ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЕКОНОМІКИ, УПРАВЛІННЯ, ПРАВА ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

Пояснювальна записка

до кваліфікаційної роботи на здобуття ступеня вищої освіти магістр

на тему: «**Модель безпеки локальної мережі підприємства на основі маршрутизатора MikroTik**»

Виконав: здобувач вищої освіти
за освітньо-професійною програмою
Інформаційні управляючі системи та технології
спеціальності 126 Інформаційні системи та технології
освітнього ступеня магістр
групи 126ІСТ_мд_21
Рашин А.І.
Керівник: Поночовний Ю.Л.
Рецензент: Брикун О.М.

Полтава – 2023 року

ВСТУП

Актуальність теми. На даний час немає жодного підприємства, яке б не мало доступу до глобальної мережі. На кожному підприємстві використовують станки, які потрібно підключати до мережі інтернет, телевізори, ноутбуки, принтери та багато іншого апаратного забезпечення. Також на кожному підприємстві використовують програмне забезпечення, якому потрібен доступ до глобальної мережі, починаючи з відділів кадрів і закінчуючи токарем, якому потрібно знайти проєкт або деталь в інтернеті. Також велика кількість підприємств використовує локальну мережу, вона застосовується частіше всього для передачі інформації між робочими станціями, які знаходяться на підприємстві.

У зв'язку з постійною оптимізацією процесів виробництва підприємства все більше і більше занурюються в діджиталізацію, але не всі розуміють, який це ризик. Якщо підприємство вирішило використовувати глобальну мережу у всіх процесах виробництва, потрібно робити великий внесок у безпеку своєї локальної мережі. На даний час у глобальній мережі є велика кількість небезпечних програм, через які підприємство може зупинити свою роботу на невідомий час, окрім цього є можливість втрати конфіденційної інформації.

Для запобігання цього на даний час підприємства використовують різні програмні засоби, але здебільшого вони не допомагають проти серйозних хакерських атак.

У дослідженні запропоновано розподілити мережі підприємства задля забезпечення їх безпеки. Так як доступ до глобальної мережі підприємства використовують різні групи людей, було запропоновано зробити окремі підмережі, адмініструвати які буде системний адміністратор.

У роботі було прийнято рішення розгорнути локальну мережу підприємства за допомогою управляючого комутатора MikroTik. Саме в програмному забезпеченні даного девайсу є можливість зробити локальну мережу безпечною.

Розробку локальної мережі для ПТРЗ «Тепловозоремонтний завод» було узгоджено з керівництвом підприємства, що також підкреслює актуальність даного питання.

Зв'язок роботи з науковими програмами, темами. Робота відповідає дослідженням в межах науково-дослідної роботи «Розвиток підприємництва: управлінські, економічні, інноваційна та правові аспекти» відповідно до договору №9 від 15.05.2023 р. між ТОВ «ПАФ Гарант» та Полтавським державним аграрним університетом (розділ «Обґрунтування показників оцінювання гарантоздатності розподілених інформаційних систем»).

Метою кваліфікаційної роботи є забезпечення нормальних та безпечних умов функціонування структурних підрозділів підприємства ПТРЗ «Тепловозоремонтний завод» за рахунок розгортання та введення в експлуатацію локальної обчислювальної мережі з заданою пропускною спроможністю.

Завданнями кваліфікаційної роботи є:

- дослідження можливих уражень локальної мережі;
- забезпечення цілісності локальної мережі підприємства;
- аналіз можливостей управляючих комутаторів при розділенні мережі;
- створення моделі локальної мережі за допомогою програмного забезпечення Cisco Pocket Tracer;
- апгрейд програмних засобів для захисту інформації на робочих станціях;
- розгортання управляючого комутатора та допоміжної периферії на підприємстві;
- встановлення IP-адресації для робочих станцій користувачів;
- представлення працездатної мережі керівництву підприємства;

Об'єктом дослідження є процеси планування та моделювання комп'ютерних мереж виробничих підприємств.

Предмет дослідження – методи проектування локальної обчислювальної мережі підприємства із виходом у глобальну комп'ютерну мережу Інтернет.

Методи дослідження – проведені в роботі дослідження в роботі дослідження базуються на методах теорії системного аналізу та розрахунку навантаження обчислювальної мережі, методах статистичного аналізу добового, місячного та річного мережевого трафіку виробничого підприємства.

Інформаційна база – інтернет-ресурси, що місять інформацію про інформаційну безпеку локальної мережі на основі управляючих комутаторів та маршрутизаторів, її персональних комп'ютерів.

Практична значущість: розроблено структурну схему IP-адресації локальної мережі, розроблено схеми підмереж, визначено склад обладнання мережі, обґрунтовано нормальну працездатність мережі шляхом розробки та перевірки функціонування у нормальному режимі імітаційної моделі локальної мережі у середовищі Cisco Packet Tracer; розгорнуто мережу підприємства ПТРЗ «Тепловозоремонтний завод» на 300 робочих місць з можливістю подальшого апгрейду.

Апробація результатів дослідження відбувалася шляхом оприлюднення доповідей на міжнародній та студентських конференціях, семінарах.

Публікації. За результатами проведеного дослідження опубліковано тези: «Створення локальної мережі за допомогою мультипортового роутера MikroTik» Матер. щорічної студентської наукової конференції Полтавського державного аграрного університету, 10 листопада 2022 р. м. Полтава; «Принципи побудови локальних мереж» Матеріали студентської наукової конференції Полтавського державного Аграрного університету, 15-16 травня 2023 року, м. Полтава; «Особливості аграрного ринку та фактори, що впливають на ціни для прогнозування вартості аграрної продукції на основі нейронної мережі» Матеріали науково-практичної конференції за підсумками проходження виробничих практик здобувачів вищої освіти спеціальності 126 Інформаційні системи та технології, кафедра інформаційних систем та технологій Полтавського державного аграрного університету, 17 вересня 2023 р. м. Полтава; «Забезпечення безпеки та цілісності даних в інформаційних системах

підприємств» Інформаційні технології в енергетиці та агропромисловому комплексі: матеріали XII Міжнар. наук. конференції Львів, 04-06 жовтня 2023 р.

Структура та обсяг кваліфікаційної роботи логічно пов'язані з задачами досліджень. Робота містить перелік умовних позначень, вступ, три розділи основної частини, висновки, список використаних джерел, додатки. Загальний обсяг текстової частини дипломної роботи складає 66 сторінок формату А4. Вона містить 31 рисунки і 5 таблиць. У роботі використано 49 науково-технічних джерел.

РОЗДІЛ 1
АНАЛІЗ ЗАСТОСУВАННЯ УПРАВЛЯЮЧИХ КОМУТАТОРІВ ТА МАРШРУТИЗАТОРІВ, ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ПІДПРИЄМСТВ

1.1 Аналіз особливостей використання локальних обчислювальних мереж на підприємстві

Комп'ютерна мережа – це складна система, з якої здійснюється передача та обмін даними за певним принципом між кількома об'єктами. Використання мережі має низку переваг, переважно зумовлених практично необмеженими можливостями з допомогою доступу до додаткових ресурсів.

Комп'ютерні мережі класифікуються за низкою ознак, таких як:

– довжина ліній;
– топологія (спосіб побудови);
– метод керування.

Щоб краще зрозуміти, якими способами управління розрізняються мережі, необхідно ознайомитися з їх різновидами відповідно до масштабу й специфіки функціонування.

PAN – персональна мережа, що забезпечує взаємодію кількох пристроїв у рамках одного проекту.

LAN – локальна мережа із замкнутою інфраструктурою незалежно від масштабу. Доступ до локальних мереж має обмежене коло користувачів, визначених адміністратором.

CAN – об'єднання кількох локальних мереж довколишніх об'єктів.

MAN – комп'ютерні мережі між установами в межах одного населеного пункту, що сполучають безліч локальних мереж.

WAN – це відкрита глобальна мережа, що обслуговує масштабні географічні регіони, до складу якої входять як локальні мережі, так й інші телекомунікаційні вузли.

Існує кілька сценаріїв побудови комп'ютерної мережі, які передбачають порядок розташування окремих робочих місць та спосіб їх з'єднання комунікаційними магістралями [1].

Є кілька топологій побудови мережі :

– шина;
– кільце;
– зірка;
– дерево.

На початку використання глобальних мереж на підприємствах було достатньо прокласти кабель за стандартом ISO 11801 (вита пара). Але з часом дротова мережа почала приносити деякий дискомфорт, кабелі постійно пошкоджувались та були не надійні. Вита пара могла використовуватись на відстані до ста метрів, якщо ж потрібно прокласти кабель на відстань більше, використовували оптичне волокно, вона мало більшу пропускну спроможність, тому може передавати сигнал на відстань до 40 км.

З часом велика кількість кабелів почала приносити труднощі для підприємців, постійно доводилося прокладати нові кабелі до можливих місць, де будуть працювати співробітники, використовувати подовжувачі кабелів, щоб додати декілька метрів до довжини кабелю.

З появою бездротової мережі ці всі складнощі стали несуттєві, Wi-Fi мережа почала набувати популярності за рахунок великої кількості користувачів, які мають змогу під’єднатися, також для такої мережі потрібен лише один дріт, який буде йти від роутера або комутатора до точки доступу або іншого роутера [2].

Аналіз особливостей використання бездротових мереж (Wi-Fi) на підприємстві важливий для забезпечення ефективного й безпечного функціонування мережі. Ось деякі ключові аспекти, які слід враховувати.

Розташування точок доступу (AP) та їхнє покриття мають бути ретельно сплановані, щоб забезпечити належне покриття в усіх необхідних зонах на підприємстві.

Ураховувати фактори, такі як: стіни, перешкоди, велика кількість пристроїв й електронних пристроїв, які можуть впливати на сигнал.

Забезпечити безпеку бездротової мережі, використовуючи шифрування (наприклад, WPA3), аутентифікацію й сегментацію мережі для зменшення ризиків несанкціонованого доступу й атак [3].

Пропускна спроможність є одним з головних факторів, на які потрібно звертати увагу при побудові мережі, необхідно враховувати потреби в пропускній здатності та швидкості мережі на підприємстві. Використовувати відповідне обладнання, яке може задовольнити ці потреби.

Потрібно уникати перевантаження мережі через надмірне використання бездротових пристроїв.

Необхідно обирати пристрої, які можна легко налаштовувати та які мають потенціал в оновлені, системи моніторингу та керування мережею, щоб слідкувати за станом бездротової мережі, виявляти проблеми й вчасно реагувати на них. Для керування точками доступу краще буде використовувати контролер для точок доступу, в контролері є власне програмне забезпечення, за допомогою якого є можливість додати всі точки доступу, що знаходяться в мережі.

Потрібно розділити бездротову мережу на окремі сегменти для різних потреб (наприклад, для гостей, орендарів та внутрішніх користувачів), щоб збільшити безпеку й зменшити ризики.

Потрібно розглянути можливість резервного живлення для точок доступу, наприклад, встановити акумулятори (неперервне живлення) для них, щоб забезпечити надійність мережі навіть під час перебоїв живлення, якщо на підприємстві використовується генератор, потрібно встановити пристрій, який буде виправляти синусоїду, наприклад, стабілізатор [4].

Потрібно регулярно оновлювати програмне забезпечення точок доступу та інших мережевих пристроїв, щоб запобігти використанню вразливостей. Необхідно обов’язково використовувати політику використання мережі для співробітників та орендарів, включаючи обмеження доступу до певних ресурсів та додатків. Також потрібно навчати співробітників компанії локальній безпеці,

тому що дуже великий ризик йде саме через них, треба розробити правила поведінки в мережі інтернет для співробітників компанії.

Також регулярний аналіз трафіку та аудит бездротової мережі допоможе виявити аномальні дії та проблеми в роботі мережі. Забезпечення безпеки й надійності, разом із належним плануванням й управлінням, є ключовими компонентами успішного впровадження бездротової мережі на підприємстві [5].

1.2 Опис логічної структури локальної обчислювальної мережі підприємства

Логічна структура бездротової мережі підприємства визначає як дані, так і комунікації, які організовані та функціонують у цій мережі. Вона включає в себе розміщення, керування, безпеку та доступ до ресурсів у бездротовому середовищі.

Логічна структура бездротової мережі має таку структуру :

1) вертикальна та горизонтальна ієрархія: Бездротова мережа підприємства може бути організована в ієрархічну структуру з різними рівнями доступу. На верхньому рівні може бути головний офіс, а на нижньому - відділення або робочі зони;

2) сегменти мережі. Мережу можна поділити на різні сегменти, які відповідають різним функціональним групам підприємства. Наприклад, можуть бути окремі сегменти для відділу продажів, відділу розробки, складу тощо;

3) точки доступу. У бездротовій мережі на кожному рівні ієрархії можуть бути встановлені точки доступу (APs). Вони забезпечують з'єднання між бездротовими пристроями й мережею;

4) середовище віртуальної приватної мережі (VPN). Для забезпечення безпеки даних і конфіденційності може бути використана VPN-технологія для побудови віртуальних приватних мереж між різними фізичними розділами мережі;

5) мережеве керівництво. Для управління мережею може бути використана система керування мережею (Network Management System), яка дозволяє адміністраторам віддалено налаштовувати, моніторити та діагностувати точки доступу та інші мережеві пристрої;

6) шифрування й безпека. Забезпечення безпеки є критично важливим аспектом. Використання шифрування (наприклад, WPA2), аутентифікації та інших заходів безпеки допомагає захистити мережу від несанкціонованого доступу;

7) мобільність. Враховуючи рухомий характер бездротових пристроїв, логічна структура повинна підтримувати мобільність співробітників і гостей у межах підприємства;

8) інтернет-з'єднання. Бездротова мережа підприємства може бути підключена до Інтернету через спеціальний шлюз або маршрутизатор;

9) керування політикою доступу. Політика доступу до мережі (Access Control Policy) визначає, які пристрої і користувачі мають доступ до різних ресурсів мережі;

10) забезпечення якості обслуговування (QoS). Для підтримки передачі різних видів даних (голос, відео, текст) може бути налаштована QoS для забезпечення якісного обслуговування [6].

Загалом, логічна структура бездротової мережі підприємства повинна бути ретельно розроблена, враховуючи потреби, безпеку й масштабованість підприємства, щоб забезпечити ефективну та надійну мережу, яку в подальшому можна з легкістю модернізувати та адмініструвати [7].

Ці аспекти є ключовими для створення стійкої та дієвої інфраструктури бездротової мережі. Необхідно враховувати швидкі технологічні зміни та постійно вдосконалювати стратегії безпеки та управління, щоб відповідати сучасним вимогам та запобігати можливим загрозам кібербезпеки. Такий підхід дозволить підприємству забезпечити ефективну роботу мережі, зберігаючи високий рівень захищеності та гнучкість у вирішенні завдань.

1.3 Аналіз засобів забезпечення локальної обчислювальної мережі підприємства

Аналіз засобів забезпечення бездротової мережі підприємства є важливим етапом при розгляді та впровадженні такої мережі. Засоби забезпечення включають в себе апаратне та програмне забезпечення, а також послуги, які допомагають створити, управляти та підтримувати бездротову мережу.

Інфраструктура точок доступу (APs) є один із найважливіших елементів бездротової мережі – це точки доступу. Важливо аналізувати виробників, моделі та можливості точок доступу. Вони повинні відповідати потребам підприємства щодо покриття, пропускної здатності та безпеки.

Для управління точками доступу повинна бути наявна система управління доступом, яка дозволяє налаштовувати, моніторити та оновлювати всі точки доступу в мережі централізовано.

Засоби забезпечення мають гарантувати надійний рівень безпеки мережі, включаючи шифрування даних (наприклад, WPA3), аутентифікацію користувачів, виявлення інтрузій і контроль доступу.

Системи виявлення та запобігання вторгнень (IDS/IPS) – ці системи дозволяють виявляти та блокувати потенційні загрози та вторгнення в бездротову мережу [8].

Управління політикою доступу. Для повноцінного контролю доступу повинна бути налаштована політика доступу до мережі, яка визначає, які користувачі та пристрої мають доступ до різних ресурсів мережі.

Інтеграція з існуючими системами має важливий аспект у побудові бездротової мережі, засоби забезпечення повинні бути сумісними з існуючою IT-інфраструктурою підприємства, включаючи сервери, мережеве обладнання та додатки.

Також потрібно не забувати про підтримку мобільних засобів, які також грають важливу роль у роботі деяких користувачів, важливо враховувати

можливість підключення мобільних пристроїв і підтримки рухомості користувачів.

Для забезпечення безпеки мережі потрібно використовувати моніторинг й аналіз мережі, засоби забезпечення повинні надавати інструменти для моніторингу та аналізу мережі, включаючи виявлення проблем, аналіз трафіку та визначення пропускної здатності, можливість блокування користувачів, які використовують трафік мережі за власною вигодою [9].

Також вдало спроектована мережа повинна передбачати можливість майбутнього апгрейду, засоби забезпечення мають бути готовими до підтримки нових технологій і стандартів бездротового зв'язку, які можуть з'явитися у майбутньому.

Під час аналізу засобів забезпечення бездротової мережі підприємства важливо враховувати потреби, обсяг і безпеку мережі, а також дотримуватися бюджету й стратегії розвитку підприємства [10].

1.4 Аналіз вимог до безпеки інформаційної системи підприємства

Аналіз вимог до інформаційної безпеки підприємства є важливим етапом при захисті мережі та інформації в організації. Управляючі комутатори та маршрутизатори можуть використовуватися для реалізації різних заходів забезпечення безпеки.

Одним з прикладів є сегментація мережі, управляючі комутатори можуть бути налаштовані для розділення мережі на логічні сегменти (VLANs). Це допомагає відокремити різні групи користувачів і ресурсів, зменшити ризик несанкціонованого доступу та обмежити розповсюдження атак.

Також важливим аспектом управляючого комутатора є керування доступом, за допомогою цього управляючі комутатори підтримують різні механізми керування доступом, такі як 802.1X або MAC-адресний фільтр, що

дозволяють обмежити доступ до мережі тільки авторизованим користувачам та пристроям [11].

Ураховуючи той факт, що наразі відбувається вимкнення світла, при увімкнені живлення напруга може бути більшою, ніж завжди, саме через це комутатор може вийти з ладу. Управляючі комутатори мають влаштоване програмне забезпечення, за допомогою якого є змога зробити резервне копіювання Config файлу. З резервним копіюванням у спеціаліста, який підтримує мережу в робочому стані, буде можливість відновити всі налаштування на новому пристрої, не витрачаючи велику кількість часу на відновлення мережі [12].

Також в управляючих комутаторів є можливість запобігати атакам на мережу, в них є влаштоване програмне забезпечення, яке постійно моніторить мережу та запобігає кібератакам. Одним із прикладів може бути така ситуація: при DDoS-атаці, пристрої в мережі відправляють запит через комутатор, якщо цих запитів буде дуже велика кількість, мережа може перевантажитись, через, що зменшиться швидкість передачі даних. Управляючі комутатори виявляють IP-адресу, через яку йде атака, та блокують її або повідомляють про порушення системному адміністратору.

Управляючі комутатори грають важливу роль у захисті інформаційної безпеки підприємства. Вони надають можливості для сегментації мережі, керування доступом, моніторингу й реагуванню на загрози, що допомагають забезпечити надійний рівень захисту мережі та інформації [13]. Управляючі комутатори є ключовими складовими у захисті мережі від потенційних загроз і забезпеченні безпеки інформації. Вони дозволяють системним адміністраторам активно реагувати на інциденти та ефективно виявляти, блокувати або повідомляти про потенційні атаки, забезпечуючи стабільну та безпечну роботу мережі.

1.5 Опис довірених відносин за допомогою програмних засобів комутаторів та маршрутизаторів MikroTik

Довірені відносини в контексті мережі та інформаційної безпеки вказують на взаємну довіру між різними суб'єктами або сутностями, що мають доступ до мережевих ресурсів або інформації. Ці довірені відносини дозволяють деяким користувачам, пристроям або системам мати спеціальний доступ до певних ресурсів або виконувати конкретні функції, зазвичай на основі авторизації та аутентифікації [14].

Довірені відносини в контексті безпеки мережі вказують на взаємну довіру між пристроями або користувачами в мережі та надають їм спеціальні привілеї або доступ до певних ресурсів.

Довірені відносини можуть створюватися за допомогою таких функцій :

- аутентифікація й авторизація;
- сегментація мережі;
- Firewall і фільтрація трафіку;
- VPN-з'єднання;
- моніторинг і журнали подій;
- оновлення та патчі;
- інтеграція з іншими системами.

MikroTik надає багато інструментів і можливостей для налаштування довірених відносин та забезпечення безпеки в мережі підприємства. Важливо належним чином налаштувати ці засоби й відповідно дотримувати політики безпеки організації [15-16]. МікроТік відомий своєю широкою функціональністю у забезпеченні безпеки мережі. Ця платформа дозволяє створювати і налаштовувати різноманітні інструменти довіри та захисту, такі як аутентифікація, сегментація мережі та фільтрація трафіку. Проте, важливо не лише використовувати ці інструменти, а й ретельно налаштовувати їх, дотримуючись встановлених політик безпеки, щоб забезпечити ефективний захист мережі підприємства.

1.6 Аналіз засобів забезпечення безпеки мережі за допомогою програмних рішень MikroTik

Аналіз засобів забезпечення безпеки мережі є важливим етапом для забезпечення захисту інформації та даних у мережі. Для проведення аналізу засобів забезпечення безпеки мережі слід виконати наступні кроки: інвентаризація пристроїв і ресурсів, ідентифікація вразливостей, оцінка доступності та цілісності даних, аналіз засобів аутентифікації, моніторинг трафіку й подій та багато чого іншого. Усі ці дії можна робити за допомогою управляючого роутера MikroTik.

MikroTik є відомою компанією, яка виробляє управляючі комутатори та інше мережеве обладнання. Управляючі комутатори MikroTik можуть бути використані для різних завдань забезпечення безпеки мережі [17].

MikroTik підтримує створення VLANs, що дозволяє сегментувати мережу на окремі логічні частини. Це допомагає відокремити різні групи користувачів і ресурси в мережі, зменшуючи ризик несанкціонованого доступу до інших сегментів.

Також є можливість налаштувати правила керування доступом на управляючому комутаторі MikroTik, визначаючи, які користувачі або пристрої мають доступ до певних портів або ресурсів. У цьому контексті використовуються ACL (списки керування доступом) [18-19].

Шифрування трафіку. Можна налаштувати шифрування трафіку на окремих портах або використовувати протоколи шифрування, такі як IPsec, для безпеки комунікації між пристроями.

Інтеграція із системами виявлення інтрузій. MikroTik може бути інтегрований із системами виявлення інтрузій для покращення виявлення й реагування на потенційні загрози.

Моніторинг трафіку. Можна використовувати інструменти MikroTik для моніторингу та аналізу трафіку в мережі для виявлення аномалій та загроз.

Оновлення і патчі. Важливо регулярно оновлювати програмне забезпечення MikroTik для виправлення вразливостей і забезпечення актуального рівня безпеки [20].

Висновки до розділу 1

У першому розділі розглянуто питання вимог до забезпечення безпеки локальної обчислювальної мережі підприємства. Безпека мережі є невід'ємною частиною безпеки підприємства, беручи до уваги те, що зараз майже кожен відділ підприємства використовує локальну або глобальну мережу, вони знаходяться в зоні ризику. Під час побудови мережі потрібно звернути велику увагу саме на безпеку. У мережі інтернет є багато рекомендацій, як можна покращити безпеку локальної мережі підприємств, але велику кількість рекомендацій не можливо втілити в життя, не маючи гарного апаратного чи програмного забезпечення. Тому при побудові мережі потрібно враховувати засоби, які допоможуть у налаштуванні мережі. Управляючий роутер MikroTik має всі необхідні варіанти для забезпечення безпеки мережі. На роутері MikroTik є можливість навіть програмувати, так як він має у своєму програмному забезпеченні інтерфейс командного рядку, за допомогою якого можна писати скрипти та налаштовувати роутер за своїми вподобаннями.

Також роутер MikroTik вважають одним із найнадійніших і безвідмовних, його пропускна спроможність вважається однією з найшвидших. У роутера є можливість налаштовувати кожен порт, використовувати не тільки виту пару, а й оптоволокно.

РОЗДІЛ 2
ПОСЛІДОВНІСТЬ РОЗГОРТАННЯ ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТВА НА БАЗІ ОБЛАДНАННЯ MIKROTIK

2.1 Характеристика підприємства

ТОВ «Тепловозоремонтний завод» (ПТРЗ) – це підприємство, яке спеціалізується на ремонті та модернізації тепловозів. Завод розташований у місті Полтава, Україна.

Підприємство був заснований у 1964 році. Завод має потужності для ремонту та модернізації тепловозів серії ТГМ23, ТГМ6, ТГМ4, ТЕ33А, а також тепловозів виробництва інших країн.

Завод має виробничі площі площею понад 100 гектарів. На заводі працює понад 1000 працівників. Підприємство є одним з найбільших тепловозоремонтних заводів в Україні. Він забезпечує ремонт та модернізацію тепловозів для залізниць України, а також для залізниць інших країн.

Основні види діяльності підприємства: ремонт тепловозів, модернізація тепловозів, виробництво запасних частин до тепловозів.

Підприємство є важливим підприємством для розвитку залізничного транспорту в Україні. Завод забезпечує ремонт та модернізацію тепловозів, що дозволяє продовжити термін їх служби та підвищити експлуатаційні характеристики.

Ось деякі з основних досягнень підприємства:

- є одним з найбільших тепловозоремонтних заводів в Україні;
- забезпечує ремонт та модернізацію тепловозів для залізниць України, а також для залізниць інших країн;
- має потужності для ремонту та модернізації тепловозів різних моделей;
- має досвід роботи з тепловозами виробництва інших країн.

Підприємство планує подальший розвиток та розширення виробничих потужностей. Завод прагне стати одним із провідних тепловозоремонтних заводів у Європі.

Для забезпечення інформаційної безпеки на підприємстві ПТРЗ розроблено та впроваджено певний комплекс заходів. Адміністративне управління інформаційною безпекою, цей напрямок передбачає розробку та впровадження політики інформаційної безпеки, а також навчання персоналу з питань інформаційної безпеки.

Також підприємство приділяє увагу технічному управлінню інформаційною безпекою, цей напрямок передбачає захист інформаційних систем і ресурсів від несанкціонованого доступу, використання, розкриття, модифікації або знищення.

Важливим аспектом інформаційної безпеки є організаційне управління інформацією. Цей напрямок передбачає розробку та впровадження процедур і процесів, які забезпечують захист інформації.

Вимоги щодо забезпечення інформаційної безпеки на підприємстві підприємство визначені в Політиці інформаційної безпеки, яка затверджена директором підприємства.

Основні вимоги Політики інформаційної безпеки:

- конфіденційність;
- інформація, яка є конфіденційною, повинна бути захищена від несанкціонованого доступу;
- цілісність;
- інформація повинна бути захищена від несанкціонованих змін;
- доступність;
- інформація повинна бути доступна лише уповноваженим користувачам.

Підприємство регулярно проводить аудити інформаційної безпеки, щоб оцінити стан інформаційної безпеки на підприємстві та виявити можливі уразливості.

Також підприємство співпрацює з державними органами з питань інформаційної безпеки, щоб отримувати інформацію про нові загрози інформаційній безпеці та розробляти заходи для їх протидії.

Підприємство постійно вдосконалює систему управління інформаційною безпекою, щоб забезпечити захист даних підприємства від можливих загроз. «Полтавський тепловозоремонтний завод» має хорошу основу для забезпечення інформаційної безпеки, оскільки має розроблену та впроваджену політику інформаційної безпеки, а також регулярно проводить аудити інформаційної безпеки. Ця основа може бути покращена шляхом впровадження додаткових заходів, які допоможуть у швидкому виявленні проблеми з мережею та інформаційним середовищем.

За допомогою управляючого комутатора підприємство отримає змогу виявляти та швидко реагувати на інциденти, пов'язані з локальною безпекою інформації. Також в можливостях комутатора є програмні методи для контролю доступу до мережі, за допомогою цього буде відбуватись контроль до доступу інформації та ресурсів підприємства.

Також за допомогою нового обладнання буде можливість упровадити систему резервного копіювання, за допомогою якої можна в будь-яку мить відновити втрачені дані, за допомогою чого отримати повністю працездатну систему [21].

2.2 Розробка моделі локальної мережі за допомогою програмного забезпечення Cisco Pocket Tracer

Створення локальної мережі (ЛМ) для підприємства – важке завдання, яке вимагає обговорення потреб підприємства та проектування інфраструктури, яка задовольнить ці потреби.

Розпочинати потрібно з докладного аналізу потреб підприємства. Потрібно розглянути, скільки пристроїв необхідно під'єднати до мережі, які функції вони повинні виконувати і які вимоги до продуктивності та безпеки існують [22].

Важливим етапом мережі є вибір необхідного обладнання, таке як: комутатори, маршрутизатори, бездротові точки доступу й сервери, враховуючи обсяги роботи та технічні вимоги. Також потрібно визначити, де буде розташоване обладнання. Важливо врахувати безпеку, охолодження та легкість обслуговування.

Планування IP-адресування потрібно розробити заздалегідь, обрати підсегменти, призначені для різних відділів або функцій. Для захисту мережі потрібно розробити стратегію безпеки мережі, включаючи файерволи, VPN, аутентифікацію та контроль доступу. Головна потреба від керівництва компанії була саме в захисті мережі, тому цьому аспекту приділялася велика увага: захист мережі від загроз і несанкціонованого доступу. Керівництву було запропоновано зробити закупівлю жорстких дисків для зберігання й відновлення резервних копій серверу й серверного обладнання [23].

Встановлення та налаштування обладнання, включаючи комутатори, маршрутизатори, сервери та програмне забезпечення відповідно до проєкту.

Проводення тестування для перевірки працездатності мережі та рішення можливих проблем під час налагодження.

Також ведемо документацію про конфігурацію мережі, адресацію IP, паролі та інші важливі дані. Створюємо схему мережі та список обладнання.

Проводимо навчання персоналу, який буде відповідати за обслуговування мережі (системного адміністратора), роботі з обладнанням, а також вирішенню потенційних проблем [24].

Після введення в експлуатацію мережі, регулярно потрібно моніторити її працездатність та вирішувати поточні проблеми.

Перед побудовою мережі потрібно скласти план, за яким буде відбуватись побудова мережі. Cisco Packet Tracer є популярним інструментом для моделювання та навчання мережевим технологіям, розроблений Cisco. Він

дозволяє створювати, налаштовувати та тестувати мережі, використовуючи віртуальне обладнання Cisco [25-26].

Вибір топології мережі є важливим етапом при проєктуванні мережі, оскільки це визначає фізичну організацію та спосіб підключення пристроїв у мережі. Вибір топології повинен відповідати потребам проєкту, обмеженням та цілям мережі. При проектуванні мережі використовують такі топології.

1) Зіркова топологія – у цій топології всі пристрої під'єднані до центрального комутатора або маршрутизатора. Вона легко керується, надійна й забезпечує простий доступ до всіх пристроїв. Приклад наведено на рис. 2.1.

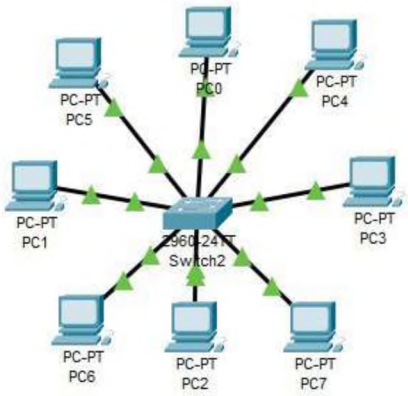

Рисунок 2.1 – Топологія «Зірка»

2) Кільцева топологія – у даній топології кожен пристрій під'єднаний до двох сусідів, утворюючи кільце. Вона відома своєю надійністю, але знижується продуктивність мережі, якщо сталася неполадка на одному з кінців кільця. Приклад наведено на рис. 2.2.

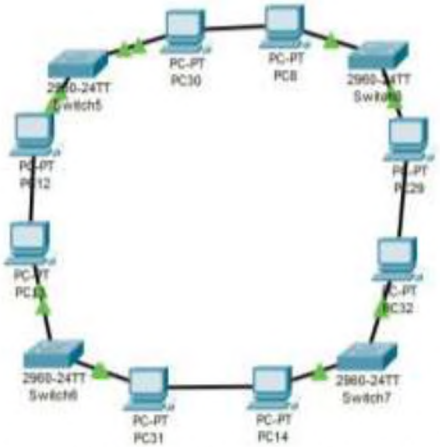

Рисунок 2.2 – Топологія «Кільце»

3) Лінійна топологія – усі пристрої під'єднані до одного основного кабеля. Вона проста та дешева, але надійність може страждати в разі пошкодження основного кабелю. Приклад наведено на рис. 2.3.

Рисунок 2.3 – «Лінійна» топологія

4) Модульна топологія – у цій топології кожен пристрій під'єднаний до кожного іншого пристрою в мережі. Це надійна, але дорога опція, яка вимагає багато кабелів та конфігураційного зусилля. Приклад наведено на рис. 2.4.

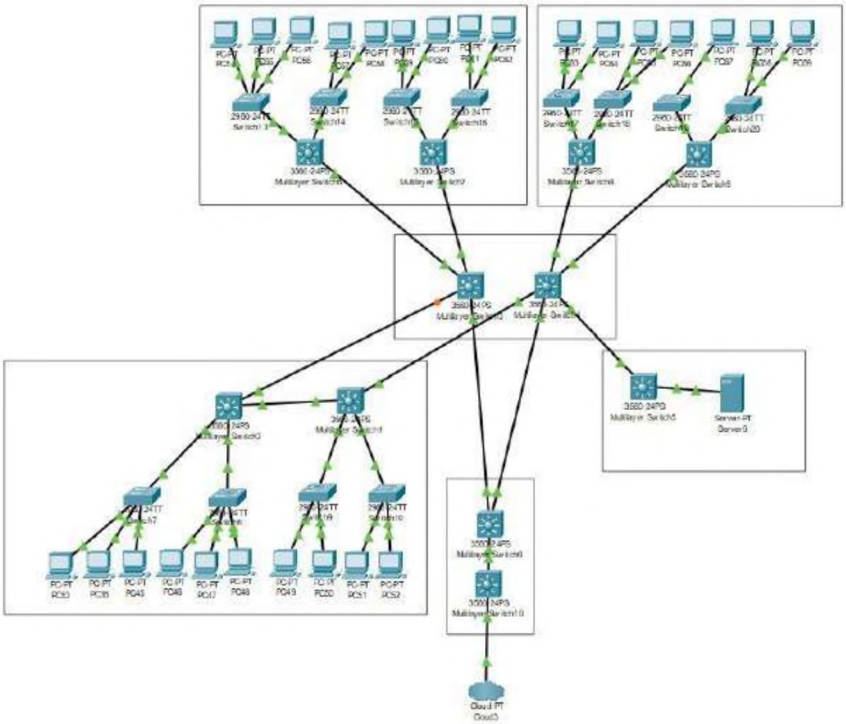

Рисунок 2.4 – «Модульна» топологія

5) Деревовидна топологія – дана топологія комбінується із зірковою та кільцевою топологією, дозволяючи створити ієрархічну структуру мережі. За допомогою цього є можливість побудувати велику мережу з різними рівнями доступу, але потребує управління та планування, приклад наведено на рис. 2.5.

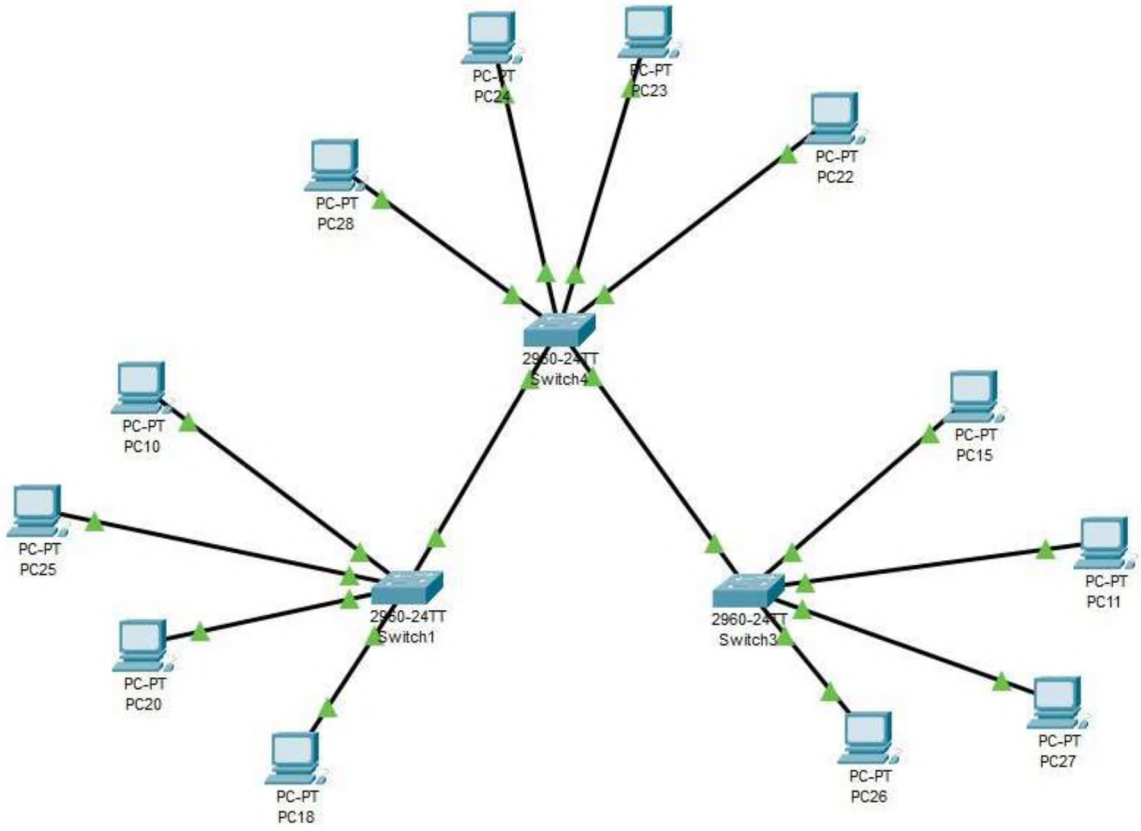

Рисунок 2.5 – «Деревовидна» топологія

6) Ланцюгова топологія – пристрої під'єднані один за одним, утворюючи послідовний ланцюг. Вона досить проста, але надійність може страждати в разі несправності в середині ланцюга, приклад наведено на рис. 2.6.

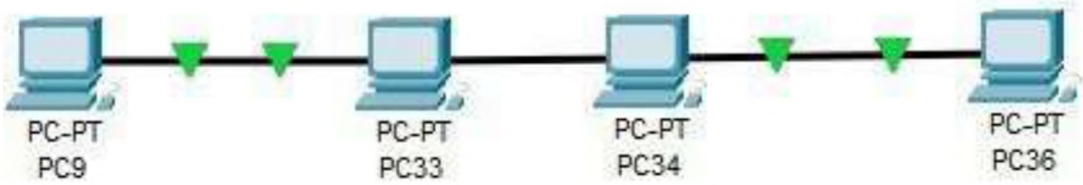

Рисунок 2.6 – «Ланцюгова» топологія

7) Гібридна топологія – у цій топології комбінуються різні типи топологій, що використовуються для під'єднання різних частин мережі. Вона дозволяє досягнути балансу між надійністю, продуктивністю та вартістю, приклад наведено на рис. 2.7.

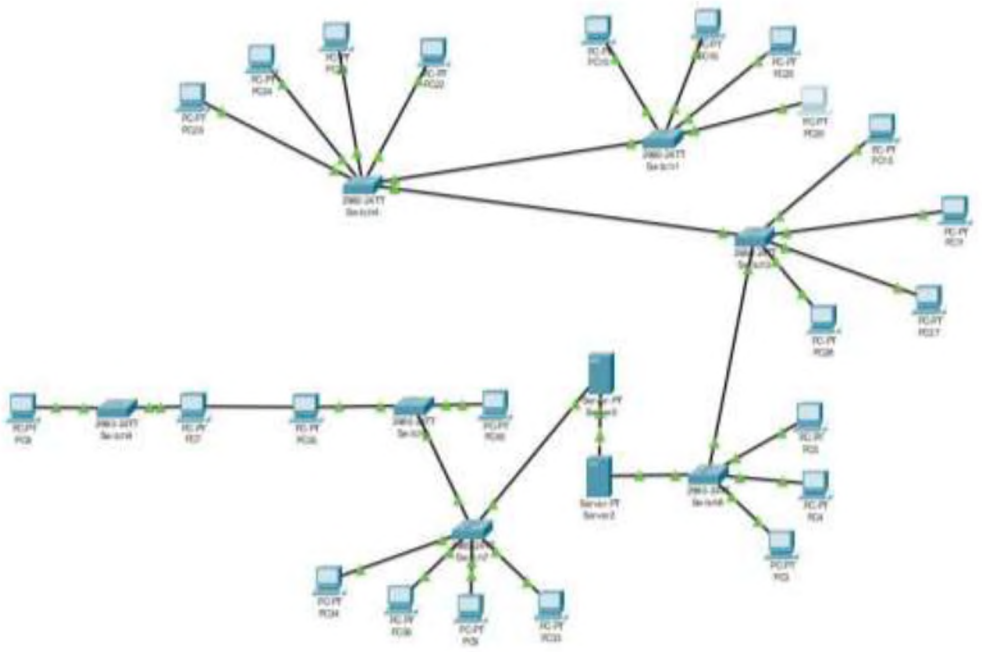

Рисунок 2.7 – «Гібридна» топологія

Вибір топології залежить від конкретних потреб проєкту, кількості пристроїв, вимог до надійності, бюджету та інших факторів. Перед вибором топології важливо ретельно проаналізувати всі ці фактори та розробити план мережі, який відповідає потребам. Перед упровадженням та закупівлею пристроїв було прийняте рішення розробити схему локальної мережі підприємства [27].

2.3 Етапи розгортання управляючого роутера MikroTik на підприємстві

На початку проектування мережі потрібно було обрати апаратне забезпечення, за допомогою якого це буде виконано. Так як керівництво планувало один поверх будівлі здавати в оренду та використання бездротової мережі з дротовою, було вирішено купити управляючий роутер, за допомогою якого буде змога розділити мережі. Також роутер повинен мати хороше програмне забезпечення. Було прийнято рішення зробити порівняльну таблицю

найпопулярніших управляючих роутерів, які є на ринку, приклад наведено в таблиці 2.1 [28].

Таблиця 2.1 – Порівняльна характеристика управляючих комутаторів

Параметр	Cisco	HP (Hewlett Packard)	Dell	MikroTik
Продуктивність	Плюси: висока продуктивність та надійність. Cisco славиться передовими технологіями та широким асортиментом моделей.	Плюси: висока продуктивність та надійність, особливо на великих підприємствах.	Плюси: добра продуктивність в рамках свого цінового діапазону.	Плюси: досить гарна продуктивність для бюджетних рішень.
Ціна	Мінуси: Cisco-комутатори зазвичай дорожчі, особливо для більших конфігурацій.	Мінуси: HP може бути дорожчим в порівнянні з іншими конкурентами в своїй категорії.	Мінуси: Dell може мати конкурентоспроможні ціни, але бракує функцій у деяких бюджетних моделях.	Мінуси: MikroTik пропонує доступні продукти, але в деяких випадках їх продуктивність обмежена
Розширені функції	Плюси: Cisco надає різноманітні продукти з різними рівнями функціональності та підтримує розширені мережеві функції.	Плюси: HP також пропонує різні рівні функціональності та має хорошу підтримку розширених функцій.	Плюси: Dell надає деякі розширені функції в бюджетних моделях, але обмежене в порівнянні з Cisco та HP.	Плюси: MikroTik пропонує розширені функції у своїх продуктах, особливо для маленьких та середніх мереж.
Підтримка і обслуговування	Плюси: Cisco та його дилерська мережа зазвичай мають високу якість обслуговування та підтримки.	Плюси: HP також має добру підтримку та обслуговування через свою мережу партнерів.	Плюси: Dell пропонує прийнятну підтримку, але вона може бути менш доступною порівняно з Cisco та HP.	Мінуси: MikroTik не має такої широкої мережі партнерів для підтримки, особливо поза межами популярних ринків.

Продовження таблиці 2.1

Параметр	Cisco	HP (Hewlett Packard)	Dell	MikroTik
Легкість налаштування	Мінуси: Cisco комутатори можуть бути складні для налаштування, особливо для новачків.	Плюси: HP пропонує простий інтерфейс та інструменти для легкого налаштування.	Плюси: Dell також має добре спроектований інтерфейс для налаштування, що полегшує роботу.	Плюси: MikroTik має дружній інтерфейс та легке налаштування, особливо для менших мереж.
Сумісність з обладнанням і ПЗ	Плюси: Cisco має широку сумісність з іншим обладнанням та ПЗ, але інколи потребує використання виробника-партнера.	Плюси: HP також має добру сумісність та може бути інтегрований з різними рішеннями.	Плюси: Dell зазвичай має хорошу сумісність з іншим обладнанням і ПЗ.	Плюси: MikroTik пропонує добру сумісність та може бути інтегрований з багатьма сторонніми рішеннями.

Після перегляду порівняльної характеристики було прийнято рішення використовувати управляючий комутатор фірми MikroTik, оскільки він має найбільше переваг, приклад наведено в таблиці 2.2.

Таблиця 2.2 – Переваги та недоліки комутатора MikroTik

Параметр	Переваги	Недоліки
Вартість	1.Зазвичай доступні вартісно, ідеально підходять для SMB та малих підприємств 2.Здатність знижувати загальні витрати на обладнання та експлуатацію мережі.	1. Деякі продукти вищого класу можуть бути дорожчими.
Простота використання	1.Легкий у використанні та налаштуванні, підходить для користувачів з різними рівнями досвіду. 2. Інтерфейс з графічними опціями спрощує налаштування та моніторинг.	Може бути складною для новачків з обмеженим досвідом мереж.

Продовження таблиці 2.2

Параметр	Переваги	Недоліки
Інтеграція	1. Здатність інтегрувати комутатори MikroTik з іншими пристроями в мережі. 2. Підтримка стандартних мережевих протоколів, що робить їх сумісними з іншим обладнанням. деякими спеціалізованими рішеннями. 3. Великий вибір різних моделей комутаторів для різних потреб.	1.Здатність працювати у взаємодії з конкретними спеціалізованими рішеннями.
Розширені функції	1. Має велику кількість розширених функцій, включаючи VLAN, VPN, маршрутизацію, QoS тощо. 2. Підтримка багатьох мережевих протоколів та IPv6. 3. Можливість налаштування правил файєровола та обробки пакетів. 4. Гнучкість у налаштуванні й адаптації до потреб користувача.	1. Деякі продукти можуть бути обмежені в певних функціях. 2. Підтримка управління журналами та аналітики може бути обмежена.
Надійність	1. Відомий своєю стабільністю та надійністю 2. Регулярні оновлення програмного забезпечення та активна спільнота користувачів. 3. Довгий термін служби.	1. Можливість обмеженої підтримки для окремих моделей.
Підтримка	1. Існує активна спільнота користувачів і форуми для підтримки й обговорення. 2. Можливість отримати допомогу на форумах та з офіційного джерела MikroTik. 3. Професійна підтримка доступна для більш складних випадків.	
Підтримка хмарних послуг	1. Підтримка хмарних послуг та інтеграція з хмарними платформами.	1. Вимагає збереження конфіденційності та безпеки даних, переданих у хмару.
Безпека	1. Можливість налаштування сильних паролів та багаторівневої автентифікації.	1. Використання слабких або залишених за замовчуванням паролів може призвести до несанкціонованого доступу та порушення безпеки.

Розгортання управляючого роутера MikroTik на підприємстві включає декілька етапів, щоб забезпечити належне налаштування та безпеку мережі:

1. Аналіз потреб підприємства: скільки користувачів та пристроїв, вимоги до продуктивності й безпеки.

2. Вибір відповідного маршрутизатора MikroTik відповідно до потреб. У нашому випадку вибір випав на Маршрутизатор MikroTik CCR2004-1G-12S+2XS. Саме цей роутер є одним з найкращих у лінійці MikroTik

3. Головним етапом розгортання є схема IP-адресування для локальної мережі та визначення підсигментів.

4. Налаштування захисту мережі за допомогою вбудованих функцій безпеки MikroTik, включаючи файерволи, VPN, аутентифікацію та контроль доступу.

5. Налаштування конфігурації маршрутизатора MikroTik, налаштування IP, налаштування DHCP, визначення маршрутів.

6. Налаштування VLAN, оскільки на підприємстві використовуються віртуальні машини, на яких налагоджені віртуальні локальні мережі.

7. Налаштування портів маршрутизатора під окремі сегменти мережі. Підключення відділів та групи користувачів до відповідних портів маршрутизатора.

8. Налаштування параметрів безпеки, включаючи фільтрацію та аутентифікацію, для захисту мережі.

9. Підготовка до резервного копіювання та відновлення в разі необхідності, розробка плану або написання скриптів, за допомогою яких буде відбуватись планове резервне копіювання.

10. Останім кроком є тестування мережі перед її впровадженням.

За допомогою цих кроків буде відбуватися розгортання управляючого роутера MikroTik на підприємстві та забезпечуватися надійна й ефективна мережа [29].

На підприємстві працює близько 300 співробітників, деякі з них працюють на робочих станціях на офісі, деякі працюють на підприємстві. Оскільки працівники використовують як стаціонарні ПК, так і ноутбуки, потрібно, щоб з'єднання було хорошим як через Wi-Fi, так і через Ethernet.

Також на підприємстві є сервери, які працюють через Ethernet з'єднання. Оскільки на підприємстві використовується програмне забезпечення Bas (для

бухгалтерського обліку), було створено термінальний сервер, доступ до якого відбувається за протоколом RDP. Таким чином при встановленні керуючого роутера потрібно зробити можливість віддаленого доступу з глобальної мережі на термінальний сервер, це можна буде зробити за допомогою перекидання портів [30].

Ураховуючи те, що на підприємстві є сервери, потрібно максимально заблокувати до них доступ стороннім користувачам, це можна зробити за допомогою облікових засобів на самому сервері firewall, який використовується на серверному обладнані, та за допомогою керуючого роутера. У нашому випадку буде заблокований доступ стороннім користувачам до підмережі LAN_PTRZ. Найвразливішою частиною мережі є Wi-Fi. Доступ до нього мають усі відвідувачі підприємства, тому потрібно заборонити доступ із підмережі Wi-Fi в мережу Ethernet, де знаходяться сервери.

Для налаштування IP-адресування локальної мережі та визначення підсегментів, потрібно враховувати ряд важливих аспектів, таких як: кількість пристроїв, які будуть підключені до мережі; потреби в розділенні мережі на логічні сегменти для забезпечення безпеки й ефективності, а також можливість майбутнього розширення. Приклад побудови локальної мережі наведено на рисунку 2.8 [31].

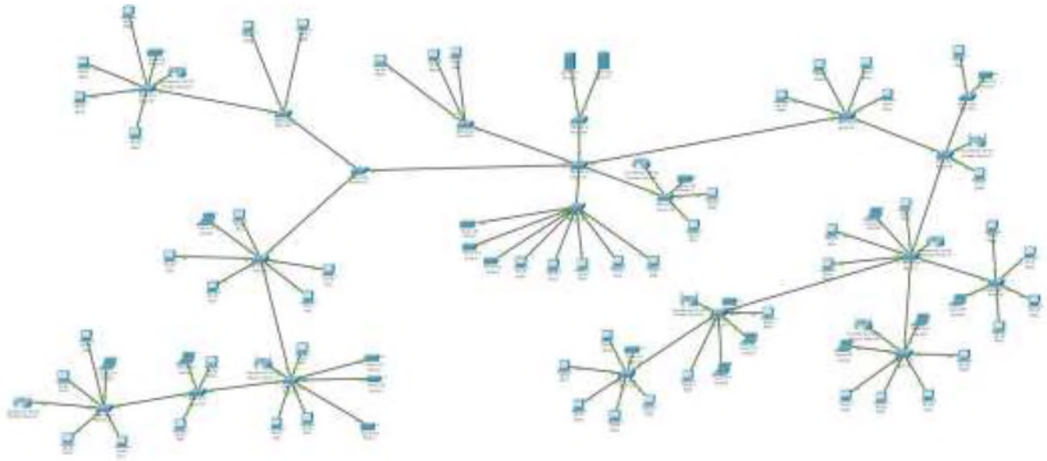

Рисунок 2.8 – Побудова локальної мережі підприємства за допомогою Cisco Packet Tracer

Оскільки мережа підприємства буде розділена на підсегменти, прийнято рішення, що орендарі, які знаходяться на третьому поверсі будівлі, повинні мати окрему підмережу, з якої не буде доступу до мережі підприємства. Також для більшої безпеки потрібно розділити локальну мережу на Ethernet та Wi-Fi.

Ось загальна схема для IP-адресування локальної мережі та визначення підсегментів:

Визначаємо діапазон для локальної мережі. Зазвичай використовуються приватні IP-адреси з діапазону IPv4, наприклад, 192.168.0.0/24 або 10.0.0.0/24. Ці діапазони дозволяють виділити адреси для внутрішнього використання в мережі. У нашому випадку використовуються адреси 10.0.0.0/22, це означає, що в нашій мережі буде діапазон IP-адрес 10.0.0.0 - 10.0.3.255 з маскою 255.255.252.0, а з кількістю IP-адрес 1024, приклад наведено на рисунку 2.9.

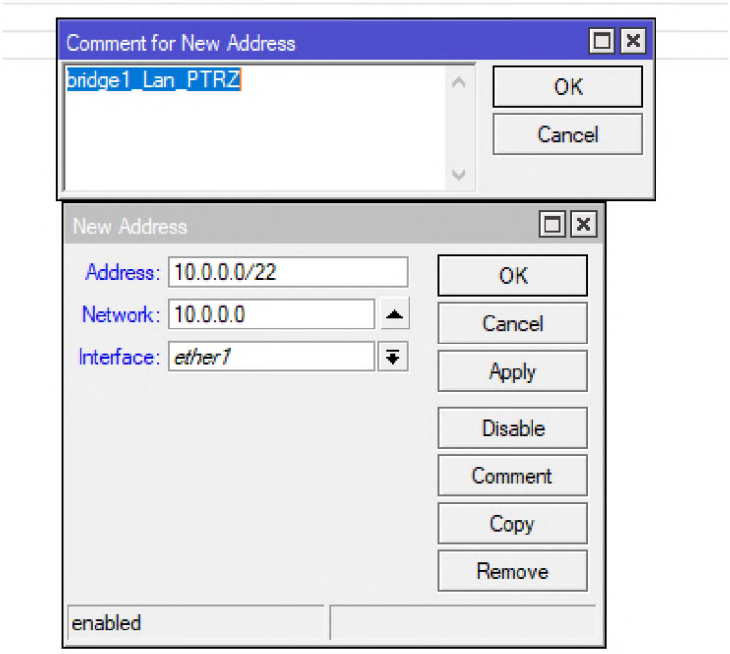

Рисунок 2.9 – Створення діапазону IP-адрес

Потрібно визначити кількість підсегментів, які потрібні. На підприємстві будуть такі підсегменти: Ethernet, Wi-Fi, орендарі.

Надаємо розмір кожного підсегменту, іншими словами, виділяємо певну кількість IP-адрес та призначаємо кожному підсегменту. На підприємстві підсегмент Ethernet – має розмір /22, підсегмент Wi-Fi – розмір /24, підсегмент

орендарі – має розмір /24 (256 адреси, 254 з яких доступні для пристроїв), приклад наведено на рисунку 2.10 [32].

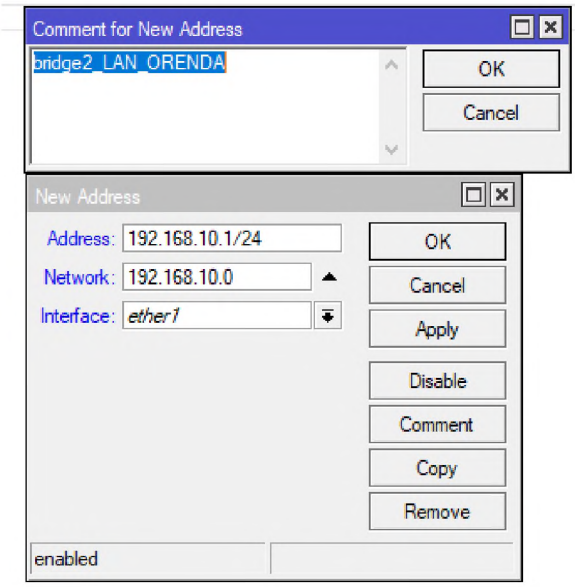

Рисунок 2.10 – Розділення мережі на підсегменти

Також встановлюємо правила маршрутизації й firewall, які дозволяють блокувати зв'язок між різними підсегментами відповідно до потреб у безпеці. На підприємстві блокується зв'язок таким чином, як наведено на рисунку 2.11 [33].

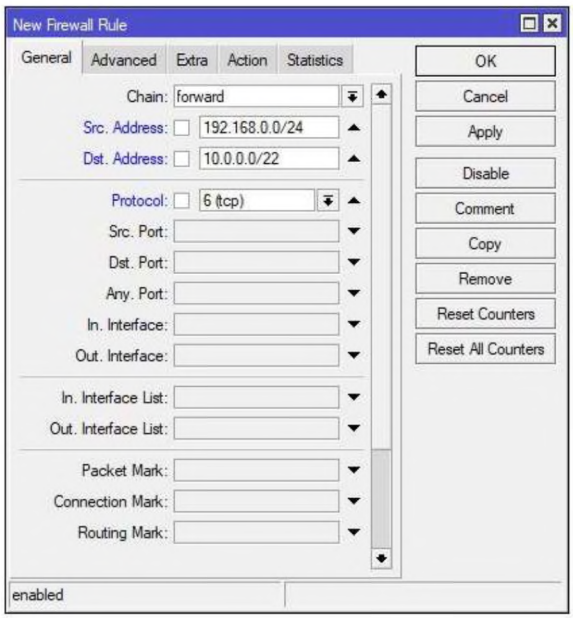

Рисунок 2.11 – Блокування переміщення пакетів з однієї підмережі в іншу

Після чого налаштовуємо IP-адресування в локальній мережі та тестуємо. Перед початком налаштування firewall, автентифікації та безпеки потрібно завантажити останні оновлення прошивки роутера, з магазину вони можуть бути застарілі. Для цього ми переходимо на офіційну сторінку MikroTik, в розділі «Продукція» обираємо наш роутер, після чого нас перекине на строінку роутера, де буде документація та остання прошивка на нього. Приклад наведено на рисунку 2.12 [34].

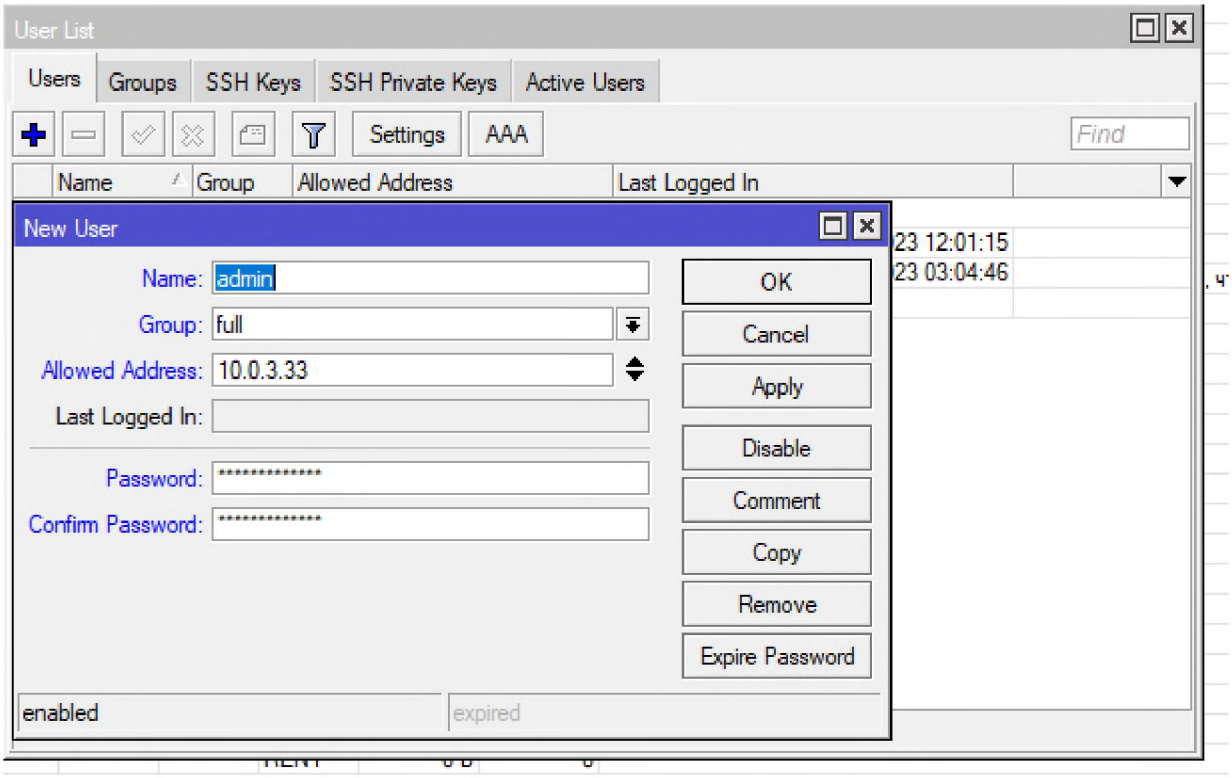

Рисунок 2.12 – Створення користувача з повними правами адміністратора на роутері MikroTik

Після завантаження оновлення потрібно створити користувача, а саме адміністратора. Найпопулярніші методи злому маршрутизаторів пов'язані з ігноруванням контролю облікових засобів. Для налаштування облікового засобу адміністратора переходимо до MikroTik, натискаємо в панелі інструментів «System-Users», після чого додаємо нового користувача з повними правами. Також на даному роутері є можливість додати нового користувача за допомогою

терміналу, для цього в панелі керування обираємо «NewTerminal», та пишемо команду «/user add name="admin" password="PASSWORD" group=full».

Створивши користувача Адміністратор, можна переходити до створення та налаштування «Address List». Для цього переходимо до панелі керування та натискаємо на «Interfaces-Interfaces list», де додаємо підсегменти мережі (листи) й надаємо інтерфейс. Наприклад, в інтернет-провайдера, який заходить до підприємства (Volia), інтерфейс буде «ether1», у резервного провайдера (Altanet) інтерфейс буде «ether2». Bridge використовується для того, щоб об'єднати всі інтерфейси локальної мережі та застосовувати до них єдині правила в налаштуваннях. Також ці налаштування можна зробити за допомогою терміналу MikroTik, для цього потрібно в терміналі прописати команду :

/interface list

add comment=defconf name=WAN

add comment=defconf name=LAN

/interface list member

add interface=Bridge-LAN list=LAN

add interface=ether1 list=WAN.

Після основних налаштувань безпеки можна переходити до налаштування Firewall (Default Rules). Важливим кроком в налагодженні локальної мережі є налаштування DHCP серверу, саме за допомогою цього роутер буде видавати IP-адреси клієнтам мережі, також при налаштуванні сервера потрібно вказати час оренди (час, на який буде видаватись IP для пристрою). Ураховуючи те, що на підприємстві користувачі часто їздять у відрядження, було вирішено виділити п’ятнадцять календарних днів [35].

Для налаштування DHCP серверу на управляючому роутері MikroTik потрібно :

1) створити пул IP-адрес, які будить виділятись. Переходимо до вкладки «IP» та обираємо «Pool», де прописуємо в нашому випадку 10.0.0.2-10.0.3.254;

2) для присвоєння часу оренди потрібно перейти до вкладки «IP» та обрати «DHCP server», після чого обрати інтерфейс, для якого ми призначаємо час

оренди та виставити відповідний час, у нашому випадку 15 днів. Приклад наведено на рисунку 2.13.

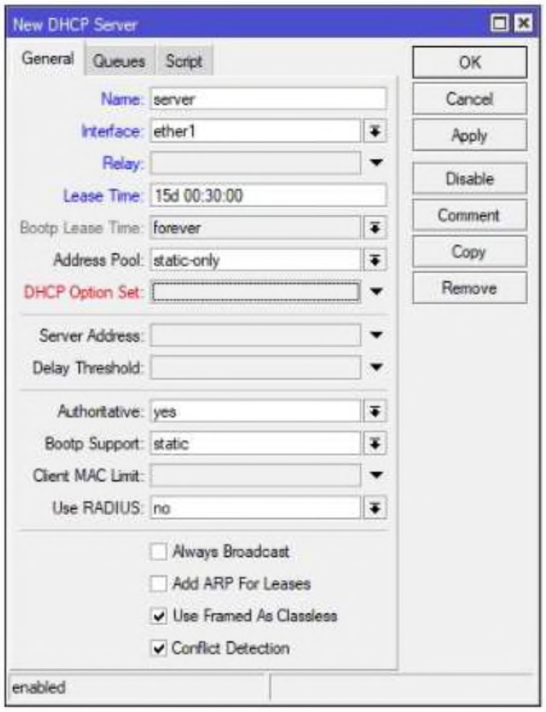

Рисунок 2.13 – Налаштування DHCP server

3) Також потрібно зробити налаштування, які буде роздавати DHCP server а саме : DNS та WINS-серверів. Приклад наведено на рисунку 2.14.

Рисунок 2.14 – Налаштування DNS та WINS-серверів

Також налаштування серверів можна зробити за допомогою терміналу MikroTik. Для цього потрібно перейти до терміналу та прописати такі команди, які наведено на рисунку 2.15. [36].

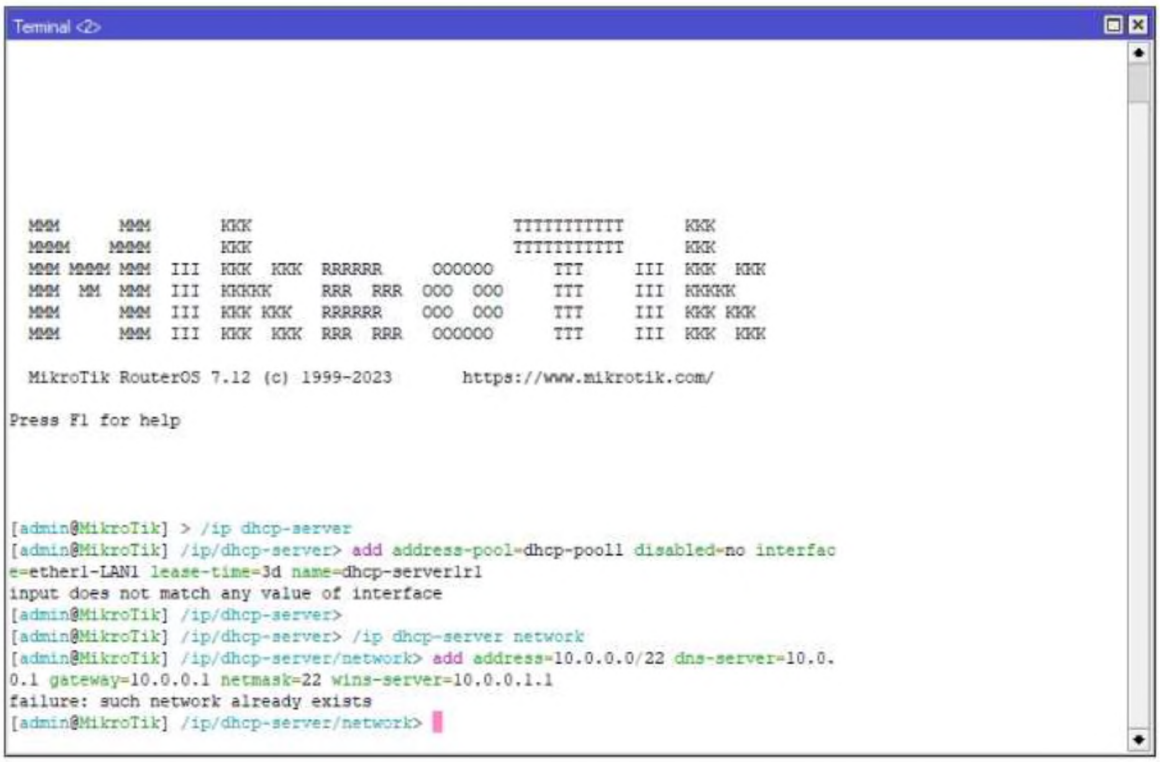

Рисунок 2.15 – Налаштування серверу через консоль

Для перевірки працездатності DHCP-сервера потрібно підключитися комп'ютером до заданого інтерфейсу, виставити в його налаштуваннях отримання IP-адреси за допомогою DHCP-сервера і перевірити, чи отримані задані нами налаштування.

Налаштування WLAN або бездротового інтерфейсу. На панелі інструментів переходимо до «Wireless», тут ми побачимо список всіх бездротових інтерфейсів, натискаємо на «Add New», обираємо потрібний нам канал надаємо потрібний SSID ідентифікатор, встановлюємо безпеку для бездротового каналу «WPA2» та зберігаємо налаштування. Приклад наведено на рисунку 2.16.

Рисунок 2.16 – Налаштування WLAN

Наступним кроком є налаштування розділення мережі на окремі сегменти за допомогою роутера MikroTik, для цього потрібно визначити відповідні VLAN-и та налаштувати порти маршрутизатора для роботи з цими VLAN-ами.

Налаштування портів відбувалось за допомогою терміналу MikroTik, так як це найшвидший варіант налаштування. Приклад налаштування портів наведено на рисунку 2.17.

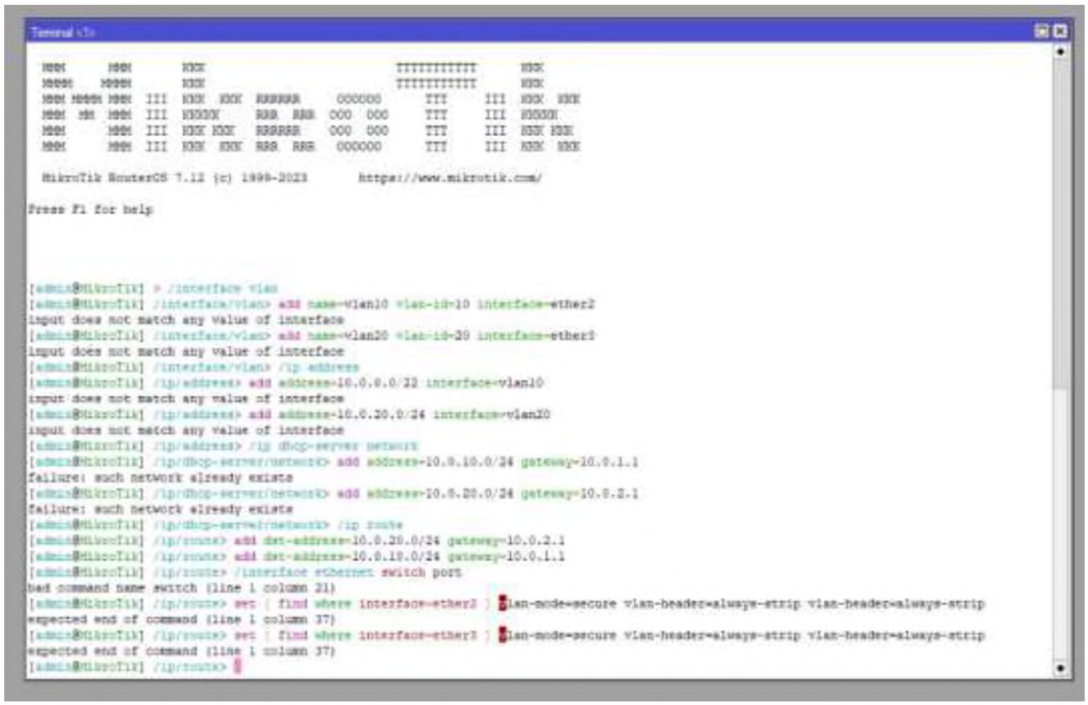

Рисунок 2.17 – Налаштування портів маршрутизатора

Підготовка до резервного копіювання та відновлення. Для автоматичного створення резервних копій MikroTik використовується скрипт на основі мови програмування Bash.

Для створення сценарію потрібно створити папку для зберігання резервних копій на локальному сервері або комп'ютері (краще всього робити резервні копії на декілька носіїв інформації). Налаштувати доступ SSH на MikroTik та забезпечити можливість, щоб віддалені команди могли виконуватися без введення пароля. Для цього можна використовувати ключі SSH. Створити Bash-скрипт, який буде підключатися до MikroTik, виконувати команди для створення резервної копії й зберігати її на локальному сервері або комп'ютері.

Для підприємства було написано такий код:

```
bash
Copy code
#!/bin/bash
# Змінні
MikroTik_IP="IP-адреса_MikroTik"
MikroTik_User="Ваш_користувач"
MikroTik_Password="Ваш_пароль"
Backup_Directory="/шлях_до_папки_з_резервними_копіями/"
# Створити ім'я файлу для резервної копії на основі поточної дати та часу
Backup_Filename="backup_$(date +'%Y%m%d_%H%M%S').backup"
# Підключення до MikroTik і створення резервної копії
sshpass -p "$MikroTik_Password" ssh "$MikroTik_User@$MikroTik_IP" /system backup save name="$Backup_Filename"
# Завантаження резервної копії на локальний сервер або комп'ютер
scp "$MikroTik_User@$MikroTik_IP:$Backup_Filename" "$Backup_Directory"
# Очистка резервної копії на MikroTik
sshpass -p "$MikroTik_Password" ssh "$MikroTik_User@$MikroTik_IP" /file remove "$Backup_Filename"
```

```
# Видалення старих резервних копій на локальному сервері
find "$Backup_Directory" -type f -mtime +7 -exec rm {} \;
```

Для працездатності цього скрипту потрібно було встановити пакет sshpass для автоматизації аутентифікації SSH.

З цим скриптом MikroTik створює резервні копії та зберігає їх на локальному сервері, комп'ютері системного адміністратора та на зовнішньому носії. У майбутньому скрипт буде покращено, за допомогою цього резервні копії будуть відправлятися на хмарне зберігання.

Для відновлення MikroTik за допомогою резервної копії потрібно відкрити WinBox (програмне забезпечення для налаштування роутерів MikroTik). Приклад наведено на рисунку 2.18.

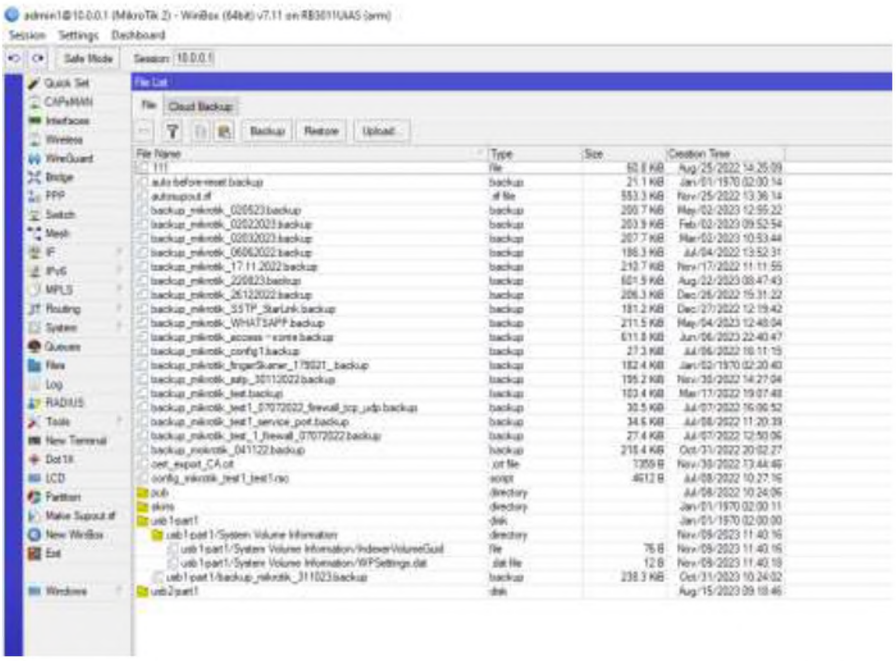

Рисунок 2.18 – Резервне відновлення с за допомогою носія інформації

Перейти на панель інструментів та натиснути на «Filles», після чого вибрати необхідний файл резервної копії, він обов’язково буде у форматі /.backup, та натиснути «Restore», після чого підтвердити відновлення. Коли роутер перезавантажився, потрібно перевірити відновлення. Приклад наведено на рисунку 2.19.

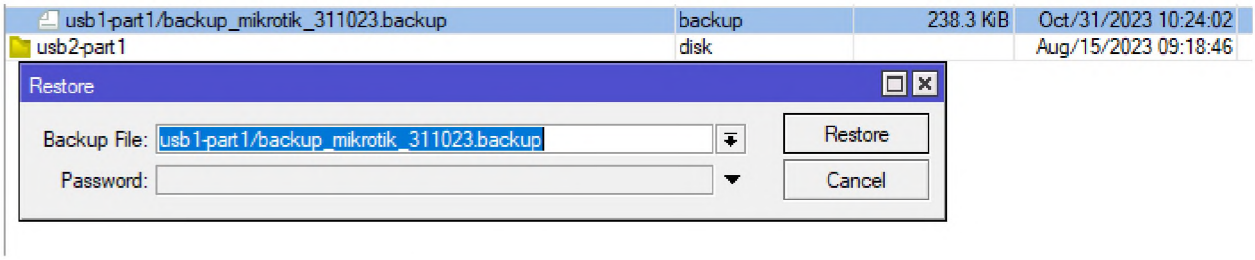

Рисунок 2.19 – Відновлення з допомогою backup

За допомогою кроків описаних вище можна з легкістю відновити маршрутизатор до потрібної версії. Також після закінчення роботи потрібно пам'ятати про ведення документації з налаштування роутера навіть після перевірки та інтеграції системи, усі важливі зміни, які будуть відбуватися в налаштуванні локальної мережі, краще за все записувати. На підприємстві використовують Google Таблиці, в яких ведеться документація про зміни на серверах, конфігурацію локальної мережі, адресацію IP, паролі та інші важливі дані, також задля безпеки існують резервні копії на зовнішніх носіях [37].

Висновки до розділу 2

У розділі розроблено структурну схему IP-адресації локальної мережі підприємства на основі керуючого маршрутизатора MikroTik. Обґрунтовано нормальну працездатність мережі шляхом розробки та перевірки функціонування у нормальному режимі імітаційної моделі ЛОМ у середовищі Cisco Packet Tracer, визначено склад обладнання мережі, зокрема проведено вибір комутаторів та маршрутизаторів. Запропонована у розділі побудова мережі із встановленням віртуальних підмереж забезпечила зручний механізм для боротьби з несанкціонованим доступом до службової інформації та збільшення продуктивності мережі.

РОЗДІЛ 3
РОЗРОБЛЕННЯ Й ДОСЛІДЖЕННЯ МОДЕЛІ БЕЗПЕКИ ТА БЕЗВІДМОВНОСТІ ЛОКАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

Надійність, безвідмовність та безпека є взаємопов'язаними поняттями. Надійна система, як правило, також буде безвідмовною і безпечною. Однак, це не завжди так. Наприклад, система може бути надійною, але не безвідмовною, якщо вона може відновитися після відмови. Або система може бути безвідмовною, але не зовсім безпечною, якщо вона не захищає свої активи від несанкціонованого доступу.

Забезпечення цих властивостей важливо не лише для забезпечення стабільності системи, але і для забезпечення довіри користувачів, ділової контингентності та відповідності регулятивним стандартам у сфері інформаційної безпеки [38].

3.1 Розрахунок показників безвідмовності локальної мережі

Розглянемо локальну мережу, представлену на рис.3.1. Мережа включає 10 комутаторів (позначені як vCDN), поєднаних лініями зв‘язку у визначеному порядку. На початковому етапі розрахунків ймовірністю відмови лінії зв‘язку можна знехтувати. Тоді безвідмовність мережі в цілому буде визначатися через показники безвідмовності віртуальних комутаторів [39].

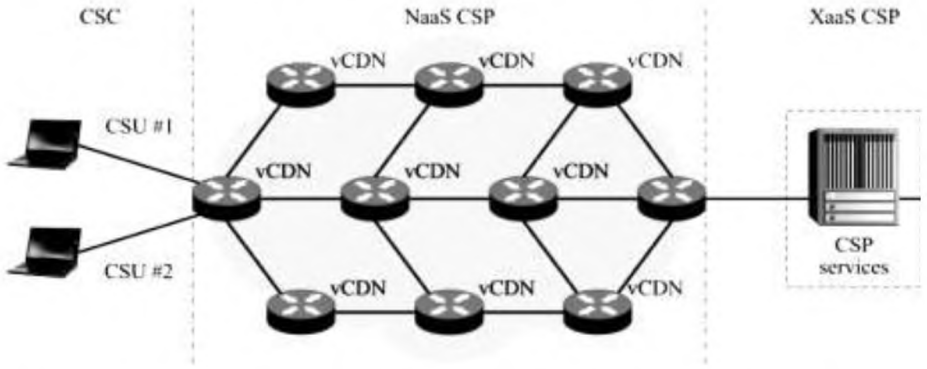

Рисунок 3.1 – Структурна схема надійності локальної мережі

Оскільки локальна мережа на рис. 3.1 має складну структуру, важко визначити її структурну схему надійності (ССН). Так очевидно, що елементи vCDN1 та vCDN10 для ССН мають послідовне підключення (оскільки їх відмова унеможливлює доставку пакетів до кінцевих пунктів). А от поєднання внутрішніх елементів важко показати на ССН, тому у роботі використано наступний підхід з визначення безвідмовності мережі. Мережа вважається працездатною за умови доставки повідомлень між елементами vCDN1 та vCDN10 у прямому та зворотному напрямках [40].

Враховуючи те, що структурна схема мережі не симетрична, необхідно розглянути окремо шляхи доставки повідомлень у цих напрямках (табл. 3.1 та табл. 3.2).

Таблиця 3.1 –Шляхи доставки повідомлень у прямому напрямку

1	vCDN1-vCDN2-vCDN5-vCDN8-vCDN10
2	vCDN1-vCDN2-vCDN5-vCDN3-vCDN7-vCDN10
3	vCDN1-vCDN2-vCDN5-vCDN3-vCDN6-vCDN9-vCDN10
4	vCDN1-vCDN3-vCDN5-vCDN8-vCDN10
5	vCDN1-vCDN3-vCDN7-vCDN10
6	vCDN1-vCDN3-vCDN6-vCDN9-vCDN10
7	vCDN1-vCDN4-vCDN6-vCDN9-vCDN10
8	vCDN1-vCDN4-vCDN6-vCDN3-vCDN7-vCDN10
9	vCDN1-vCDN4-vCDN6-vCDN3-vCDN5-vCDN8-vCDN10

Таблиця 3.2 – Шляхи доставки повідомлень у зворотному напрямку

1	vCDN10-vCDN8-vCDN5-vCDN2-vCDN1
2	vCDN10-vCDN8-vCDN5-vCDN3-vCDN1
3	vCDN10-vCDN8-vCDN7-vCDN3-vCDN1
4	vCDN10-vCDN8-vCDN7-vCDN9-vCDN6-vCDN4-vCDN1
5	vCDN10-vCDN7-vCDN3-vCDN1
6	vCDN10-vCDN7-vCDN8-vCDN5-vCDN2-vCDN1
7	vCDN10-vCDN7-vCDN9-vCDN6-vCDN4-vCDN1
8	vCDN10-vCDN7-vCDN9-vCDN6-vCDN4-vCDN1
9	vCDN10-vCDN9-vCDN5-vCDN2-vCDN1
10	vCDN10-vCDN8-vCDN5-vCDN3-vCDN1
11	vCDN10-vCDN8-vCDN7-vCDN3-vCDN1

Оскільки розглянуті шляхи доставки повідомлень в кожному з напрямків є альтернативними, то для ССН їх поєднання еквівалентно параллельному з‘єднанню. Поєднання підмножин комбінації прямого і зворотного напрямів для ССН еквівалентно послідовному з‘єднанню.

Всі елементи системи працюють у періоді нормальної експлуатації, тому ймовірність безвідмовної роботи елементів vCDN з 1 по 10 (рис. 3.1) підпорядковуються експоненціальному закону:

$$p_i(t) = \exp(-\lambda_i \cdot t) = \exp\left(-2,5 \cdot 10^{-4} \cdot t\right) \tag{3.1}$$

Оскільки всі vCDN відповідно до SLA мають однакову інтенсивність відмов, розрахункову формулу для визначення ймовірності безвідмовної роботи мережі можна спростити:

$$\begin{aligned} P_{NaaS} &= P_{\text{forward direction}} \cdot P_{\text{reverse direction}} = \\ &= \left[1-\left(1-p_i^{\,4}\right)\left(1-p_i^{\,5}\right)^4\left(1-p_i^{\,6}\right)^2\left(1-p_i^{\,7}\right)^2\right]\times \\ &\times\left[1-\left(1-p_i^{\,4}\right)\left(1-p_i^{\,5}\right)^6\left(1-p_i^{\,6}\right)^3\left(1-p_i^{\,7}\right)\right]. \end{aligned} \tag{3.2}$$

Результати обчислення функції безвідмовної роботи локальної мережі представлені у вигляді графіка на рис. 3.2.

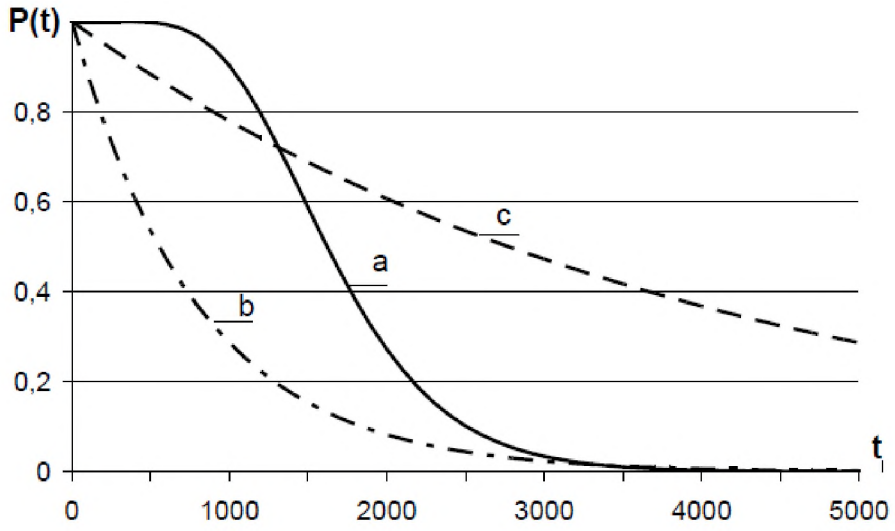

Рисунок 3.2 – Залежність безвідмовної роботи локальної мережі (a), п‘яти послідовно з‘єднаних vCDN (b) та одного vCDN (c)

Для порівняння на графік також винесені криві безвідмовності одного та п‘яти послідовно з‘єднаних vCDN.

Очевидно, що безвідмовність віртуальної мережі має виграш порівняно з одним елементом на інтервалі 0…1360 годин, а в подальшому не гірша безвідмовності ланцюжка з п‘яти послідовно з‘єднаних vCDN. Відповідно до цих результатів може буди обраховано середнє напрацювання до відмови:

$$T_{сер.} = \int_0^{\infty} P(t) \cdot dt \tag{3.3}$$

та інтенсивність відмов:

$$\lambda(t) = \frac{-P'(t)}{P(t)} \tag{3.4}$$

3.2 Розрахунок показників безвідмовності локальної мережі за її структурною схемою надійності

Розрахунок показників відмовостійкості локальної мережі зазвичай виконується в припущенні, що вся система і будь-який її компонент можуть перебувати тільки в одному з двох можливих станів (робочий і неробочий) і що відмови компонентів не залежать один від одного. Стан системи (працючий чи непрацездатний) визначається станом елементів та їх комбінацій. Тому безвідмовні розрахунки теоретично зводяться до пошуку всіх можливих комбінацій станів елементів, визначення ймовірності кожного елемента та додавання ймовірностей робочих станів системи. Цей метод (метод прямого сортування) є фактично універсальним і може використовуватися для будь-якої системи розрахунків.

Однак при великій кількості елементів системи n такий шлях стає нереальним через великий обсяг обчислень (наприклад, при n = 10 число

можливих станів системи $2^n = 1024$, при n=20 перевищує 10^6, при n=30 - більше 10^9). Тому на практиці використовують більш ефективні і економічні методи розрахунку, не пов'язані з великим обсягом обчислень. Можливість застосування таких методів пов'язана зі структурою ІТ-системи.

Більшість реальних ІТ-систем має складну комбіновану структуру, частина елементів якої утворює послідовне з'єднання, інша частина - паралельне, окремі гілки елементи або гілки структури утворюють мостові схеми або типу "m з n".

Прямі методи класифікації таких систем на практиці виявилися непрактичними. У цих випадках доцільніше спочатку розкласти систему на прості підсистеми (групи елементів), для яких відомі методи розрахунку надійності. Потім ці підсистеми в структурі надійності замінюються квазіелементами, ймовірності безвідмовної роботи яких дорівнюють ймовірностям безвідмовної роботи, розрахованими для цих підсистем. При необхідності цей процес можна виконати кілька разів, поки залишилися квазіелементи не сформують структуру, також відомі методи розрахунку їх надійності.

Структурна схема надійності наведена на рис 3.3. Значення інтенсивності відмов елементів дані в 10^{-6} 1/год.

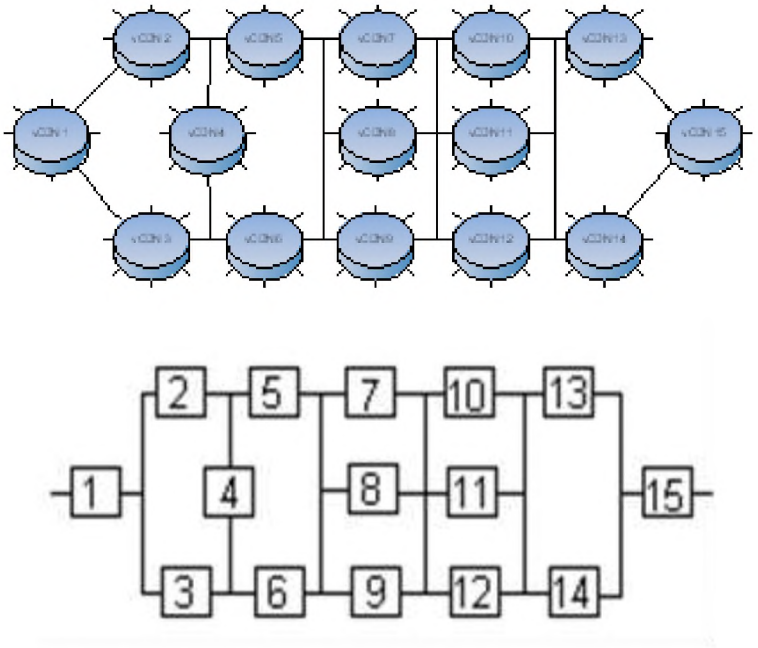

Рисунок 3.3 – Структурна схема надійності локальної мережі

$$\begin{aligned}
&\lambda_1 = 0{,}1\cdot 10^{-6}\ {}^{1}\!/_{\text{годин}}\\
&\lambda_2 = \lambda_3 = 1\cdot 10^{-6}\ {}^{1}\!/_{\text{годин}}\\
&\lambda_4 = 2\cdot 10^{-6}\ {}^{1}\!/_{\text{годин}}\\
&\lambda_5 = \lambda_6 = 1\cdot 10^{-6}\ {}^{1}\!/_{\text{годин}}\\
&\lambda_7 = \lambda_8 = \lambda_9 = 5\cdot 10^{-6}\ {}^{1}\!/_{\text{годин}}\\
&\lambda_{10} = \lambda_{11} = \lambda_{12} = 3\cdot 10^{-6}\ {}^{1}\!/_{\text{годин}}\\
&\lambda_{13} = \lambda_{14} = 1\cdot 10^{-6}\ {}^{1}\!/_{\text{годин}}\\
&\lambda_{15} = 0{,}05\cdot 10^{-6}\ {}^{1}\!/_{\text{годин}}
\end{aligned} \qquad (3.5)$$

Елементи 2, 3, 4, 5 і 6 утворюють (рис. 3.4) мостикову систему, яку можна замінити квазіелементом А.

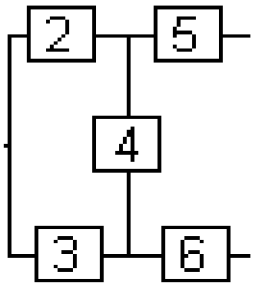

Рисунок 3.4 – Мостикова схема

Мостикова структура (рис.3.4) не зводиться до паралельного або послідовного типу з'єднання елементів, а являє собою паралельне з'єднання послідовних ланцюжків елементів з діагональними елементами, включеними між вузлами різних паралельних гілок (елемент 3 на рис. 3.5 а, елементи 3 і 6 на рис. 3.5 б). Працездатність такої системи визначається не тільки кількістю відмовили елементів, але і їх становищем у структурній схемі. Наприклад, працездатність системи, схема якої приведена на рис. 3.5 а, буде втрачена при одночасному відмову елементів 1 і 2, або 4 і 5, або 2, 3 і 4 і т.д. У той же час відмова елементів 1 і 5, або 2 і 4, або 1, 3 і 4, або 2, 3 і 5 до відмови системи не призводить.

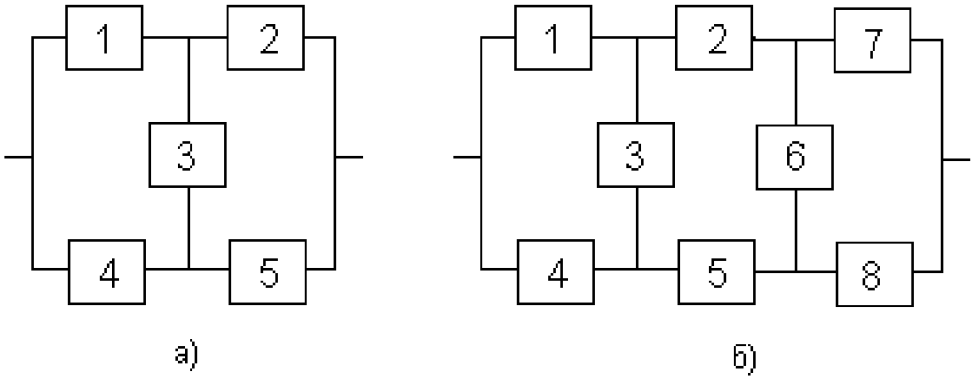

Рисунок 3.5 – Мостикова структура

Для розрахунку надійності мостікових систем можна скористатися методом прямого перебору, як це було зроблено для систем "m з n", але при аналізі працездатності кожного стану системи необхідно враховувати не тільки число відмовили елементів, але і їх положення в схемі. Імовірність безвідмовної роботи системи визначається як сума ймовірностей всіх працездатних станів:

$$\begin{aligned} P = {} & p_1p_2p_3p_4p_5 + p_1p_2p_3p_4q_5 + p_1p_2p_3q_4p_5 + p_1p_2q_3p_4p_5 + \\ & + p_1q_2p_3p_4p_5 + q_1p_2p_3p_4p_5 + p_1p_2q_3p_4q_5 + p_1q_2p_3p_4q_5 + \\ & + q_1p_2p_3p_4q_5 + p_1p_2q_3q_4p_5 + p_1q_2p_3q_4p_5 + q_1p_2p_3q_4p_5 + \\ & + p_1q_2q_3p_4p_5 + q_1p_2q_3p_4p_5 + q_1q_2q_3p_4p_5 + p_1q_2q_3p_4q_5. \end{aligned} \tag{3.6}$$

У разі рівнонадійних елементів:

$$P = p^5 + 5p^4q + 8p^3q^2 + 2p^2q^3 = 2p^5 - 5p^4 + 2p^3 + 2p^2. \tag{3.7}$$

Для розрахунку ймовірності безвідмовної роботи скористаємося методом розкладання щодо особливого елемента в якості якого виберемо елемент 4, тоді

$$\begin{aligned} p_A = {} & p_4\left[1-(1-p_2)(1-p_3)\right]\cdot\left[1-(1-p_5)(1-p_6)\right] + \\ & + (1+p_4)\left[1-(1-p_2p_5)(1-p_3p_6)\right] \end{aligned} \tag{3.8}$$

Розрахунок безвідмовності паралельно з‘єднаних елементів

Системою з паралельним з'єднанням елементів називається система, відмова якої відбувається тільки в разі відмови всіх її елементів . Такі схеми надійності характерні для ТС, в яких елементи дублюються або резервуються, тобто паралельне з'єднання використовується як метод підвищення надійності. Однак такі системи зустрічаються і самостійно (наприклад, системи двигунів

чотиримоторного літака або паралельне включення діодів в потужних випрямлячах) [41].

Для відмови системи з паралельним з'єднанням елементів протягом напрацювання t необхідно і достатньо, щоб всі її елементи відмовили протягом цього напрацювання. Так що відмова системи полягає в спільному відмову всіх елементів, ймовірність чого (при допущенні незалежності відмов) може бути знайдена по теоремі множення ймовірностей як твір ймовірностей відмови елементів:

$$Q = q_1 q_2 \ldots q_n = \prod_{i=1}^{n} q_i = \prod_{i=1}^{n} (1 - p_i). \tag{3.9}$$

Відповідно, ймовірність безвідмовної роботи:

$$P = 1 - Q = 1 - \prod_{i=1}^{n} q_i = 1 - \prod_{i=1}^{n} (1 - p_i). \tag{3.10}$$

Для систем з рівнонадійних елементів ($p_i = p$):

$$Q = q^n \quad , \quad P = 1 - (1 - p)^n, \tag{3.11}$$

тобто надійність системи з паралельним з'єднанням підвищується при збільшенні числа елементів (наприклад, при $p = 0.9$ и $n = 2$ $P = 0.99$, а при $n = 3$ $P = 0.999$).

Елементи 7,8 і 9 утворюють паралельне з'єднання, замінивши яке елементом B і враховуючи, що $p_7 = p_8 = p_9$, отримаємо:

$$p_B = 1 - (1 - p_7)(1 - p_8)(1 - p_9) \tag{3.12}$$

Елементи 10,11 і 12 також утворюють паралельне з'єднання, замінивши яке елементом C отримаємо

$$p_c = 1 - (1 - p_{10})(1 - p_{11})(1 - p_{12}) \tag{3.13}$$

Елементи 13 і 14 утворюють паралельне з'єднання. Замінюємо їх елементом D, для якого при $p_{13} = p_{14}$, отримаємо:

$$p_D = 1 - q_{13} q_{14} = 1 - q_{13}^2 = 1 - (1 - p_{13})^2 \tag{3.14}$$

Після перетворень схема зображена на рис. 3.6.

Рисунок 3.6 – Перетворена схема

Система з послідовно з'єднаними компонентами – це система, в якій відмова будь-якого одного компонента спричинить відмову всієї системи. Таке поєднання технічних елементів зустрічається найчастіше і тому називається первинною ланкою.

В системі з послідовним з'єднанням для безвідмовної роботи протягом деякого напрацювання t необхідно і досить, щоб кожен з її n елементів працював безвідмовно протягом цієї напрацювання. Вважаючи відмови елементів незалежними, ймовірність одночасної безвідмовної роботи n елементів визначається по теоремі множення ймовірностей: ймовірність спільного появи незалежних подій дорівнює добутку ймовірностей цих подій:

$$P(t) = p_1(t)p_2(t)\dots p_n(t) = \prod_{i=1}^{n} p_i(t) = \prod_{i=1}^{n}(1-q_i(t)) \qquad (3.15)$$

(далі аргумент t в дужках, що показує залежність показників надійності від часу, опускаємо для скорочення записів формул). Відповідно, ймовірність відмови такий ТЗ:

$$Q = 1 - P = 1 - \prod_{i=1}^{n} p_i = 1 - \prod_{i=1}^{n}(1-q_i). \qquad (3.16)$$

Якщо система складається з рівнонадійних елементів ($p_i = p$), то

$$P = p_i^n, \quad Q = 1-(1-q)^n. \qquad (3.17)$$

У перетвореній схемі (рис. 3.4) елементи 1, A, B, C, D і F утворюють послідовне з'єднання. Тоді ймовірність безвідмовної роботи всієї системи.

$$P = p_1 p_A p_B p_C p_D p_{15} \qquad (3.18)$$

Оскільки за умовою всі елементи системи працюють у періоді нормальної експлуатації, то ймовірність безвідмовної роботи елементів з 1 по 15 (рис. 3.1) підпорядковуються експоненціальним законом:

$$p_i = \exp(-\lambda_i t). \qquad (3.19)$$

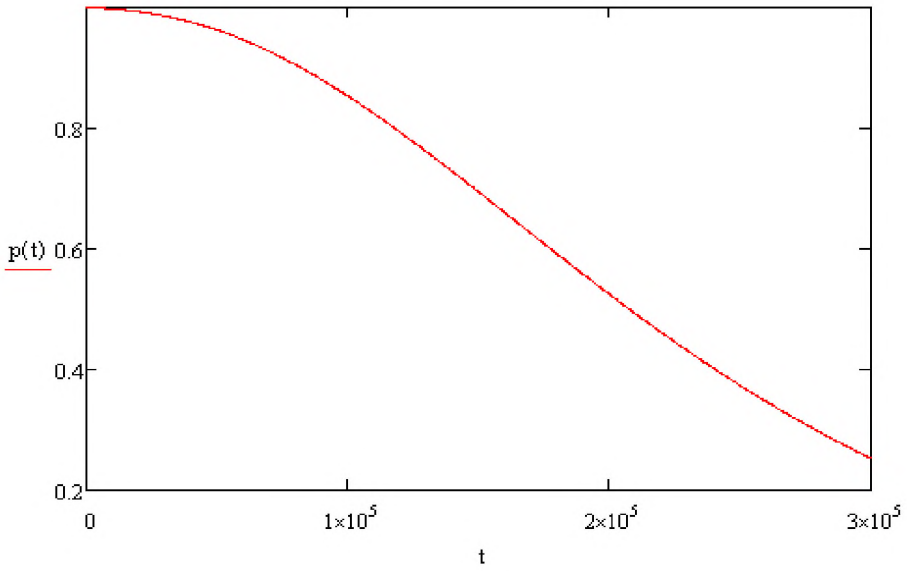

Рисунок 3.7 – Графік залежності ймовірності безвідмовної роботи системи P від часу (напрацювання) t

На рис. 3.7. представлений графік залежності ймовірності безвідмовної роботи системи P від часу напрацювання t.

3.3 Підвищення показників безвідмовності локальної мережі за рахунок більш надійних елементів

За графіком (рис. 3.8, крива P) знаходимо для $\gamma = 80\%$ $(P_\gamma = 0.8)$ γ - процентне напрацювання системи $T_\gamma = 1.1885 \cdot 10^5$ год.

Перевірочний розрахунок при $t = 1.1885 \cdot 10^5$ год показує, що $P_\gamma = 0.797 \approx 0.8$

За умовами завдання необхідно забезпечити підвищення γ - процентного напрацювання системи до $T_\gamma' = 1.5 \cdot T_\gamma = 1.5 \cdot 1.1885 \cdot 10^5 = 1.782 \cdot 10^5$ год.

Розрахунок показує, що при $t = 1.172 \cdot 10^5$ год для елементів перетвореної схеми $p_1 = 0.982$, $p_A = 0.854$, $p_B = 0.795$, $p_C = 0.929$, $p_D = 0.973$ и $p_{15} = 0.991$. Отже, із п’яти послідовно з'єднаних елементів мінімальне значення ймовірності

безвідмовної роботи має елемент В і саме збільшення його надійності дасть максимальне збільшення надійності системи в цілому. А також збільшимо надійність елемента С.

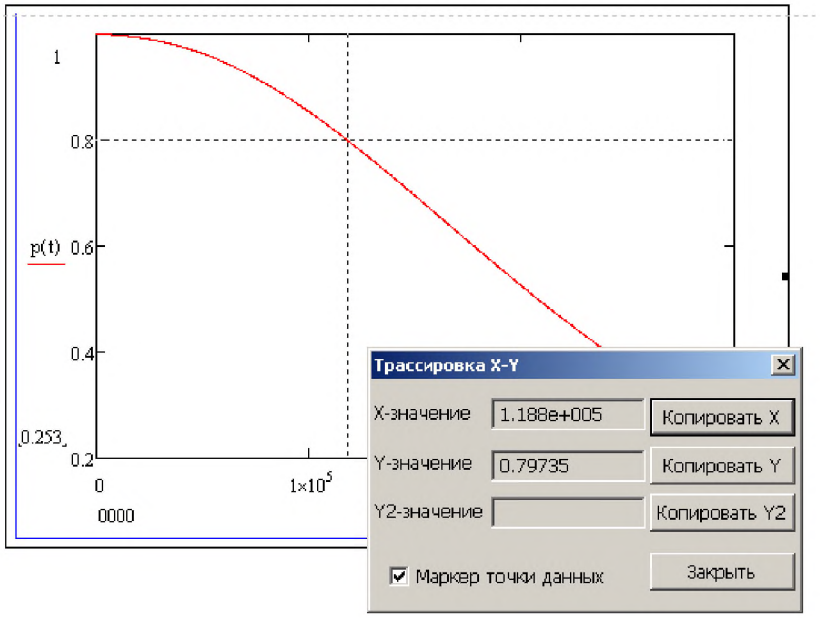

Рисунок 3.8 – γ - процентне напрацювання системи

Для того, щоб при $T_\gamma^{'} = 1.782 \cdot 10^5$ год система в цілому мала ймовірність безвідмовної роботи $P_\gamma = 0.8$, необхідно, щоб елементи В і С мали ймовірність

$$p_{B,C} = \frac{p_\gamma}{p_A p_1 p_D p_{15}} = \frac{0.8}{0.854 \cdot 0.982 \cdot 0.973 \cdot 0.991} = 0.988 \qquad (3.20)$$

$$\text{dpb} := \sqrt{\text{dpbpc}} = 0.994 \qquad (3.21)$$

безвідмовної роботи,

Очевидно, значення $p_{B,C}$, є мінімальним для виконання умови збільшення напрацювання не менше, ніж в 1.5 рази, при більш високих значеннях $p_{B,C}$ збільшення надійності системи буде більшим [44].

Для визначення мінімально необхідної ймовірності безвідмовної роботи елементів 7 - 12 (рис. 3.3) необхідно розв‘язати рівняння $p_B = 1 - (1 - p_7)(1 - p_8)(1 - p_9)$ відносно p_7 при $p_{B,C} = 0{,}994$.

$$\text{dpx} := 1 - \sqrt[3]{1 - \text{dpb}} = 0.818 \qquad (3.22)$$

Оскільки за умовами завдання всі елементи працюють у періоді нормальної експлуатації і підлягають експоненціальним законом, то для елементів 7 - 12 при $t = 1.172 \cdot 10^5$ год знаходимо

$$\lambda'_7 = \lambda'_8 = \lambda'_9 = \lambda'_{10} = \lambda'_{11} = \lambda'_{12} = -\frac{\ln p_7}{t} = -\frac{\ln 0.818}{1.172 \cdot 10^5} = 1.125 \cdot 10^6 \text{ год}^{-1} \qquad (3.23)$$

Таким чином, для збільшення γ - процентного напрацювання системи необхідно збільшити надійність елементів 7, 8, 9,10,11 і 12 і знизити інтенсивність їх відмов з 3 до $1.125 \cdot 10^{-6}$ год$^{-1}$, тобто в 2.66 рази.

При $t = 1.172 \cdot 10^5$ год ймовірність безвідмовної роботи системи $P' = 0.80005 \approx 0.8$, що відповідає умовам завдання. Графік наведено на рис 3.9.

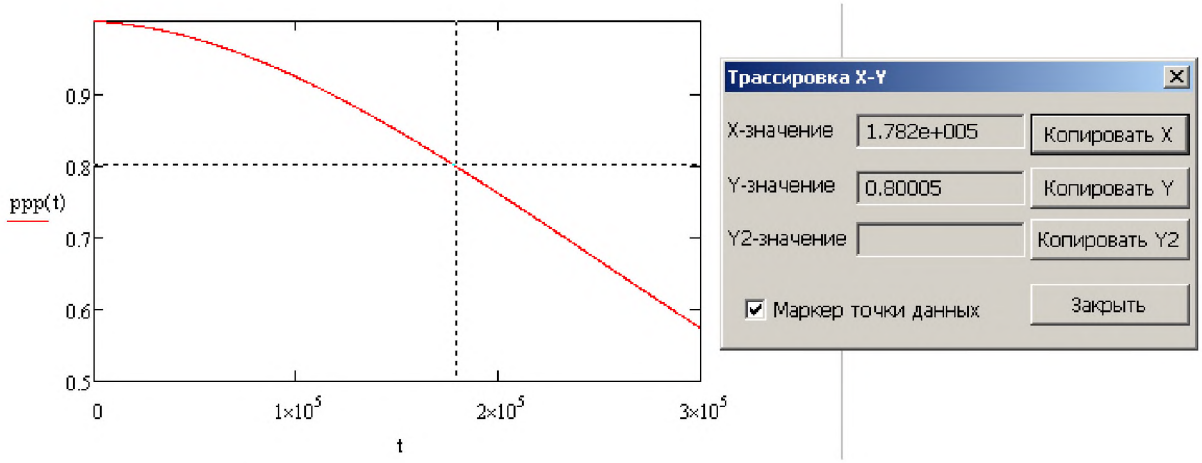

Рисунок 3.9 – Ймовірність безвідмовної роботи системи при $t = 1.172 \cdot 10^5$ год

3.4 Підвищення показників безвідмовності локальної мережі за рахунок зміни структурної схеми надійності

Для другого способу збільшення ймовірності безвідмовної роботи системи - структурного резервування також вибираємо елементи B і C, імовірність безвідмовної роботи яких після резервування повинна бути не нижче $p''_{B,C} = 0.994$

Для елементів системи B і C - резервування означає збільшення загального

числа елементів. Аналітично визначити мінімально необхідну кількість елементів неможливо, тому число елементів має бути цілим і функція $p_F = f(n)$ дискретна.

Для підвищення надійності системи додаємо до неї елементи, ідентичні по надійності вихідним елементам 7 - 9 і 10-12, до тих пір, поки ймовірність безвідмовної роботи квазіелементом В і С не досягне заданого значення.

Для розрахунку скористаємося формулами для розрахунку ймовірності безвідмовної роботи систем типу "m з n".

До системи В додаємо елементи 16-22, отримуємо систему “1 із 10”:

$$p16(t) := 1 - (1 - p10(t))^6 \qquad (3.24)$$

До системи С добавляємо елемент 23-25, отримуємо систему “1 із 6”:

$$p16(t2) = 0.995 > 0.994 \qquad (3.25)$$

Таким чином, для підвищення надійності до необхідного рівня необхідно у вихідній схемі (рис.3.3) систему В добудувати елементами 16, 17,18,19,20,21 і 22 до системи “1 з 10” (рис. 3.10). А також систему С добудувати елементами 23,24 і 25 до системи “1 з 6” (рис. 3.10) [45].

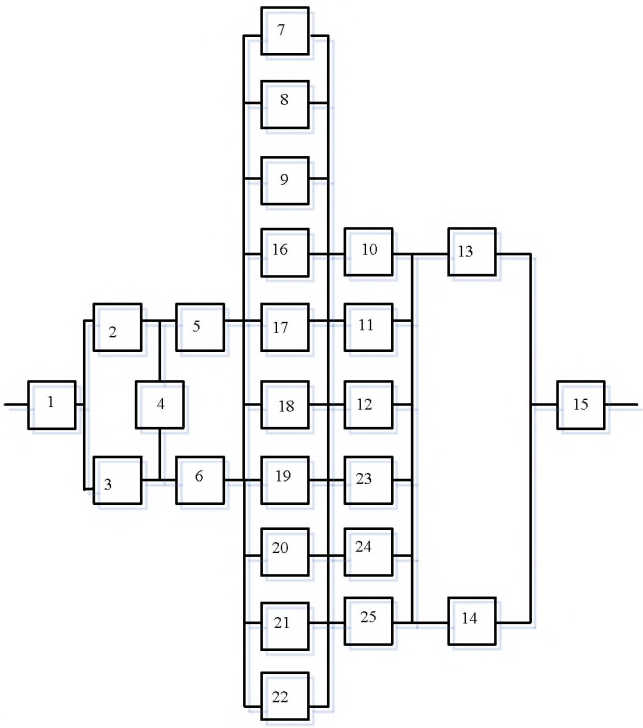

Рисунок 3.10 – Схема локальної мережі після структурного резервування

Розрахунки показують, що при $t = 1.172 \cdot 10^5$ год $P'' = 0.8076 > 0.8$, що відповідає умові завдання.

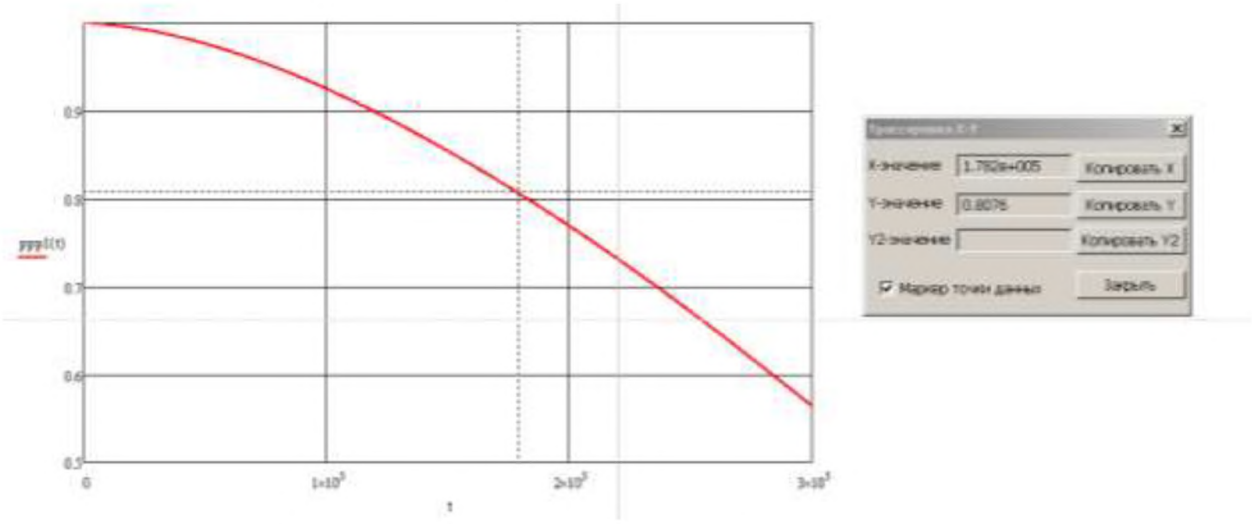

Рисунок 3.11 – Ймовірність безвідмовної роботи системи $t = 1.172 \cdot 10^5$ год. після структурного резервування.

На рис. 3.12 нанесені криві залежностей ймовірності безвідмовної роботи системи до (крива P)та після підвищення надійності елементів 7 - 12 (крива P') і після структурного резервування (крива P'').

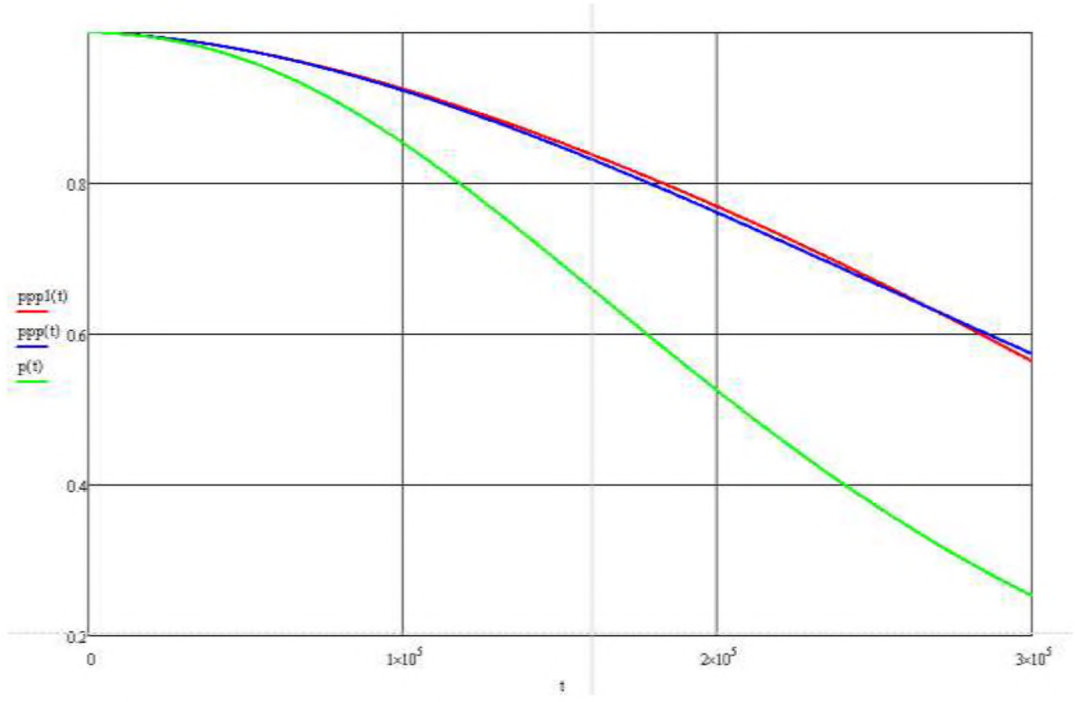

Рисунок 3.12 – Криві залежностей ймовірності безвідмовної роботи системи

3.5 Економічне обґрунтування модернізації локальної мережі підприємства

Економічне обґрунтування модернізації локальної мережі підприємства ґрунтується на ряді факторів, які впливають на продуктивність, ефективність та загальні витрати. При модернізації локальної мережі підприємства враховувались такі фактори:

1) Підвищення продуктивності праці, швидший доступ до ресурсів, оновлення обладнання та інфраструктури покращить швидкість доступу до мережевих ресурсів, що в свою чергу призведе до збільшення продуктивності праці співробітників. Оптимізація робочих процесів, висока швидкість передачі даних та покращена надійність мережі сприятиме оптимізації робочих процесів, зменшенню часу очікування та покращенню загальної ефективності робочого середовища;

2) Зменшення витрат на обслуговування, зменшення ризику відмов, актуалізація обладнання зменшить ризик відмов та підвищить стійкість мережі, що в свою чергу зменшить витрати на її обслуговування та ремонт. Зменшення часу простою, модернізація покращать загальну надійність системи та зменшать час простою, що важливо для продуктивності підприємства;

3) Збільшення безпеки, захист від кіберзагроз, сучасні мережеві технології можуть надати більший рівень захисту від кіберзагроз, що важливо для збереження конфіденційності та цілісності даних підприємства. Моніторинг та аудит безпеки: Оновлені мережеві рішення можуть надавати більше можливостей для моніторингу та аудиту безпеки, що дозволяє швидше виявляти та виправляти потенційні загрози;

4) Підготовка до майбутніх потреб. Маштабованість та гнучкість. Модернізована мережа може легше маштабуватися та адаптуватися до змін у розмірі підприємства та вимог до мережі.

Підтримка нових технологій. Оновлення дозволить використовувати нові технології та інновації, що може бути важливим для конкурентоспроможності підприємства;

5) Оптимізація витрат та енергоефективність. Сучасне обладнання часто є більш енергоефективним, що може призвести до зменшення витрат на електроенергію та, відповідно, до зменшення витрат на утримання мережі.

Модернізація локальної мережі призведе до покращення продуктивності, зниження витрат та підвищення загальної конкурентоспроможності підприємства.

Перед початком модернізації були зроблені економічні підрахунки, щоб переконатися в доцільності апгрейду.

Етап 1. Оцінка затрат на інформаційні технології. На даному етапі визначається обсяг інвестицій в інформаційні технології необхідний для досягнення поставлених цілей.

Оцінка витрат на інформаційні технології здійснюється в свою чергу в два етапи:

Оцінювання витрат проекту прогнозує визначення всіх капітальних і поточних витрат, поєднаних із впровадженням, а саме:

а) оцінка прямих витрат визначається за формулою:

$$B_П = B_{ТЗ} + B_{ППЗ} + B_{ОП} + B_{ВСЗ} + B_{ПСП} + B_У + B_{РПЗ} + B_I, \quad (3.25)$$

де:

$B_{ТЗ}$ – купівля управляючого комутатора MikroTik;

$B_{ППЗ}$ – купівля серверної Windows Server 2019;

$B_{ОП}$ – закупівля сучасної серверної стійки;

$B_{ВСЗ}$ – соціальні заходи, не потрібні для модернізації локальної мережі;

$B_{ПСП}$ – стороні підприємства відсутні;

$B_У$ – підключення та проведення інтернету 5000 грн, також потрібна оплата тарифного плану 900 грн/міс. Річна плата становить 10800 грн;

$B_{РПЗ}$ – усе програмне забезпечення, окрім операційної системи, є безкоштовним;

B_I – навчання персоналу (тренінги про безпеку в локальній мережі) 4000 грн

$$B_П = =21,789+16,000+30,000+0+0+10,800+0+4000=82,589$$

б) Оцінка непрямих витрат на проект упровадження, який визначається за формулою, грн:

$$B_Н = B_{Н1} + B_{Н2}, \quad (3.26)$$

де $B_{Н1}$ – витрати, пов'язані з простоями, тобто вихід з ладу управляючого комутатора, 4000грн за тестування;

$B_{Н2}$ – витрати, пов'язані з людським фактором, наприклад, пошкодження кабелю Ethernet, 100 грн за заміну.

Результат обчислень за формулою (3.2): $B_Н = 4000+100=4,100$

в) Оцінка витрат на обслуговування мережі за період її життєвого циклу.

$$B_{УТР} = B_{ОП} + B_{ВСЗ} + B_П + B_І, \quad (3.27)$$

де $B_{ОП}$ – витрати на оплату зарплатні системному адміністратору;

$B_{ВСЗ}$ – соціальні заходи не використовувались;

$B_П$ – оцінка непрямих витрат;

$B_І$ – витрати на вдосконалення мережі 8000 грн.

Результати обчислень за формулою (3.3):

$$B_{УТР} =12,000+0+82,589+8000=102,589$$

Визначення загальних витрат на проєкт буде розраховуватися за формулою:

$$B_{ІТ}=B_П+B_Н+B_{УТР}, \quad (3.28)$$

Результати обчислень за формулою (3.4):

$$B_{ІТ} = 82,589+4,100+102,589=189,278$$

Етап 2. Оцінка вимог використання інформаційних технологій.

Упровадження проєкту на підприємстві виконується за допомого

результатів операційної діяльності, які здійснюється помісячно. Приклад показано в табл.3.3.

Таблиця 3.3 – Операційна діяльність по проекту

Показники	Значення на кроці, тис. грн.	
	1	2
1. Ціна, грн./ш	23.000	23.000
2. Виручка, тис. грн.	80.000	80.000
4. Постійні витрати, тис. грн.	900	900
5. Амортизація устаткування, тис. грн.	1.200	1.200
7. Результат від операційної діяльності, тис. грн.	43.256	43.256

Дохід оподаткування розраховується за формулою:

$$\text{Пр} = \text{Виручка} - \text{Затрати} = 443{,}000\text{-}189{,}278 = 253{,}722. \quad (3.29)$$

Податок на приріст:

$$\text{Под} = \text{Пр} \cdot \text{Ст}_{\text{под}} = \quad 253{,}722*0.25 = 63{,}430. \quad (3.30)$$

де: $Cm_{под}$ – ставка податку на приріст використовує стале значення 0,25

Чистий приріст складе:

$$\text{Прч} = \text{Пр} - \text{Под} = 253{,}722 - 63{,}430 = 190{,}292. \quad (3.31)$$

Підсумок операційної діяльності буде складати:

$$CF_2(t) = \text{Пр}_\text{ч} + \text{А} = 190{,}292 + 4{,}300 = 194{,}592. \quad (3.32)$$

Для розробки, упровадження та навчання персоналу доменного серверу потрібні затрати підприємству на даний момент 48.600 грн.

Етап 3. На цьому етапі ми розрахуємо економічну ефективність проекту по створенню локальної мережі. Потрібно розрахувати чисту вартість при одноразовому здійснені інвестиційних витрат на початку здійснення проєкту. Розрахування буде здійснюватися за допомогою формули :

$$\text{NPV} = \sum_{t=1}^{n} \frac{CF_t}{(1+i)^t} - \text{INV}_0. \quad (3.33)$$

Результат розрахунку за формулою (3.9): $\text{NPV} = \sum_{t=1}^{n} \frac{194{,}592_1}{(1+25)^1} - \text{INV}_0 = 73{,}435.$

Наступним кроком буде показник бухгалтерської рентабельності інвестиційного проекту (ROI):

$$ROI = \frac{AP}{(INV_1 + INV_2)/2} * 100 \qquad (3.34)$$

$$ROI = \frac{194{,}592}{(189{,}278_1 + 189{,}278_2)/2} * 100 = 204{,}126.$$

Отже, для розробки, упровадження та адміністрування серверу компанії доведеться витратити 189,278 грн, щоб упорядкувати систему облікових записів та контролю за безпекою інформації.

Висновки до розділу 3

У третьому розділі було розглянуто залежність між безпекою локальної мережі та безвідмовністю її елементів. Розроблено модель оцінювання безвідмовності локальної мережі без використання та на основі структурної схеми надійності. Обґрунтовано основні завдання щодо розробки моделі функціонування елементів локальної мережі та оцінювання їх надійності, розраховано функції безвідмовності мережі з заданою топологією для оцінювання надійності та безпеки.

Результати обчислення функції безвідмовної роботи локальної мережі показали, що безвідмовність мережі має виграш порівняно з одним елементом на інтервалі 0…1360 годин, а в подальшому не гірша безвідмовності ланцюжка з п‘яти послідовно з‘єднаних комутаторів. Визначено, що для збільшення γ - процентного напрацювання системи необхідно збільшити надійність елементів 7, 8, 9,10,11 і 12 і знизити інтенсивність їх відмов з 3 до 1,125e-6, тобто в 2.66 рази. Або використати альтернативний варіант і систему В добудувати елементами 16, 17,18,19,20,21 і 22 до системи “1 з 10”. У розділі виконано економічне обґрунтування модернізації локальної мережі підприємства, яке ґрунтується на ряді факторів, що впливають на продуктивність, ефективність та загальні витрати.

ВИСНОВКИ

У процесі виконання роботи її мета була досягнута, а завдання вирішені. Було проаналізовано основні джерела за темою дослідження і розкриті основні етапи проєктування та розгортання локальної мережі підприємства. Забезпечення безпеки мережі потребує постійної роботи та ретельної уваги до деталей.

Розглянуто питання вимог до забезпечення безпеки локальної обчислювальної мережі підприємства. Безпека мережі є невід'ємною частиною безпеки підприємства, беручи до уваги те, що зараз майже кожен відділ підприємства використовує локальну або глобальну мережу, вони знаходяться в зоні ризику. Під час побудови мережі потрібно звернути велику увагу саме на безпеку. У мережі інтернет є багато рекомендацій, як можна покращити безпеку локальної мережі підприємств, але велику кількість рекомендацій не можливо втілити в життя, не маючи гарного апаратного чи програмного забезпечення. Тому при побудові мережі потрібно враховувати засоби, які допоможуть у налаштуванні мережі. Управляючий роутер MikroTik має всі необхідні варіанти для забезпечення безпеки мережі. На роутері MikroTik є можливість навіть програмувати, так як він має у своєму програмному забезпеченні інтерфейс командного рядку, за допомогою якого можна писати скрипти та налаштовувати роутер за своїми вподобаннями.

Розроблено структурну схему IP-адресації локальної мережі підприємства на основі керуючого маршрутизатора MikroTik. Обґрунтовано нормальну працездатність мережі шляхом розробки та перевірки функціонування у нормальному режимі імітаційної моделі ЛОМ у середовищі Cisco Packet Tracer, визначено склад обладнання мережі, зокрема проведено вибір комутаторів та маршрутизаторів. Запропонована у роботі побудова мережі із встановленням віртуальних підмереж забезпечила зручний механізм для боротьби з несанкціонованим доступом до службової інформації та збільшення продуктивності мережі.

Було розглянуто залежність між безпекою локальної мережі та безвідмовністю її елементів. Розроблено модель оцінювання безвідмовності локальної мережі без використання та на основі структурної схеми надійності. Обґрунтовано основні завдання щодо розробки моделі функціонування елементів локальної мережі та оцінювання їх надійності, розраховано функції безвідмовності мережі з заданою топологією для оцінювання надійності та безпеки.

Результати обчислення функції безвідмовної роботи локальної мережі показали, що безвідмовність мережі має виграш порівняно з одним елементом на інтервалі 0…1360 годин, а в подальшому не гірша безвідмовності ланцюжка з п‘яти послідовно з‘єднаних комутаторів. Визначено, що для збільшення γ - процентного напрацювання системи необхідно збільшити надійність елементів 7, 8, 9,10,11 і 12 і знизити інтенсивність їх відмов з 3 до 1,125e-6, тобто в 2.66 рази. Або використати альтернативний варіант і систему В добудувати елементами 16, 17,18,19,20,21 і 22 до системи “1 з 10”. У розділі виконано економічне обґрунтування модернізації локальної мережі підприємства, яке ґрунтується на ряді факторів, що впливають на продуктивність, ефективність та загальні витрати.

Таким чином, поставлені задачі розв‘язано у повному обсязі. Напрямком подальших досліджень є адаптація розробленої моделі безвідмовності локальної мережі для врахування параметрів дротових, оптоволоконних та бездротових зв‘язків між вузлами мережі.