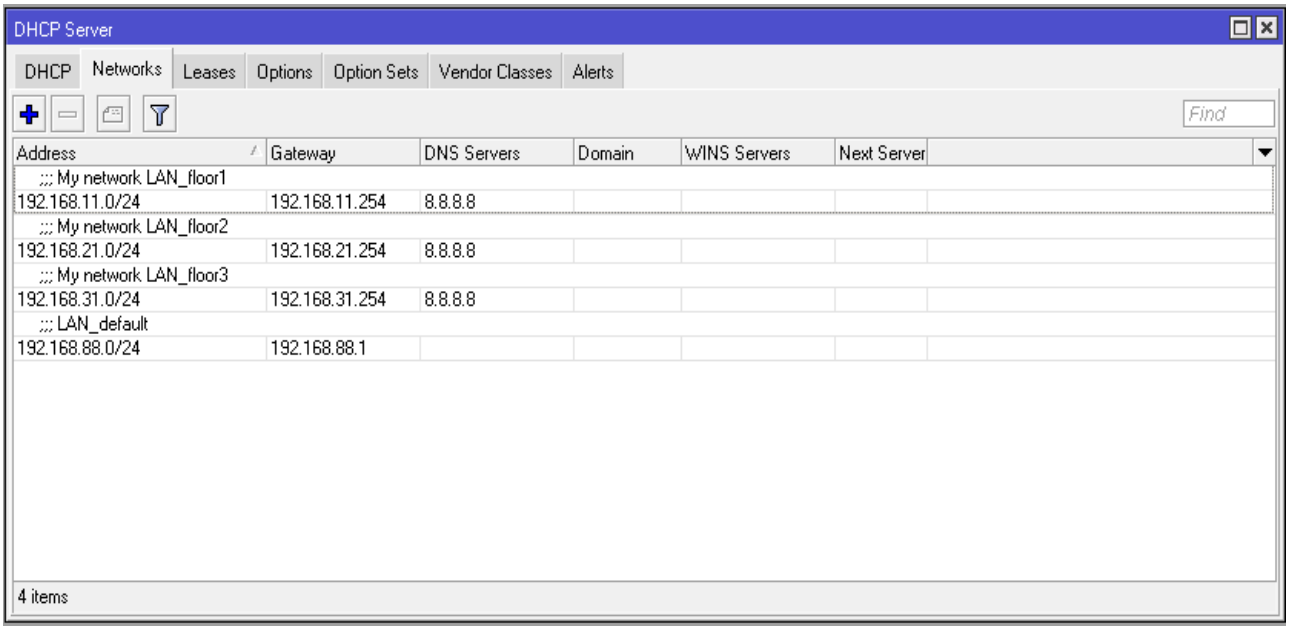

Рисунок 3.16 – Налаштування DHCP-сервера вкладка «Networks»

Результат налаштування та відображення активних з'єднань DHCP-сервера показано на рисунку 3.17.

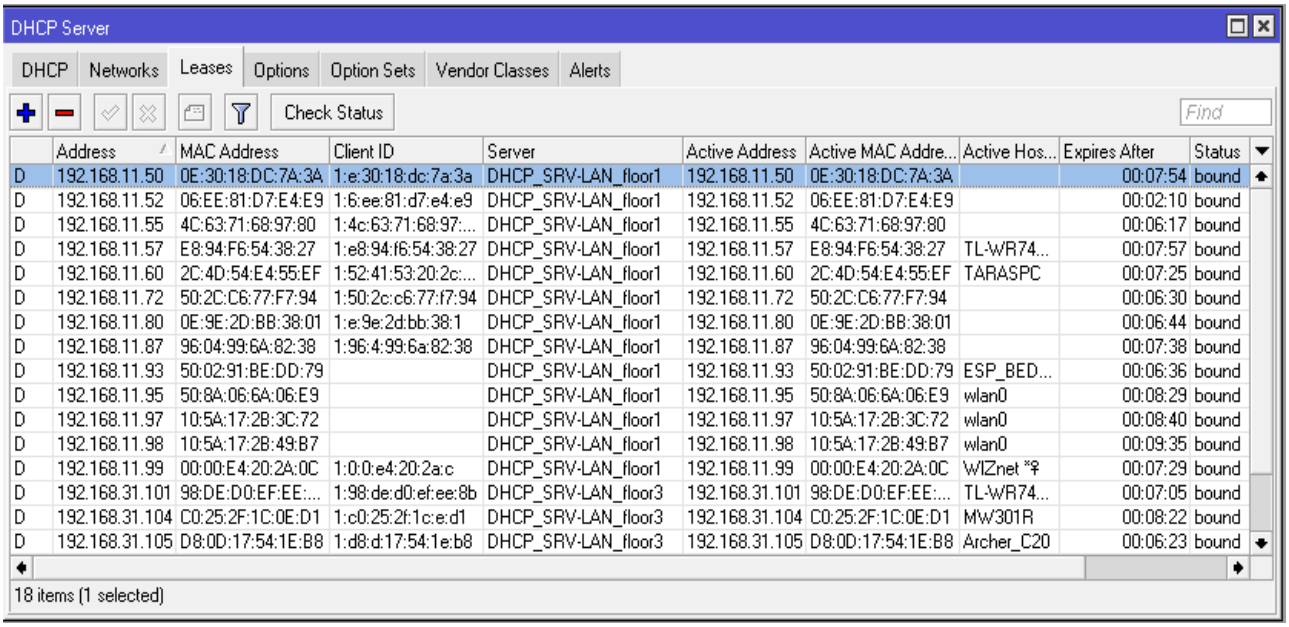

Рисунок 3.17 – Вкладка «Leases»

Для одержання інформації про DHCP клієнтів потрібно обрати відповідне меню у налаштуваннях маршрутизатора, як показано на рисунку 3.18.

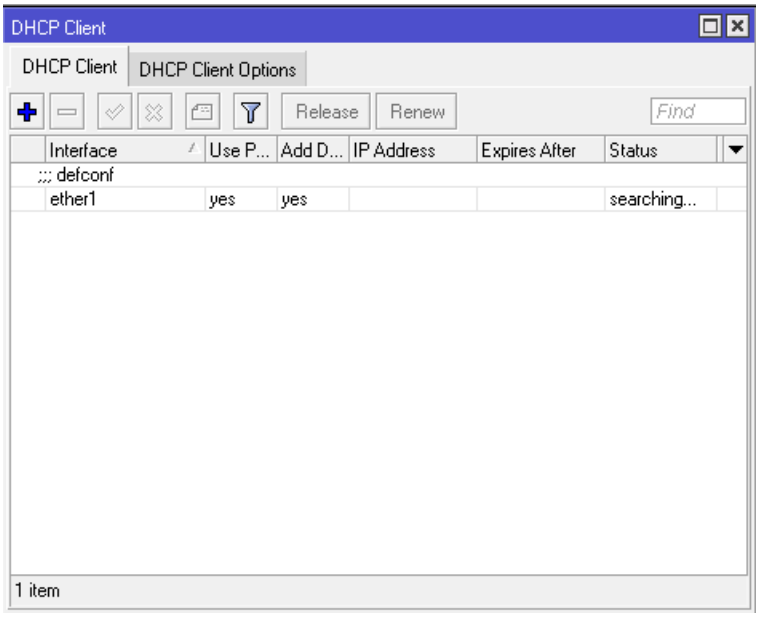

Рисунок 3.18 – Вікно налаштування та відображення інформації про DHCP Client.

Скрипт налаштування DNS показано у лістингу 3.4.

Лістинг 3.4 – Налаштування DNS

```
/ip dhcp-server network
add address=192.168.11.0/24 comment="My network LAN_floor1"
dns-server=\
    8.8.8.8 gateway=192.168.11.254
add address=192.168.21.0/24 comment="My network LAN_floor2"
dns-server=\
    8.8.8.8 gateway=192.168.21.254
add address=192.168.31.0/24 comment="My network LAN_floor3"
dns-server=\
    8.8.8.8 gateway=192.168.31.254
add address=192.168.88.0/24 comment=LAN_default
gateway=192.168.88.1
/ip dns
set allow-remote-requests=yes servers=8.8.8.8,8.8.4.4
/ip dns static
add address=192.168.88.1 comment=defconf name=router.lan
```

Візуальна форма для налаштування DNS показана на рисунку 3.19.

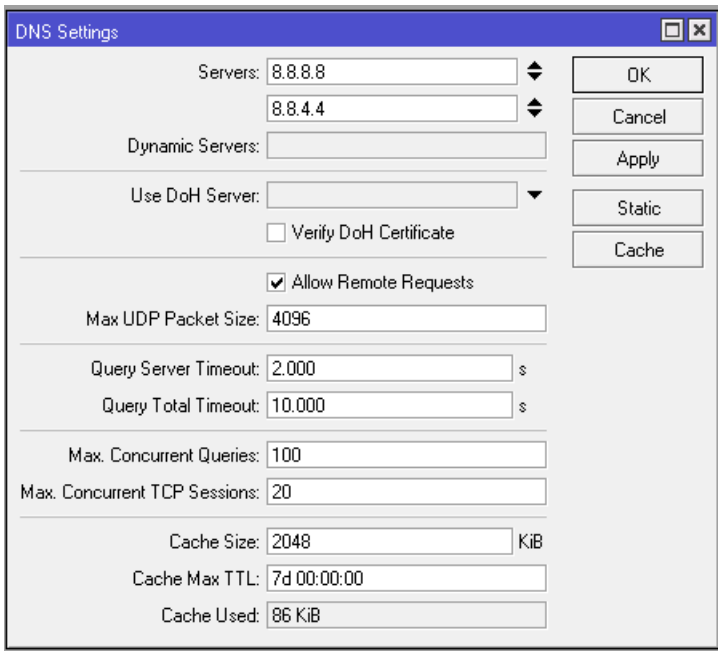

Рисунок 3.19 – Форма налаштування DNS

У результаті виконання таких маніпуляцій налаштовано запропоновану логічну взаємодію між сегментами комп'ютерної мережі та мережевими компонентами.

3.2.2 Налаштування сервісу безпеки

Сервіс безпеки комп'ютерної мережі запропоновано організувати шляхом налаштування FireWall на маршрутизаторі, а також політик безпеки локальних робочих станцій. Оскільки, налаштування безпеки локальних станцій є тривіальною задачею, зосередимо основний акцент на налаштуванні FireWall MikroTik RB750Gr3

Для налаштування правил фільтрації та роботи сервісу безпеки у візуальному режимі використовується вікно, яке показано на рисунку 3.20.

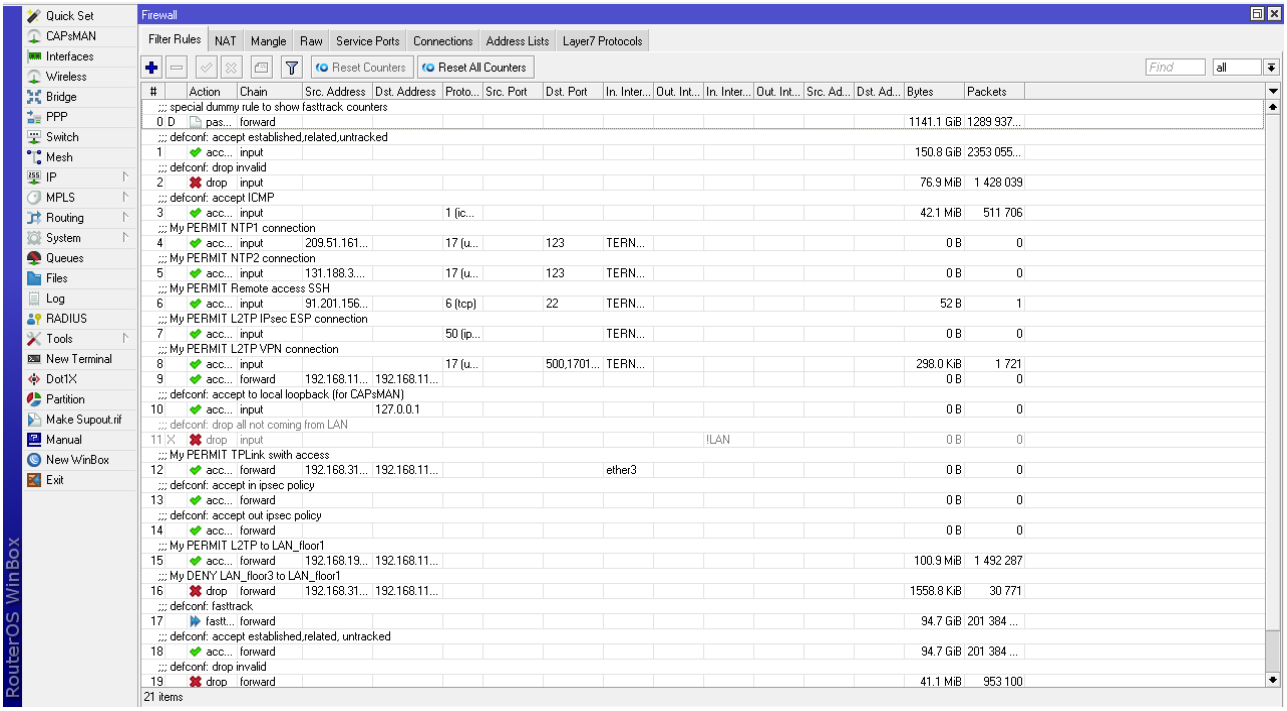

Рисунок 3.20 – Вікно налаштування правил FireWall

Формування правил функціонування FireWall можна задати за допомогою відповідного скрипта з правилами. При налаштуванні сервісу безпеки використано лістинг 3.5, який подано нижче.

Лістинг 3.5 – Скрипт правил фільтрації FireWall

```
/ip firewall filter
add action=accept chain=input comment=\
    "defconf: accept established,related,untracked" connection-
state=\
    established,related,untracked
add action=drop chain=input comment="defconf: drop invalid"
connection-state=\
    invalid
add action=accept chain=input comment="defconf: accept ICMP"
protocol=icmp
add action=accept chain=input comment="My PERMIT NTP1 connection"
dst-port=\
    123 in-interface=TERNET-PPPoE protocol=udp src-
address=209.xx.xxx.xxx
```

```
add action=accept chain=input comment="My PERMIT NTP2
connection" dst-port=\
    123 in-interface=TERNET-PPPoE protocol=udp src-
address=131.xxx.x.xxx
add action=accept chain=input comment="My PERMIT Remote access
SSH" dst-port=\
    22 in-interface=TERNET-PPPoE protocol=tcp src-
address=91.xxx.xxx.x/24
add action=accept chain=input comment="My PERMIT L2TP IPsec ESP
connection" \
    in-interface=TERNET-PPPoE protocol=ipsec-esp
add action=accept chain=input comment="My PERMIT L2TP VPN
connection" \
    dst-port=5xx,17xx,45xx in-interface=TERNET-PPPoE
protocol=udp
add action=accept chain=forward dst-address=192.168.11.0/24 src-
address=\
    192.168.11.0/24
add action=accept chain=input comment=\
    "defconf: accept to local loopback (for CAPsMAN)" dst-
address=127.0.0.1
add action=drop chain=input comment="defconf: drop all not coming
from LAN" \
    disabled=yes in-interface-list=!LAN
add action=accept chain=forward comment="My PERMIT TPLink swith
access" \
    dst-address=192.168.11.0/24 in-interface=ether3 src-
address=\
    192.168.31.250
add action=accept chain=forward comment="defconf: accept in
ipsec policy" \
    ipsec-policy=in,ipsec

add action=accept chain=forward comment="defconf: accept out
ipsec policy" \
    ipsec-policy=out,ipsec
```

```
    dst-address=192.168.11.0/24 src-address=192.168.xx.xx/24
add action=drop chain=forward comment="My DENY LAN_floor3 to
LAN_floor1" \
    dst-address=192.168.11.0/24 src-address=192.168.31.0/24
add action=fasttrack-connection chain=forward comment="defconf:
fasttrack" \
    connection-state=established,related
add action=accept chain=forward comment=\
    "defconf: accept established,related, untracked"
connection-state=\
    established,related,untracked
add action=drop chain=forward comment="defconf: drop invalid" \
    connection-state=invalid
add action=drop chain=forward comment=\
    "defconf: drop all from WAN not DSTNATed" connection-nat-
state=!dstnat \
    connection-state=new disabled=yes out-interface=TERNET-
PPPoE
```

Вікно налаштування NAT FireWall показано на рисунку 3.21, а скрипт опису правил наведено у лістингу 3.6.

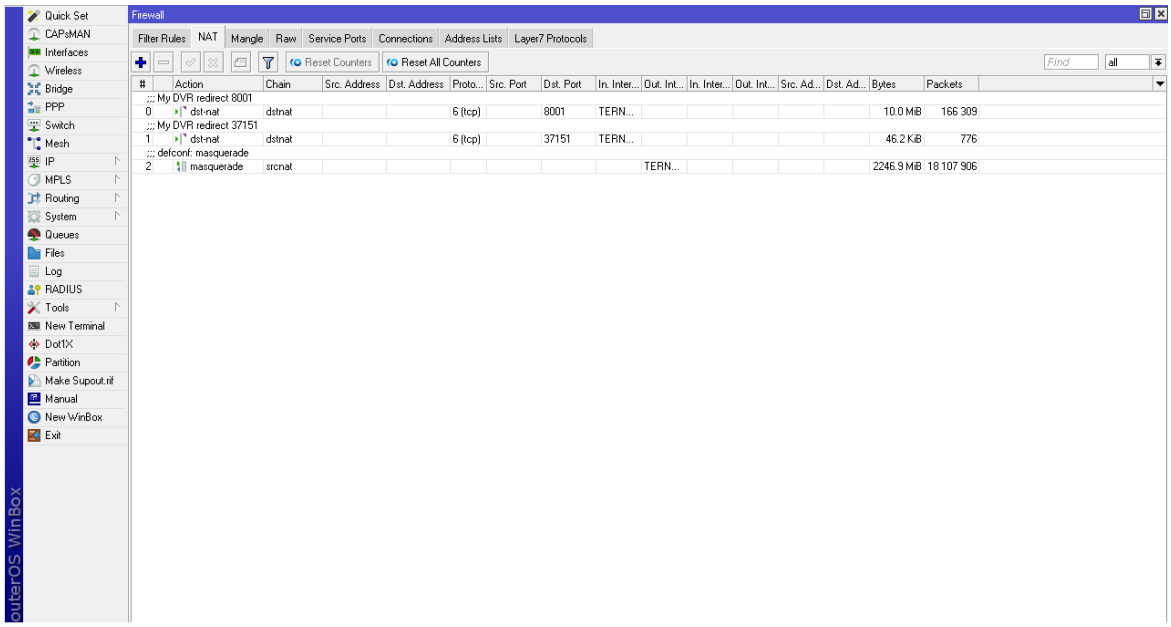

Рисунок 3.21 – Налаштування NAT

Лістинг 3.6 – Налаштування NAT FireWall

```
/ip firewall nat
add action=dst-nat chain=dstnat comment="My DVR redirect 80xx"
dst-port=80xx \
    in-interface=TERNET-PPPoE protocol=tcp to-
addresses=192.168.xx.xxx \
    to-ports=80xx
add action=dst-nat chain=dstnat comment="My DVR redirect 37xxx"
dst-port=\
    37xxx in-interface=TERNET-PPPoE protocol=tcp to-
addresses=192.168.xx.xxx \
    to-ports=37xxx
add action=masquerade chain=srcnat comment="defconf:
masquerade" \
    ipsec-policy=out,none out-interface=TERNET-PPPoE
```

Таким чином забезпечено базові налаштування безпеки у вигляді відповідного сервісу, що функціонує на основі MikroTik. Наступний крок полягає у створенні безпечного сервісу віддаленого доступу до ресурсів управління підприємства. Під ресурсами управління підприємством у даному випадку будемо розуміти віддалений доступ до системи відеоспостерження та управління бухгалтерським обліком на основі 1С: Бухгалтерія.

3.3 Організація безпечного віддаленого доступу до ресурсів управління підприємством

Безпосередню організацію безпечного віддаленого доступу запропоновано реалізувати на основі технологій IPsec та L2TP.

IPSec представляє собою сукупність протоколів, які дозволяють забезпечити захист повідомлень, передача яких виконується на основі IP-протоколу. Дана технологія дає змогу забезпечити і підтвердити справжність, а

також шифрування пакетів. IPsec володіє набором протоколів щодо захисту процесу обміну ключами при використанні мережі Інтернет.

Варто відмітити, що на відміну від широко використовуваних протоколів SSL і TLS, IPsec є більш гнучким за рахунок того, що функціонує на третьому мережевому рівні моделі OSI. Це дозволяє його застосування для забезпечення захищеності будь-яких протоколів, які базовані на TCP та/або UDP.

Функціонування IPsec передбачає виконання наступних функцій:

– «Authentication Header (AH)» – протокол, що орієнтований на забезпечення цілісності віртуальної передачі даних, виявлення та аутентифікацію справжності джерела з яким встановлюється комунікація, а також недопущення повторного передавання пакетів;

– «Encapsulating Security Payload (ESP)» – протокол, який орієнтований на забезпечення конфіденційності передачі даних шляхом шифрування та обмеження такого роду трафіку, а також володіє функціями подібними до AH;

– «Security Association (SA)» – дозволяє забезпечити комплексність і цілісність відповідності алгоритмів і даних, які формують налаштування, що необхідні для ефективного функціонування Authentication Header і/або Encapsulating Security Payload;

– «Internet security association and key management protocol (ISAKMP)» – забезпечує і формує базис аутентифікації та обміну ключами, а також виконує функцію встановлення їх справжності.

«Layer 2 Tunneling Protocol (L2TP)» представляє собою протокол тунелювання другого рівня, що є розширенням іншого протоколу тунелювання «точка-точка» (PPTP). Ці протоколи широко використовуються інтернет-провайдерами для організації функціонування VPN через мережу Інтернет.

L2TP поєднує найкращі функції двох інших протоколів тунелювання: PPTP від Microsoft та L2F від Cisco Systems. Два основних компоненти, які складають L2TP, - це L2TP Access Concentrator, який є пристроєм, що фізично завершує виклик і мережевий сервер L2TP Network Serve (LNS), який є пристроєм, що завершує і, можливо, аутентифікує потік PPP.

На рисунку 3.22 показано принцип організації типової схеми L2TP.

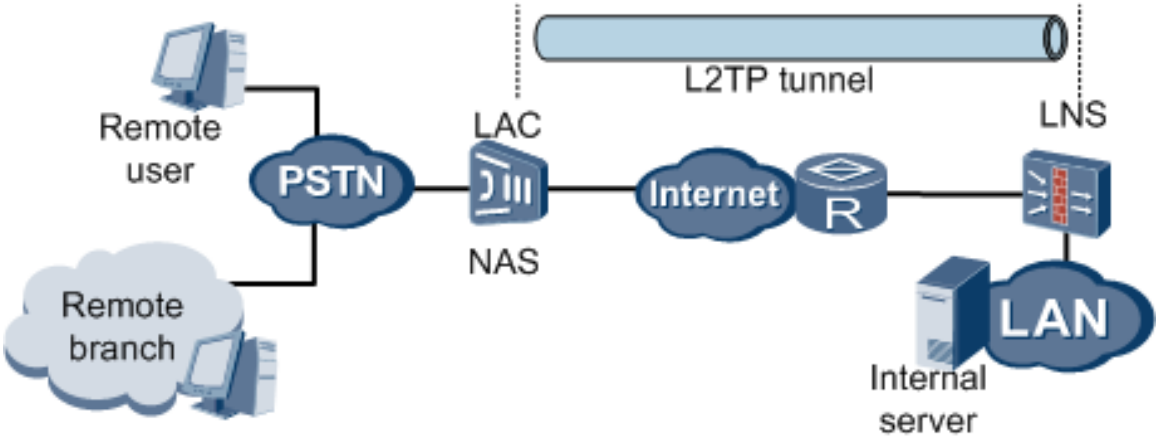

Рисунок 3.22 – Принцип організації VPN на основі L2TP

Опис NAT правила і відповідно реакція на звернення до порту 8001 показано на рисунку 3.23.

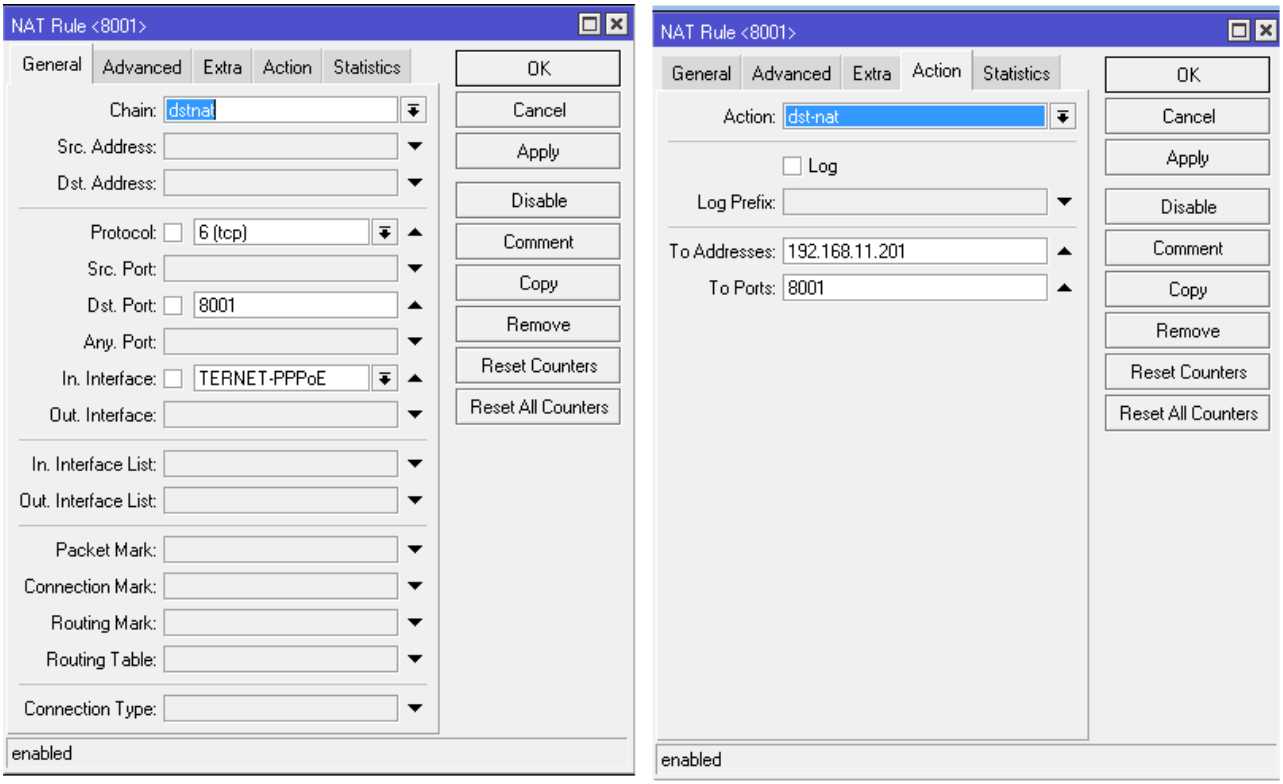

Рисунок 3.23 – Налаштування NAT правил

По аналогії до встановлених параметрів, які показано на рисунку 3.23, виконано налаштування на інший порт для доступу до ресурсів підприємства, що наведено на рис. 3.24.

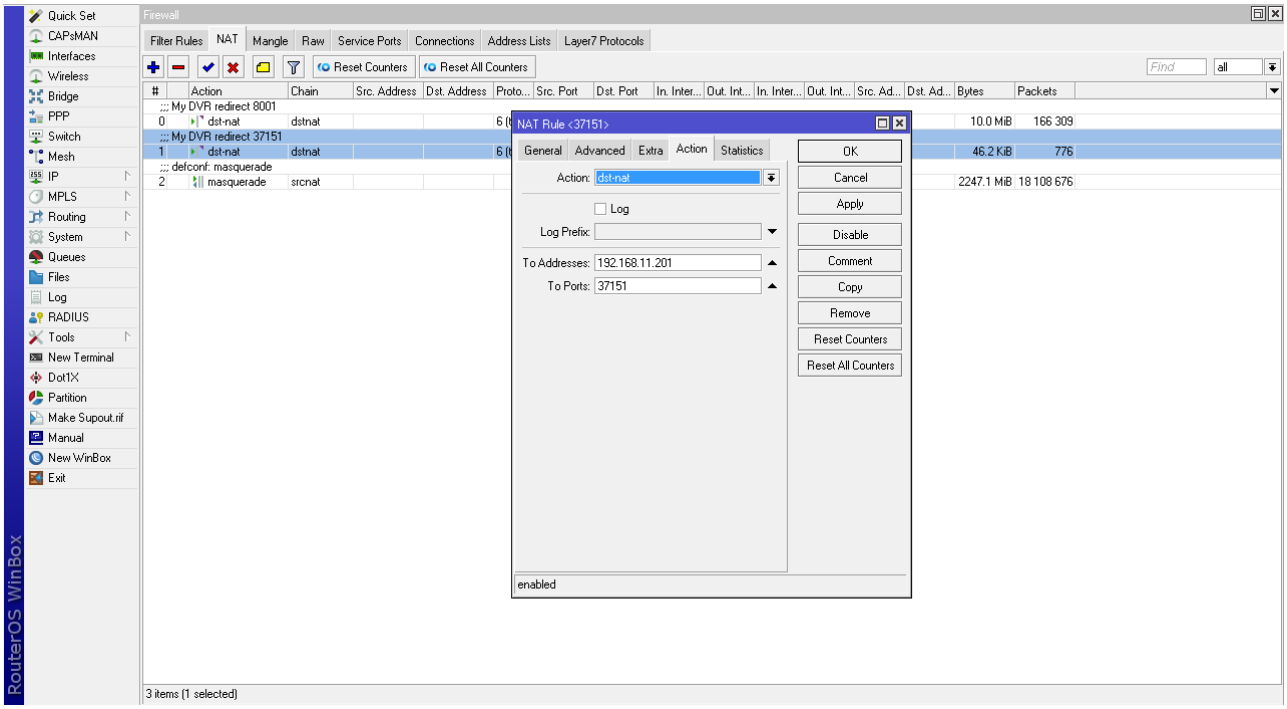

Рисунок 3.24 – Налаштування NAT правил для додаткового порту

У лістингу 3.7 наведено системні параметри для синхронізації дати і часу, що в подальшому дозволить проводити актуальне логування щодо трафіку, який проходить через маршрутизатор.

Лістинг 3.7 – Налаштування системної дати і часу

```
/system clock
set time-zone-name=Europe/Kiev
/system identity
set name=BUoffice
/system ntp client
set enabled=yes primary-ntp=209.51.161.238 secondary-
ntp=131.188.3.220
/tool mac-server
set allowed-interface-list=LAN
/tool mac-server mac-winbox
set allowed-interface-list=LAN
```

Результат роботи налаштованого FireWall показано на рисунку 3.25, а опис взаємодії дозволених пристроїв і технологій передачі даних на основі IPsec показано на рисунку 3.26.

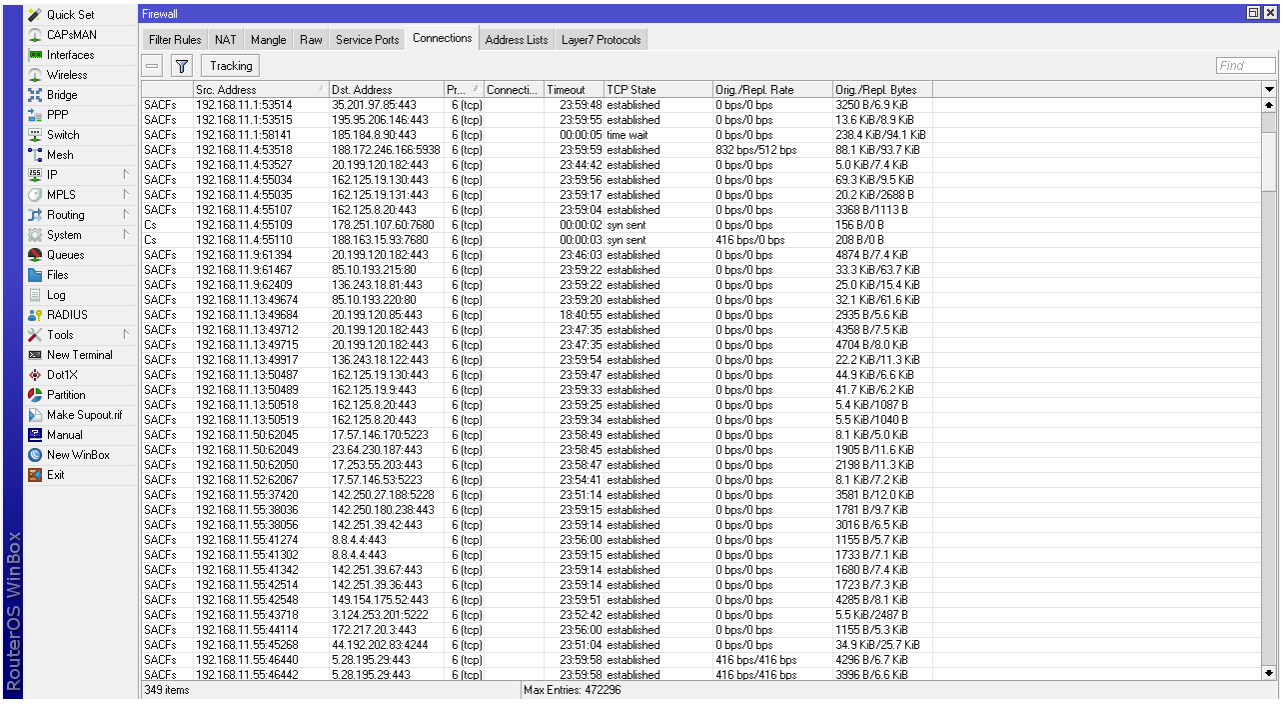

Рисунок 3.25 – Результат функціонування налаштованого FireWall

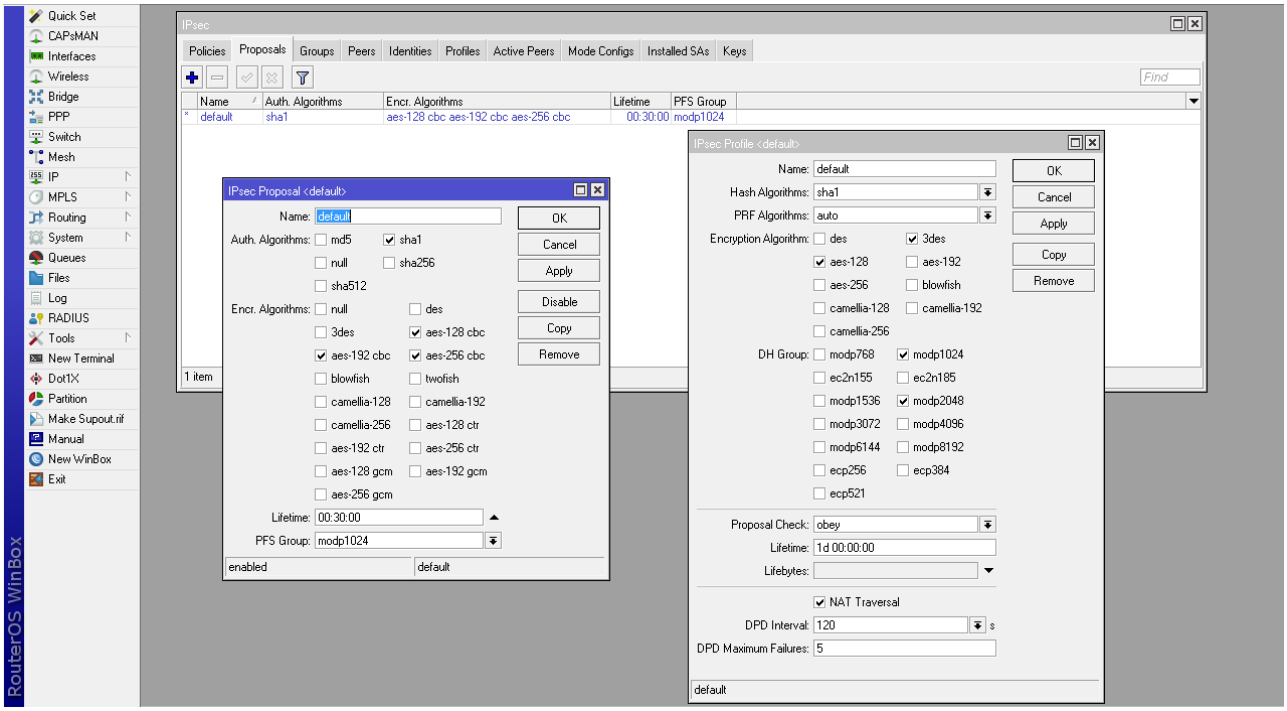

Рисунок 3.26 – Правила функціонування IPsec

У лістингу 3.9 наведено налаштування віддаленого доступу до ресурсів управління підприємством з використанням L2TP.

Лістинг 3.9 – Скрипт налаштування віддаленого доступу на основі L2TP

```
/ppp secret
add comment="L2TP VPN user99" name=test1 password=test_1
profile=\
    L2TP_profile service=l2tp
add comment="L2TP VPN user1" name=test2 password=test_2
profile=\
    L2TP_profile service=l2tp
add comment="L2TP VPN user2" name=test3 password=test_3 \
    profile=L2TP_profile service=l2tp
add comment="L2TP VPN user3 " name=test4 password=\
    test4_4 profile=L2TP_profile service=l2tp
add comment="L2TP VPN user4 " name=test5 password=\
    test_5 profile=L2TP_profile service=l2tp
```

У результаті впровадження налаштування сервісів безпеки та віддаленого доступу до ресурсів управління підприємством одержано логи, які показують доступність до мережі визначених груп користувачів та блокування сторонніх з'єднань, що показано на рисунках 3.27-3.28.

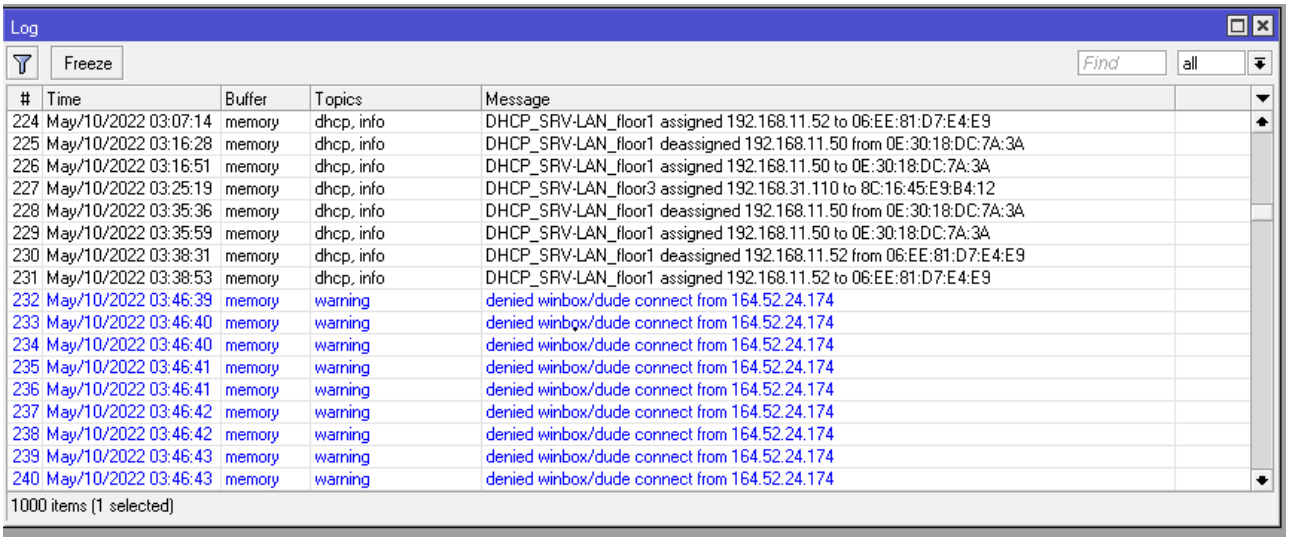

Рисунок 3.27 – Лог зверень з локальної мережі

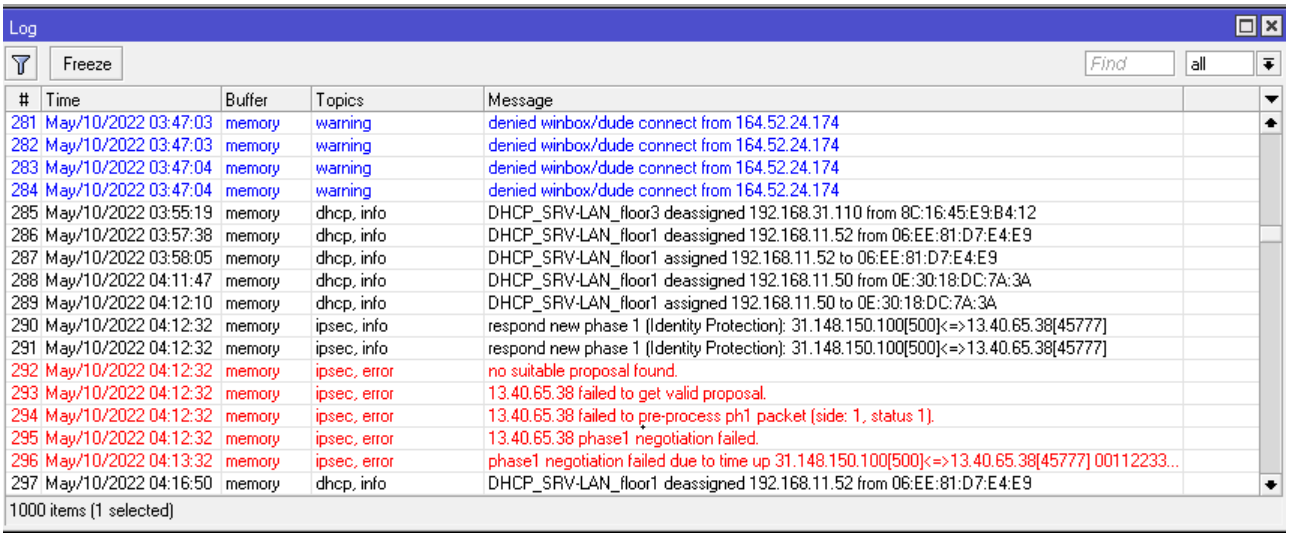

Рисунок 3.28 – Спроби з’єднання з мережею через віддалений доступ

Таким чином, у результаті проведених налаштувань організовано сервіси безпеки та віддаленого доступу до ресурсів управління підприємством, що показує ефективність застосування методів IPsec та L2TP.

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Організація служби охорони праці на підприємстві

Роботодавець зобов'язаний згідно Закону України «Про охорону праці» стаття 13 «Управління охороною праці та обов’язки роботодавця» створити на робочому місці в кожному структурному підрозділі умови праці відповідно до нормативно-правових актів, а також забезпечити додержання вимог законодавства щодо прав працівників у галузі охорони праці.

Із цією метою роботодавець забезпечує функціонування системи управління охороною праці, а саме:

– створює відповідні служби і призначає посадових осіб, які забезпечують вирішення конкретних питань охорони праці, затверджує інструкції про їхні обов'язки, права та відповідальність за виконання покладених на них функцій, а також контролює їх додержання;

– розробляє за участю сторін колективного договору і реалізує комплексні заходи для досягнення встановлених нормативів та підвищення існуючого рівня охорони праці;

– забезпечує виконання необхідних профілактичних заходів відповідно до обставин, що змінюються;

– впроваджує прогресивні технології, досягнення науки і техніки, засоби механізації та автоматизації виробництва, вимоги ергономіки, позитивний досвід з охорони праці тощо;

– забезпечує належне утримання будівель та споруд, виробничого обладнання та устаткування, моніторинг за їх технічним станом;

– забезпечує усунення причин, що призводять до нещасних випадків, професійних захворювань, та здійснення профілактичних заходів, визначених

комісіями за підсумками розслідування цих причин;

– організовує проведення аудиту охорони праці, лабораторних досліджень умов праці, оцінку технічного стану виробничого обладнання та устаткування, атестацій робочих місць на відповідність нормативно-правовим актам з охорони праці в порядку і строки, що визначаються законодавством, та за їх підсумками вживає заходів з усунення небезпечних і шкідливих для здоров'я виробничих факторів;

– розробляє і затверджує положення, інструкції, інші акти з охорони праці, що діють у межах підприємства та встановлюють правила виконання робіт і поведінки працівників на території підприємства, у виробничих приміщеннях, на будівельних майданчиках, робочих місцях відповідно до нормативно-правових актів з охорони праці, забезпечує безоплатно працівників нормативно-правовими актами підприємства з охорони праці;

– здійснює контроль за додержанням працівником технологічних процесів, правил поведінки з машинами, механізмами, устаткуванням та іншими засобами виробництва, використанням засобів колективного та індивідуального захисту, виконанням робіт відповідно до вимог з охорони праці;

– організовує пропаганду безпечних методів праці та співробітництво з працівниками у галузі охорони праці.

Роботодавець несе безпосередню відповідальність за порушення нормативно-правових актів з охорони праці. Служба охорони праці створюється роботодавцем на підприємстві з кількістю працівників 50 і більше. На підприємстві з кількістю працівників менше 50 осіб функції цієї служби можуть виконувати у порядку сумісництва особи, що пройшли перевірку знань з охорони праці відповідними державними службами. Якщо кількість працівників менше 20 осіб, для виконання функцій служби охорони праці можуть залучатися сторонні спеціалісти на договірних засадах. Служба охорони праці підпорядковується безпосередньо роботодавцю і прирівнюється до керівників і спеціалістів основних виробничо-технічних служб.

Спеціалісти служби охорони праці у разі виявлення порушень охорони праці мають право:

– видавати керівникам структурних підрозділів підприємства обов'язкові для виконання приписи щодо усунення наявних недоліків, одержувати від них необхідні відомості, документацію і пояснення з питань охорони праці;

– вимагати відсторонення від роботи осіб, які не пройшли передбачених законодавством медичного огляду, навчання, інструктажу, перевірки знань і не мають допуску до відповідних робіт або не виконують вимог нормативно-правових актів з охорони праці;

– зупиняти роботу виробництва, дільниці, машин, механізмів, устаткування та інших засобів виробництва у разі порушень, які створюють загрозу життю або здоров'ю працівників;

– надсилати роботодавцю подання про притягнення до відповідальності працівників, які порушують вимоги щодо охорони праці.

Ліквідація служби охорони праці допускається тільки у разі ліквідації підприємства чи припинення використання найманої праці фізичною особою.

Законодавство про охорону праці передбачає і обов'язки працівників. Зокрема вони зобов'язані:

– дбати про особисту безпеку і здоров'я, а також про безпеку і здоров'я оточуючих людей у процесі виконання будь-яких робіт під час перебування на території підприємства;

– знати і виконувати вимоги нормативно-правових актів з охорони праці, правила поведінки з машинами, механізмами, устаткуванням та іншими засобами виробництва, користуватися засобами колективного та індивідуального захисту;

– проходити у встановленому законодавством порядку попередні та періодичні медичні огляди.

Працівник несе безпосередню відповідальність за порушення зазначених вимог. Дотримання правил безпеки і виробничої санітарії залежить не тільки

від виконання роботодавцем своїх обов'язків, а й від того, наскільки кожен працівник знає і виконує правила під час роботи. Тому всі працівники при прийомі на роботу і в процесі роботи проходять на підприємстві інструктаж з охорони праці, надання першої медичної допомоги потерпілим від нещасних випадків, правил поведінки при виникненні аварій.

Навчання й інструктаж працівників з охорони праці є складовою частиною системи управління охороною праці і проводиться з усіма працівниками в процесі їхньої трудової діяльності. Інструктаж працівників залежно від характеру та часу його проведення буває вступний (при прийомі на роботу); первинний (на робочому місці з усіма працівниками: на роботах із підвищеною небезпекою - один раз на квартал, на інших роботах — один раз на півроку; проводиться або індивідуально, або з групою працівників, що виконують однотипні роботи, за програмою первинного інструктажу); позаплановий (при зміні правил з охорони праці, заміні устаткування чи за інших змін факторів, що впливають на безпеку праці); цільовий (при виконанні разових робіт, не пов'язаних із прямими обов'язками за фахом).

Навчання та інструктаж працівників з охорони праці проводиться у відповідності до Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці від 26.012005 р. № 15 – НПАОП 0.00.4.36 – 05.

4.2 Заходи, які забезпечують створення оптимальних метеорологічних умов у приміщеннях з використанням ПК

Метеорологічні умови визначаються такими параметрами:

– температурою повітря, t (С);
– відносною вологістю, ф (%);
– швидкістю повітря, v ($^{м}/_{с}$).

Крім цих параметрів, що є основними, не слід забувати і про атмосферний тиск (Р, Па), який впливає не тільки на парціальний тиск основних компонентів повітря (кисень та азот), а й на процес дихання.

Життєдіяльність людини проходить в умовах достатньо широкого діапазону тиску 734—1276 гПа. Однак тут треба пам'ятати, що для здоров'я людини є небезпечною швидка зміна тиску, а не сама величина цього тиску. Наприклад, швидке зниження тиску лише на декілька гектопаскалей щодо нормальної величини 1013 гПа спричиняє хворобливі відчуття.

Необхідність урахування основних параметрів метеорологічних умов диктується наслідками в змінах стану людини. Особливо переконливо це можна пояснити під час розглядання теплового балансу між організмом людини і навколишнім середовищем.

Величина тепловиділення (Q) організмом людини залежить від ступеня фізичного напруження у певних метеорологічних умовах і складає від 85 (у стані спокою) до 500 Дж/с (тяжка робота).

Людина постійно перебуває в процесі теплової взаємодії з навколишнім середовищем. Для того, щоб фізіологічні процеси проходили нормально, теплота, що виділяє організм, повинна віддаватись в навколишнє середовище. Співвідношення між кількістю цієї теплоти йохолоджувальною здатністю середовища характеризує умови як комфортні. В умовах комфорту у людини не виникає турбот щодо її температурних відчуттів охолодження чи перегрівання.

Віддача теплоти організмом людини в навколишнє середовище відбувається через теплопровідність крізь одяг (Q_T), конвекцією тіла (Q_K), випромінюванням на навколишні поверхні (Q_B), випаровуванням вологи з поверхні шкіри (Q_{BIffl}). Частина теплоти витрачається на нагрівання повітря, яким дихає людина (Q_r).

Кількість теплоти, яка віддається організмом людини будь-якими шляхами, залежить від того чи іншого параметра мікроклімату. Так, тепловіддача конвекцією залежить від температури навколишнього повітря і швидкості його переміщення. Випромінювання теплоти відбувається у напрямі поверхонь, що оточують людину, мають нижчу температуру поверхні одягу (27—31 °С) і відкритих частин тіла людини (близько 33,4 °С). Під час впливу високих температур навколишньої поверхні (ЗО—35 °С) тепловіддача випромінюванням повністю відсутня, а під час впливу більш високих

температур теплообіг йде у зворотному напрямі — від поверхні до людини. Віддача теплоти за рахунок випаровування залежить від відносної вологості і швидкості переміщення повітря. У стані спокою, коли температура навколишнього середовища 18°С, частка Q_K складає близько ЗО % всієї теплоти, яка віддається людиною, Q_{BIin} = 20 % і Q_n ~ 5 %.

Під час зміни температури повітря, швидкості його руху і вологості, наявності близько людини нагрітої поверхні, в умовах її фізичної праці тощо — це співвідношення змінюється.

Нормальне теплове самопочуття (комфортні умови), відповідно до конкретних видів роботи, забезпечується при дотриманні теплового балансу: $Q = Q_T + Q_K + Q_{Bim} + Q_n$> тому температура внутрішніх органів людини залишається постійною (близько 36,6°С). Ця здатність людського організму до утримання постійної температури під час зміни параметрів мікроклімату та під час виконання роботи будь-якої важкості називається *терморегуляцією.*

Висока температура впливає на людину і сприяє розширенню судин кровообігу. Відповідно має місце підвищений приплив крові до поверхні тіла, і тепловіддача в навколишнє середовище значно підвищується. Однак, коли температура навколишнього середовища і поверхні досягає 30—35°С, віддача теплоти конвекцією і випромінюванням в основному припиняється. Більш висока температура повітря сприяє тому, що більша частина теплоти віддається через випаровування її з поверхні шкіри. В таких умовах організм губить відповідну кількість вологи, а разом з нею і солі, які відіграють важливу роль в життєдіяльності організму.

В умовах зниження температури повітря реакція людського організму на ці зміни інша — судини кровообігу шкіри звужуються, приплив крові до поверхні тіла зменшується, і віддача теплоти конвекцією і випромінюванням зменшується. Таким чином, для теплового самопочуття людини важливим є певне сполучення температури, відносної вологості і швидкості руху повітря.

Вологість повітря значною мірою впливає на терморегулювання організму. Підвищена вологість (ф > 85 %) ускладнює терморегулювання через зниження випару поту, а досить низька вологість (ф < 20 %) спричиняє сухоту

слизових оболонок шляхів дихання. Оптимальні величини відносної вологості складають 40 — 60 %.

Рух повітря в приміщеннях є важливим чинником, який впливає на теплове самопочуття людини. В умовах спекоти рух повітря сприяє підвищенню віддачі теплоти організмом і поліпшує його стан, але в холодну пору року цей вплив не є сприятливим.

Мінімальна швидкість руху повітря, яку відчуває людина, складає 0,2 м/с. Взимку швидкість руху повітря не повинна перевищувати 0,2—0,5 м/с, а влітку 0,2—1,0 м/с.

Швидкість повітря також впливає на розподіл шкідливих речовин у приміщенні. Повітряні потоки можуть розповсюджувати їх по всьому об'єму приміщення, переводити пил з осілого у зважений стан.

Під впливом високої температури повітря, інтенсивного теплового випромінювання виникає загроза перегрівання організму людини, яке характеризується підвищенням температури тіла, рясним потовиділенням, прискореним пульсом і диханням, різкою слабкістю, запамороченням, а в тяжких випадках — появою судом і виникненням теплового удару.

ВИСНОВКИ

У даній кваліфікаційній роботі на здобуття освітнього ступеня бакалавра спроектовано комп'ютерну мережу підприємства, що знаходиться у трьохповерховій будівлі. На основі технологій IPsec та L2TP організовано сервіси безпечного віддаленого доступу та налаштовано параметри FireWall.

При налаштуванні параметрів безпеки встановлено групи користувачів та визначено дозволи щодо використання ресурсів підприємства, зокрема, в контексті віддаленого доступу до системи відеоспостереження та фінансової звітності й обліку підприємства.

Налаштування сервісів безпеки та віддаленого доступу виконано на основі MikroTik hEX (RB750Gr3), повністю налаштовано його FireWall, реалізовано запропоновані рішення щодо сегментації локальної комп'ютерної мережі та логічної топології.

В якості комутаторів використано комутатори другого рівня, зокрема один TL-SL5428E і два HP ProCurve 1700 – 24, які розташовано у стійках 19". Кабельна інфраструктура побудована на основі вимог і рекомендацій стандартів структурованих кабельних систем

У роботі також розроблено IP-адресну схему, яка передбачає сегментацію мережі на три логічні VLAN та схему з'єднань від інформаційних розеток до патч-панелей, а від патч-панелей до комутаторів. Це дозволило забезпечити гнучкість обслуговування та монтажу компонентів комп'ютерної мережі і підвищити ефективність її функціонування.

Організація проекту комп'ютерної мережі з сервісами безпеки та віддаленого доступу до ресурсів управління підприємством є відтестованою, працездатною та ефективною, що підтверджено відповідними лог-файлами, де можна побачити дозволені визначеними правилами з'єднання, а також з'єднання, які не пройшли відповідну аутентифікацію за IPsec або L2TP.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Городецька О. Комп’ютерні мережі. Навчальний посібник / О. С. Городецька, В. А, Гикавий, О. В. Онищук – Вінниця: ВНТУ, 2015. – 128 с.

2. Комп’ютерні мережі : навчальний посібник / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. – Львів : «Магнолія 2006», 2013. – 256 с.

3. Мельник І. Проектування та дослідження комп'ютерних мереж / І. Мельник, А. Лунтовський. – К. : Університет «Україна», 2010. – 362 с.

4. Ткаченко В. Комп’ютерні мережі та телекомунікації: навч. посіб. / В. А. Ткаченко, О. В. Касілов, В. А. Рябик – Харків: НТУ “КПІ”, 2011. – 224 с.

5. Семёнов А.В. Структурированные кабельные системы / Семенов А.Б, Стрижаков С.К, Сунчелей И.Р. // 1999Ворона В. А., Тихонов В. А. Системы контроля и управления доступом. М.: Горячая линияТелеком. 2010. 272 с

6. Царьов Р. Ю. Структуровані кабельні системи : навч. посіб. для студентів вищих навчальних закладів / Р. Ю. Царьов, Л. А. Нікітюк, П. І. Резніченко. – Одеса : ОНАЗ ім. О.С. Попова, 2013. – 260 с.

7. Уэнделл О. Официальное руководство Cisco по подготовке к сертификационным екзаменам CCENT/CCNA ICND1 100-101, акад. изд. / О. Уэнделл : Пер. с англ. – М.: ООО «И.Д. Вильямс», 2015. – 912 с.

8. Хилл Б. Полный справочник по Cisco / Б. Хилл : Пер. с англ. – М.: ООО «И.Д. Вильямс», 2004. – 772 с.

9. Медные компоненты СКС, Кабель витая пара, патч-корды, патч-панели, модули, розетки СКС. Цена, описание [Електронний ресурс]. – Режим доступу: URL: http://sklad.scs.ua/copper-components/ – Назва з екрану.

10. Бесекерский В.А. Руководство по проектированию систем автоматического управления. Москва.: Высшая школа, 2007. 295с.

11. Кузин Л.Т. Расчет и проектирование дискретных систем управления.- М.: ГН ТИМЛ, 2012.- 648 с.

12. Жидецький В.Ц. Охорона праці користувачів комп’ютерів. Львів: Афіша, 2000. 176 с.

13. НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями»/Міністерство соціальної політики України. Офіц. вид. К. : Парлам. вид-во, 2018. 24 с.

14. Желібо Є., Заверуха Н., Зацарний В. Безпека життєдіяльності. К.: 2001. 483 с.

Додаток А.

Технічне завдання

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії

Кафедра комп'ютерних систем та мереж

"Затверджую"

Завідувач кафедри КС

_____ Осухівська Г.М.

"___" _____2022 р

СЕРВІСИ БЕЗПЕКИ ТА ВІДДАЛЕНОГО ДОСТУПУ ДО РЕСУРСІВ СИСТЕМИ УПРАВЛІННЯ ПІДПРИЄМСТВОМ

ТЕХНІЧНЕ ЗАВДАННЯ

на _*10*_ листках

Вид робіт: Кваліфікаційна робота

На здобуття освітнього ступеня «Бакалавр»

Спеціальність 123 «Комп'ютерна інженерія»

«УЗГОДЖЕНО»	«ВИКОНАВЕЦЬ»
Керівник кваліфікаційної роботи	Студент групи СІс-43
_____ к.т.н., доц. Яцишин В.В.	_____ Іваночко Н.А.
«____» _____ 2022 р.	«____» _____ 2022 р.

Тернопіль 2022

1 Загальні відомості

1.1 Повна назва та її умовне позначення

Повна назва теми кваліфікаційної роботи: «Сервіси безпеки та віддаленого доступу до ресурсів системи управління підприємством».

Умовне позначення кваліфікаційної роботи: КС КРБ 123.215.00.00

1.2 Виконавець

Студент групи СІс-44, факультету комп’ютерно-інформаційних систем і програмної інженерії, кафедри комп’ютерних систем та мереж, Тернопільського національного технічного університету імені Івана Пулюя, Іваночко Назар Андрійович.

1.3 Підстава для виконання роботи

Підставою для виконання кваліфікаційної роботи є наказ по університету (№ 4.7-180 від 23.03.2022 р.)

1.4 Планові терміни початку та завершення роботи

Плановий термін початку виконання кваліфікаційної роботи – 23.03.2022 р.

Плановий термін завершення виконання кваліфікаційної роботи – 22.06.2022 р.

1.5 Порядок оформлення та пред’явлення результатів роботи

Порядок оформлення пояснювальної записки та графічного матеріалу здійснюється у відповідності до чинних норм та правил ІСО, ГОСТ, ЕСКД, ЕСПД та ДСТУ.

Пред’явлення проміжних результатів роботи з виконання кваліфікаційної роботи здійснюється у відповідності до графіку, затвердженого керівником роботи.

Попередній захист кваліфікаційної роботи відбувається при готовності роботи на 90% , наявності пояснювальної записки та графічного матеріалу.

Пред’явлення результатів кваліфікаційної роботи відбувається шляхом захисту на відповідному засіданні ЕК, ілюстрацією основних досягнень за допомогою графічного матеріалу.

2 Призначення і цілі створення системи

2.1 Призначення системи

Сервіси безпеки та віддаленого доступу до ресурсів системи управління підприємством функціонують на основі комунікаційної складової інформаційної системи підприємства. Основне призначення таких сервісів полягає у забезпеченні захисту та авторизованого доступу до наявних інформаційних ресурсів, а також забезпечення віддаленого доступу до бухгалтерських документів і звітності, доступу до камер відеоспостереження, які наявні на підприємстві.

Такі сервіси повинні забезпечувати логічну і фізичну стійкість при доступі до ресурсів, а також забезпечувати локальний авторизований доступ до програмного та інформаційного забезпечення. Наявність сервісів безпеки та віддаленого доступу повинні сприяти підвищенню ефективності функціонування підприємства, запобігти витокам інформації, а також чітко розподілити права і ролі користувачів при опрацюванні даних та забезпечити захист інформації.

2.2 Мета створення системи

Мета реалізації та налаштування сервісів безпеки та віддаленого доступу до інформаційних ресурсів управління підприємством полягає у підвищенні безпекового і захисного потенціалу при автоматизації бізнес-процесів фірми, а також забезпечення гнучкості і доступу з віддаленого географічного розташування визначених груп користувачів.

До переліку основних задач, які повинні реалізовувати сервіси безпеки та віддаленого доступу належать:

– автоматизація процесу аутентифікованого доступу до ресурсів управління підприємством;

– здатність налаштування дозволів для визначених груп користувачів;

– здатність логувати та зберігати інформацію про доступ до ресурсів управління підприємством з фіксацією дати і часу;

– можливість аналізу логів звернення до інформаційних ресурсів;

– можливість визначення групи IP-адрес в межах пісочниці інтернет-провайдера;

– можливість трансляції відеопотоку із встановлених відеокамер;

– забезпечення можливості управління інформаційними та відеопотоками;

– здатність захищеного входу/виходу користувачів з локальної мережі в інтернет-простір;

– здатність до взаємодії з довіреними зовнішніми програмними та інформаційними ресурсами;

– забезпечення віддаленого доступу з використанням двохфакторної авторизації користувачів.

2.3 Характеристика об'єкту

2.3.1 Основні задачі та функції об’єкту

Найбільш важливими функціями і задачами, які покликані розв’язати сервіси безпеки і віддаленого доступу до інформаційних ресурсів є здатність гнучко та надійно проводити аутентифікацію користувачів, надавати можливість віддаленого використання інформаційних ресурсів та ресурсів управління бухгалтерським обліком підприємства, а також організації доступу до комунікаційної частини інфраструктури в контексті відеоспостереження.

Реалізація таких сервісів дозволить адміністратору проводити моніторинг використання інформаційних ресурсів, фіксувати дату і час їхньої зміни, а також проводити додаткові заходи щодо підвищення ефективності процесів кіберзахисту із застосування сучасних технологій, зокрема штучного інтелекту, в контексті розпізнавання шахраїв.

Досягнення цілі щодо реалізації сервісів безпеки та віддаленого доступу передбачає виконання ряду задач. Серед найбільш важливих серед них є аналіз існуючої комунікаційної інфраструктури, визначення груп користувачів з відповідними правами і дозволами доступу до ресурсів, проектування фізичної і логічної топологій комп’ютерної мережі та системи відеоспостереження, налаштування параметрів доступу до мережі Інтернет, обміну даними у локальній комп’ютерній мережі.

Важливою задачею також є організація віртуальних мереж, що дозволяють відобразити концептуально подібні групи користувачів. Це забезпечує можливість спільно, в авторизованому режимі, використовувати інформаційні ресурси.

Безпека у комп’ютерній мережі передбачає налаштування на логічному та фізичному рівні засобів авторизованого доступу за різними рівнями. Система логування дозволяє проводити аналіз даних щодо використання інформації користувачами, віддалений доступ до інформації управління підприємством, зокрема, 1С Бухгалтерія.

3 Вимоги до системи

3.1 Вимоги до системи в цілому

Сервіси безпеки та віддаленого доступу до ресурсів управління підприємства, що функціонують на основі комунікаційної складової інформаційної системи повинні забезпечувати доступ до інформації в межах окремого структурного підрозділу та підприємства в цілому на основі визначених прав доступу і дозволів. Доступ до ресурсів повинен бути авторизованим, захищеним та безперебійним. Кожен користувач системи, в залежності від типу прав, повинен мати доступ до глобальної мережі Internet. Середовище передачі даних має забезпечувати швидкодію на рівні не менше, ніж 100 Мб/с.

3.1.1 Вимоги до структури та функціонування системи

Структура комп’ютерної мережі та відповідних сервісів безпеки і віддаленого доступу до ресурсів системи включає в себе:

– структуру об’єднання комп’ютерів в межах кожного окремого відділу, що включає в себе:

- інженерно-технічний відділ – 4 комп’ютери;
- аналітичний відділ – 2 комп’ютери;
- адміністративний підрозділ – 4 комп’ютери;
- сукупність робочих місць в орендованих приміщеннях – 15 комп’ютерів;
- комутаційна кімната – 1 комп’ютерів;
- відділ кадрів – 3 комп’ютери

– структуру засобів та зв’язків при організації доступу до Internet;

– організацію суміжного зв’язку між структурними підрозділами підприємства;

В загальному випадку, логічна структура мережі повинна відображати логічний зв’язок взаємодії підрозділів підприємства та схему організації доступу до мережі Internet.

Функціональні вимоги:

- надійність всіх вузлів комп’ютерної мережі;
- швидкість передачі даних 100 Мб/с;
- безперебійний обмін даними протягом встановленого терміну часу;
- захищеність від неавторизованого доступу (фізичного, логічного);
- зручність монтажу та модернізації;
- часова ефективність в межах 2 с.;
- масштабованість в межах 6 робочих місць.

3.1.2 Вимоги до способів та засобів зв’язку між компонентами системи

Зв’язок між компонентами локальної комп’ютерної мережі базується на використанні кабельних систем та безпровідного середовища передачі даних. Налаштування параметрів мережі здійснюється на рівні операційних систем та програмного забезпечення активного комутаційного обладнання. Засобами зв’язку між комп’ютерами виступають мережеві плати та комутатори.

3.1.3 Вимоги по діагностуванню системи

Діагностування комп’ютерної мережі з відповідними сервісами безпеки та віддаленого доступу до ресурсів управління підприємством відбувається у відповідності до графіку обслуговування. Режими функціонування системи бувають двох видів: в межах норми та аварійні. Вимоги до режимів функціонування в межах норми, передбачають безперебійну роботу всіх вузлів та компонентів локальної мережі з максимальною ефективністю. Вимоги щодо режимів аварійного функціонування включають в себе часткову втрату швидкодії, або перехід на резервне функціонування.

3.1.4 Перспективи розвитку, модернізація системи

Передбачаються перспективи розвитку системи, що включають перехід на інше середовище передачі даних та масштабованість.

3.1.5 Вимоги до надійності системи

Комп’ютерна мережа з сервісами безпеки та віддаленого доступу повинна бути захищена від фізичних чи механічних пошкоджень на рівні апаратного забезпечення, шляхом обмеження доступу до коробів (кабельних), комутаційних розеток, комутаторів, комутаційних шаф і т.д.

Розподілена комп’ютерна мережа повинна бути захищена і на рівні програмного забезпечення.

Надійність системи повинна забезпечувати відновлюваність функціонування у випадку збою апаратного чи програмного забезпечення.

3.1.6 Вимоги до функцій та задач, які виконує система

Вимоги до функцій та задач, які виконує система, передбачають:

– кероване управління інформаційними ресурсами;
– організацію доступу до мережі Internet;
– забезпечення авторизованого доступу на програмному рівні до мережі;
– забезпечення контролю над мережею;
– забезпечення швидкодії 100 Мб/с всередині локальної комп’ютерної мережі та вхідного інтернет-трафіку – 40 Мб/с;
– відповідність стандартам побудови комп’ютерних мереж.

3.1.7 Вимоги до апаратного забезпечення

Вимоги до серверів:

– процесор - тактова частота не менше 4,6 ГГц;
– об'єм оперативної пам'яті - не менше 4096 Мб;
– об'єм жорсткого диску - не менше 700 Гб.

Вимоги до робочих станцій:

– процесор - тактова частота не менше 3,0 ГГц;
– об'єм оперативної пам'яті - не менше 2048 Мб;
– об'єм жорсткого диску - не менше 500 Гб.

Мережеве обладнання:

– комутатори – 3 шт.;
– маршрутизатори – 1 шт.

Периферійні пристрої:

– принтер Canon 3010 – 2 шт.
– принтер HP LaserJet 1022N – 3 шт.
– багатофункціональний пристрій Epson AcuLaser CX11N – 1 шт.

3.1.8 Вимоги до програмного забезпечення

Програмне забезпечення робочих станцій – Windows 10, Windows 7, або UNIX-подібні ОС та прикладне програмне забезпечення, зокрема Python IDLE, веб-браузер та ін.

4 Вимоги до документації

Документація повинна відповідати вимогам ЄСКД та ДСТУ

Комплект документації повинен складатись з:

– пояснювальної записки;
– графічного матеріалу:

1 Фізична топологія комп’ютерної мережі (1 поверх).
2 Фізична топологія комп’ютерної мережі (2 поверх).
3 Фізична топологія комп’ютерної мережі (3 поверх).
4 Логічна топологія мережі
5 Схема IP-адресації.
6 Схема з’єднань комп’ютерної мережі.

*Примітка: У комплект документації можуть вноситися міни та доповнення в процесі розробки.

5 Стадії та етапи проектування

Таблиця 1 – Стадії та етапи виконання кваліфікаційної роботи бакалавра

№ етапу	Назва етапу виконання кваліфікаційної роботи	Термін виконання
1	Розробка і затвердження технічного завдання	23.03-28.03.2022
2	Аналіз технічного завдання	28.03-02.04.2022
3	Визначення вимог до апаратного та програмного забезпечення комп'ютерної мережі	03.04-18.04.2022
4	Проектування схеми організації сервісів безпеки та віддаленого доступу	19.04-04.05.2022
5	Налаштування сервісів безпеки та віддаленого доступу до ресурсів управління підприємством	04.05-12.05.2022
6	Розробка інструкцій із встановлення та налаштування параметрів комп'ютерної мережі і відповідних сервісів	12.05-29.05.2022
7	Безпека життєдіяльності, основи охорони праці	01.06-08.06.2022
8	Оформлення кваліфікаційної роботи	09.06-18.06.2022
9	Попередній захист кваліфікаційної роботи	18.06-22.06.2022
10	Захист кваліфікаційної роботи	22.06-24.06.2022

6 Додаткові умови виконання кваліфікаційної роботи

Під час виконання кваліфікаційної роботи у дане технічне завдання можуть вноситися зміни та доповнення.