Міністерство освіти і науки України

Відокремлений структурний підрозділ «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя»
(повне найменування вищого навчального закладу)

Відділення телекомунікацій та електронних систем
(назва відділення)

Циклова комісія комп'ютерної інженерії
(повна назва циклової комісії)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

бакалавра
(освітній ступінь)

на тему: **Розробка проєкту комп'ютерної мережі Івано-Франківського відділення Львівської філії АБ «Експрес-Банк»**

Виконав: студент VII курсу, групи КІб-703

Спеціальності **123 Комп'ютерна інженерія**
(шифр і назва спеціальності)

_____ Василь ДЖЕРДЖ
(ім'я та прізвище)

Керівник Андрій ЛЯПАНДРА
(ім'я та прізвище)

Рецензент _____
(ім'я та прізвище)

Тернопіль – 2026

ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ТЕРНОПІЛЬСЬКИЙ ФАХОВИЙ КОЛЕДЖ
ТЕРНОПІЛЬСЬКОГО НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
імені ІВАНА ПУЛЮЯ»

Відділення телекомунікацій та електронних систем
Циклова комісія комп'ютерної інженерії
Освітній ступінь бакалавр
Освітньо-професійна програма: Комп'ютерна інженерія
Спеціальність: 123 Комп'ютерна інженерія
Галузь знань: 12 Інформаційні технології

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"18" травня 2026 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Джерджу Василю Івановичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи **Розробка проєкту комп'ютерної мережі Івано-Франківського відділення Львівської філії АБ «Експрес-Банк».**

керівник роботи Ляпандра Андрій Степанович
(прізвище, ім'я, по батькові)

затверджені наказом Відокремленого структурного підрозділу «Тернопільський фаховий коледж Тернопільського національного технічного університетут імені Івана Пулюя» від 18.05.2026р №4/9-252.

2. Строк подання студентом роботи: 22 червня 2026 року.

3. Вихідні дані до роботи: плани приміщень, завдання на проектування, стандарти побудови СКС, документація на мережеве обладнання і сервери

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): Загальний розділ. Розробка технічного та робочого проєкту. Спеціальний розділ. Економічний розділ. Безпека життєдіяльності, основи охорони праці.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): План приміщень. Логічна топологія. Фізична топологія. Таблиця IP-адрес. Таблиця техніко-економічних показників. Модель мережі

6. Консультанти розділів роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Ірина ЛЕЩИК Методист, викладач		
Безпека життєдіяльності, основи охорони праці	Володимир ШТОКАЛО викладач		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	18.05	
2	Збір і узагальнення інформації	21.05	
3	Написання першого розділу	25.05	
4	Розробка технічного та робочого проекту	1.06	
5	Написання спеціального розділу	8.06	
6	Розрахунок економічної частини	11.06	
7	Написання розділу охорони праці	12.06	
8	Виконання графічної частини	14.06	
9	Оформлення проекту	18.06	
10	Погодження нормоконтролю	19.06	
11	Попередній захист роботи	22.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 18 травня 2026 року

Студент _____ Василь ДЖЕРДЖ
(підпис) (ім'я та прізвище)

Керівник роботи _____ Андрій ЛЯПАНДРА
(підпис) (ім'я та прізвище)

АНОТАЦІЯ

Джердж Василь. Розробка проєкту комп'ютерної мережі Івано-Франківського відділення Львівської філії АБ «Експрес-Банк»: кваліфікаційна робота на здобуття освітнього ступеня бакалавра за спеціальністю 123 Комп'ютерна інженерія. – Тернопіль: ВСП «ТФК ТНТУ», 2026. – 93с.

В кваліфікаційній роботі розроблено проєкт локальної комп'ютерної мережі Івано-Франківського відділення Львівської філії АБ «Експрес-Банк» та налаштування корпоративної мережі для об'єднання банківських відділень. Для побудови мережевої інфраструктури використано технологію Gigabit Ethernet IEEE 802.3ab. Проєктом передбачено організацію захищеного обміну даними між вузлами мережі із застосуванням засобів шифрування та використанням програмного забезпечення Open Source. Розроблено фізичну і логічну топології мережі та виконано моделювання роботи мержі.

Ключові слова: комп'ютерна мережа, корпоративна мережа, шифрування даних, Gigabit Ethernet, Open Source, VLAV.

ABSTRACT

Vasyl Dzherdzh. Development of a Computer Network Project for the Ivano-Frankivsk Branch of the Lviv Regional Branch of JSC "Express-Bank": Bachelor's Qualification Thesis in Specialty 123 Computer Engineering. – Ternopil: Separate Structural Unit "Ternopil Applied College of Ternopil Ivan Puluj National Technical University", 2026. – 93p.

The qualification thesis presents the development of a local computer network for the Ivano-Frankivsk Branch of the Lviv Regional Branch of JSC "Express-Bank" and the configuration of a corporate network for interconnecting the bank's branches. Gigabit Ethernet IEEE 802.3ab technology was used to build the network infrastructure. The project provides secure data exchange between network nodes through the use of encryption mechanisms and Open Source software. The physical and logical network topologies were designed, and the network operation was simulated.

Keywords: computer network, corporate network, data encryption, Gigabit Ethernet, Open Source, VLAN.

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

802.3ad (Link Aggregation) – технологія об’єднання каналів зв’язку;

802.3ae - 10 GbE;

DHCP (Dynamic Host Configuration Protocol) - протокол динамічного конфігурування стеку протоколів TCP/IP робочих станцій.

DNS (Domain Name System) - сервер доменних імен.

DNS (Domain Name System) - сервер доменних імен;

HTTP (Hypertext Transfer Protocol) - протокол передачі гіпертексту.

IEEE 802.3ab - 1000BASE-T Gigabit Ethernet;

IP (Internet Protocol) – Інтернет-протокол;

LAN (Local Area Network) – локальна мережа;

MAC (Media Access Control) - апаратна адреса ПК;

NAT (Network Address Translation) – мережева трансляція адес;

OSI (Open System Interface) – модель з’єднання відкритих систем;

Server Message Block (SMB) протокол прикладного рівня (в моделі OSI), зазвичай використовується для надання розділеного доступу до файлів, принтерів, послідовних портів передачі даних, та іншої взаємодії між вузлами в комп'ютерній мережі.

SNMP (Simple Network Management Protocol) – протокол керування мережею.

TCP/IP (Transmission Control Protocol/Internet Protocol) – протокол управління передачею/Інтернет протокол;

UTP (Unshielded Twisted Pair) – кабель типу неекранована скручена пара;

UTP (Unshielded Twisted Pair) – кабель типу неекранована скручена пара.

ЛМ – локальна мережа.

ОС - операційна система.

ПК - персональний комп’ютер.

СКС – структурована кабельна система.

ВСТУП

Сучасна локальна обчислювальна мережа (ЛОМ) є фундаментальним елементом інформаційної інфраструктури будь-якого підприємства, забезпечуючи інтеграцію комп'ютерного обладнання в єдине середовище для швидкого та захищеного обміну даними. Впровадження ЛОМ дозволяє суттєво оптимізувати фінансові витрати установи. При цьому пряма економія на придбанні апаратних засобів є лише вторинним фактором; головний економічний ефект досягається завдяки автоматизації бізнес-процесів, ліквідації непродуктивних втрат робочого часу персоналу та підвищенню швидкості обробки інформації.

Для організацій фінансового сектора наявність високошвидкісної та відмовостійкої мережі є критичною умовою для повсякденного функціонування. Специфіка банківської діяльності, роботи касових вузлів та розрахунково-касочих центрів виключає можливість ізольованої роботи підрозділів, оскільки вимагає безперервного, одночасного та захищеного доступу багатьох співробітників до спільних централізованих баз даних, банківських систем та реєстрів у режимі реального часу.

Основною метою цієї кваліфікаційної роботи є розробка проєкту високопродуктивної комп’ютерної мережі Івано-Франківського відділення Львівської філії АБ «Експрес-Банк». Архітектура мережі базується на впровадженні передових галузевих стандартів, серед яких: Gigabit Ethernet (IEEE 802.3ab) для забезпечення високої пропускної здатності, IEEE 802.1Q для віртуалізації мережевого простору (VLAN), механізми пріоритезації трафіку IEEE 802.1p (QoS), а також технології статичної маршрутизації на рівні ядра мережі.

Проєкт комп’ютерної мережі є високоактуальним, оскільки поєднання апаратної маршрутизації Inter-VLAN на комутаторі 3-го рівня із гнучко налаштованим програмним фаєрволом на периметрі дозволяє повною мірою

вирішити поставлені завдання, гарантуючи високу швидкість транзакцій, надійний захист банківської таємниці та можливість масштабування інфраструктури в майбутньому.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Кваліфікаційна робота бакалавра на тему: Розробка проєкту комп'ютерної мережі Івано-Франківського відділення Львівської філії АБ «Експрес-Банк».

Дана установа функціонує у фінансово-банківській сфері, надаючи повний спектр послуг юридичним та фізичним особам. В Івано-Франківську розташоване обласне відділення Львівської філії. У цьому офісі зосереджені ключові корпоративні мережеві ресурси та бази даних, доступ до яких мають отримувати співробітники установи незалежно від їхнього поточного географічного розташування. Також відділення здійснює обслуговування клієнтів та реалізовує широкий спект фінансових послуг.

Результати розробки мають практичне значення для побудови чимодернізації корпоративних мереж банківського сектора, де пріоритетом є створення інтегрованої інфраструктури з використанням захищених каналів зв'язку.

1.1.2 Призначення розробки

Проєкт комп'ютерної мережі розробляється з метою реалізації комплексу взаємопов'язаних технічних завдань, спрямованих на побудову ефективної, масштабованої та захищеної мережевої інфраструктури банківського відділення.

Першочерговим завданням є організація комутації кінцевих вузлів, що передбачає об'єднання всіх робочих станцій користувачів, серверного

обладнання та периферійних пристроїв у єдину логічну та фізичну мережу. Це забезпечує цілісність інформаційного середовища та спрощує адміністрування ресурсів.

Наступним важливим аспектом є забезпечення централізованого доступу до мережевих сервісів. Це включає надання користувачам контрольованого доступу до спільних ресурсів локальної мережі, а також організацію безпечного виходу до глобальної мережі Інтернет із застосуванням політик безпеки та засобів фільтрації трафіку.

Проєкт також передбачає можливість масштабування та подальшої модернізації мережі. Архітектура повинна підтримувати розширення кількості робочих місць, інтеграцію додаткових мережевих сегментів, а також впровадження нових високошвидкісних технологій передачі даних без необхідності суттєвої реконструкції існуючої інфраструктури.

Окрему увагу приділено забезпеченню безпечного міжфіліального обміну даними. Для цього передбачається використання захищених каналів зв’язку (VPN-тунелів), які гарантують конфіденційність, цілісність та автентичність інформації під час її передачі між центральним офісом та віддаленими підрозділами банку.

Важливим завданням є підвищення відмовостійкості мережі. Це досягається шляхом резервування критично важливих вузлів, використання надійних комутаційних рішень та оптимізації топології для мінімізації впливу можливих відмов окремих елементів інфраструктури.

Додатково передбачається налаштування базових мережевих сервісів і служб, що дозволяє автоматизувати внутрішні бізнес-процеси банку, підвищити ефективність обробки даних та забезпечити стабільну роботу інформаційної системи в цілому.

1.1.3 Вимоги до апаратного і програмного забезпечення

Для розгортання та стабільного функціонування мережі відділення необхідний комплекс узгоджених апаратних і програмних засобів.

Сервери включать в себе : сервер-шлюз (програмний маршрутизатор периметра) та файловий сервер. Перший використовується для організації віддаленого доступу працівників філій, терміналів і підключення локальної мережі до Інтернету. Обчислювальні ресурси (процесор, RAM) вибираються з надлишковим запасом для стабільної роботи за умов пікових навантажень. Інший сервер призначений для централізованого, захищеного та надійного зберігання даних. Обов’язковою є інтеграція апаратного RAID-масиву для збереження даних у разі відмови накопичувачів.

Головний комутатор (рівень ядра/розподілу) – це високопродуктивний керований комутатор 3-го рівня (Layer 3) з підтримкою апаратної маршрутизації віртуальних мереж (Inter-VLAN Routing) та стандартів: IEEE 802.3 (10Base-T), IEEE 802.3u (100Base-TX), IEEE 802.3ab (1000Base-T), IEEE 802.3z (1000Base-X, оптика), автоузгодження NWay та стандарту IEEE 802.1Q (VLAN).

Комутатори робочих груп та відділів (рівень доступу) - комутатори 2-го рівня (Layer 2) з підтримкою швидкості 100/1000 Мбіт/с на кожному порту, обов'язковою функцією автовизначення швидкості та типу кабелю (Auto-MDI/MDIX). Кількість портів на периферійних пристроях - не менше 8 (відповідно до щільності робочих місць в робочих групах).

Програмне забезпечення серверів: операційна система серверного шлюзу повинна забезпечувати високу безпеку та підтримувати розгортання шифрованих криптографічних VPN-тунелів на основі технологій SSL/TLS.

Програмне забезпечення робочих місць: на кінцевих станціях користувачів (WS) та операціоністів використовується сучасна ліцензійна

операційна система Windows 11 Pro, що відповідає поточним стандартам кібербезпеки та сумісності з банківським ПЗ

1.1.4 Вимоги до документації

До складу технічного проєкту комп'ютерної мережі банку мають входити такі документи:

1. Покрокові інструкції з адміністрування та конфігурування активного мережевого обладнання та серверних платформ.
2. Логічна схема об’єднаної корпоративної мережі банку (з урахуванням філій та ЦО).
3. Логічна схема мережевої інфраструктури Івано-Франківського відділення.
4. Поповерховий план будівлі відділення з нанесенням елементів СКС.
5. Фізична топологія та схема кабельних з'єднань локальної мережі підрозділу.

1.1.5 Техніко-економічні показники

Базовою технологією побудови інтегрованої мережі відділення банку узгоджено з замовником використання віртуальних приватних мереж (VPN). Як програмну платформу VPN застосовано OpenVPN із реалізацією криптографічного захисту на основі SSL/TLS.

У сегменті локальної мережі використовується технологія Gigabit Ethernet (1000Base-T), що функціонує на принципах комутації пакетів. Фізична організація мережі побудована за ієрархічною структурою типу «розширена зірка».

Функції міжмережевого захисту реалізуються програмним засобом IPFW (IP Firewall), інтегрованим у ядро операційної системи.

Як базову ОС шлюзу до Інтернету буде застосовано FreeBSD 14 - актуальну стабільну версію платформи. На робочих станціях планується використання операційна система Windows 11 Professional.

Для адресації та сегментації трафіку застосовано технологію NAT/PAT (Network Address Translation / Port Address Translation).

Граничний бюджет реалізації проєкту встановлено на рівні до 500 тис. грн. Очікуваний економічний ефект становить не менше 50 тис. грн на рік, що досягається за рахунок зниження витрат на технічне обслуговування та підвищення ефективності обробки транзакцій.

1.1.6 Стадії та етапи розробки

Процес створення комп'ютерної мережі банківської установи поділено на такі послідовні кроки:

1. Формування та аналіз логічної структури мережі Івано-Франківського відділення.

2. Проєктування фізичного розміщення елементів мережі та структурованої кабельної системи (СКС).

3. Техніко-економічне обґрунтування та підбір активного й пасивного обладнання.

4. Розробка архітектури об'єднання віддалених підрозділів у загальну захищену WAN-мережу.

5. Інсталяція та конфігурування серверних систем і шлюзів безпеки філій.

6. Комплексне тестування, оптимізація та здача мережі в експлуатацію.

Чіткий розподіл процесу проєктування на послідовні етапи дозволяє мінімізувати ризики виникнення помилок при побудові мережі, забезпечує раціональне використання бюджетних коштів під час вибору обладнання, а також гарантує, що створена інфраструктура повністю відповідатиме суворим

корпоративним стандартам безпеки, надійності та масштабованості АБ «Експрес-Банк»

1.1.7 Порядок контролю та прийому

Приймання спроєктованої мережі здійснюється на основі випробувань її ключових технічних і швидкісних характеристик, які повинні повністю відповідати критеріям надійності фінансових установ.

Діагностика та контроль параметрів виконуються за допомогою спеціалізованих утиліт та інструментальних наборів, детальний опис яких наведено у підрозділі 3.2 «Інструкція з використання тестових наборів та тестових програм»

1.2 Постановка задачі на розробку проекту. Характеристика підприємства, для якого створюється проект мережі

Ключовим завданням цієї кваліфікаційної роботи є комплексне проєктування сучасної, захищеної та відмовостійкої комп'ютерної мережі для Івано-Франківського обласного відділення Львівської філії АБ «Експрес-Банк».

Структура фінансової установи передбачає наявність головного офісу та кількох периферійних відділень із тенденцією до подальшого розширення мережі точок обслуговування. Головна інженерна задача створити локальну інфраструктуру Івано-Франківського підрозділу та інтегрувати її в загальну корпоративну мережу через Інтернет. При підключенні зовнішніх каналів зв'язку обов'язково враховується потреба в симетричному Інтернет-каналі з високою пропускною здатністю для забезпечення миттєвого проведення банківських операцій.

Архітектурні особливості об'єкта: Банківське відділення розташоване в окремій двоповерховій будівлі, де зони чітко розмежовані за функціональним призначенням:

Перший поверх: Орієнтований на пряму взаємодію з клієнтами. Тут розташовані операційні зали, касові кабіни, зони очікування. Також на вході до будівлі передбачено підключення двох зовнішніх терміналів-банкоматів, які вимагають максимального рівня фізичного та мережевого захисту.

Другий поверх: Призначений для адміністративного персоналу, внутрішніх службових відділів, бухгалтерії, а також тут розташовується серверна кімната.

Конфігурація логічної структури та безпеки: Для реалізації проєкту необхідно виконати розгортання та тонке налаштування програмного маршрутизатора на базі ОС FreeBSD останньої стабільної версії. Безпека периметра забезпечується за допомогою вбудованого міжмережевого екрана IPFW, правила якого мають суворо обмежувати доступ до внутрішніх ресурсів банку ззовні.

Об’єднання філій у єдину захищену інфраструктуру покладається на технологію OpenVPN. Для підвищення внутрішньої безпеки та продуктивності мережі, inter-VLAN маршрутизація переноситься на апаратний рівень центрального комутатора L3 (SW_2). Розроблені технічні інструкції з налаштування та інсталяції систем описано в підрозділі 3.1 «Інструкція з інсталяції програмного забезпечення серверів та активного комутаційного обладнання».

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Опис та обґрунтування вибору логічного типу мережі

Проєктування локальної обчислювальної мережі (ЛОМ) Івано-Франківського відділення АБ «Експрес-Банк» базується на архітектурі Gigabit Ethernet. Вибір цього технологічного стандарту зумовлений високою пропускною здатністю (до 1 Гбіт/с), економічною доцільністю впровадження та значним експлуатаційним ресурсом для подальшого масштабування інфраструктури без необхідності повної заміни пасивного обладнання.

Для оптимізації внутрішнього трафіку та розмежування прав доступу застосовано технологію віртуальних локальних мереж (VLAN) відповідно до міжнародного стандарту IEEE 802.1Q. Логічний поділ єдиного фізичного простору на ізольовані широкомовні домени дозволяє вирішити такі ключові завдання:

1. Інформаційна безпека. Реалізується шляхом повної ізоляції банківських підрозділів (касова зона, кредитний відділ, сервери) на канальному рівні, що мінімізує ризики несанкційного міжмережевого перехоплення пакетів.

2. Продуктивність та гнучкість досягається шляхом локалізації широкомовного шторму (Broadcast traffic) у межах одного сегмента, зменшення навантаження на процесори комутаторів та можливість гнучкої реконфігурації логічної структури без зміни фізичних з'єднань.

3. Централізоване керування дозволяє спростити процес впровадження групових політик безпеки та маршрутизації за допомогою віртуальних інтерфейсів (SVI) на комутаторі третього рівня (L3).

Повні телекомунікаційні метрики сформованих підмереж та детальні параметри розподілу фізичних портів обладнання наведено відповідно у Таблиці Б.1 «Логічна адресація в ЛОМ» та Таблиці Б.2 «Таблиця

конфігурування VLAN» додатка Б. Зазначені константи є фундаментальною основою для практичної реалізації, описаної в третьому розділі проєкту.

Об'єднання територіально розподілених структурних підрозділів банку в єдину корпоративну мережу може здійснюватися двома шляхами: орендою виділених волоконно-оптичних ліній зв'язку або використанням публічної мережі Інтернет як транспортного середовища. З огляду на капітальні витрати, у цьому проєкті впроваджено другий варіант із розгортанням технології віртуальних приватних мереж (VPN).

Для нівелювання загроз цілісності та конфіденційності даних під час транзиту через публічні канали, як базовий інструментарій обрано програмний комплекс OpenVPN. Схема логічної взаємодії вузлів розподіленої мережі філії представлена на рисунку 2.1.

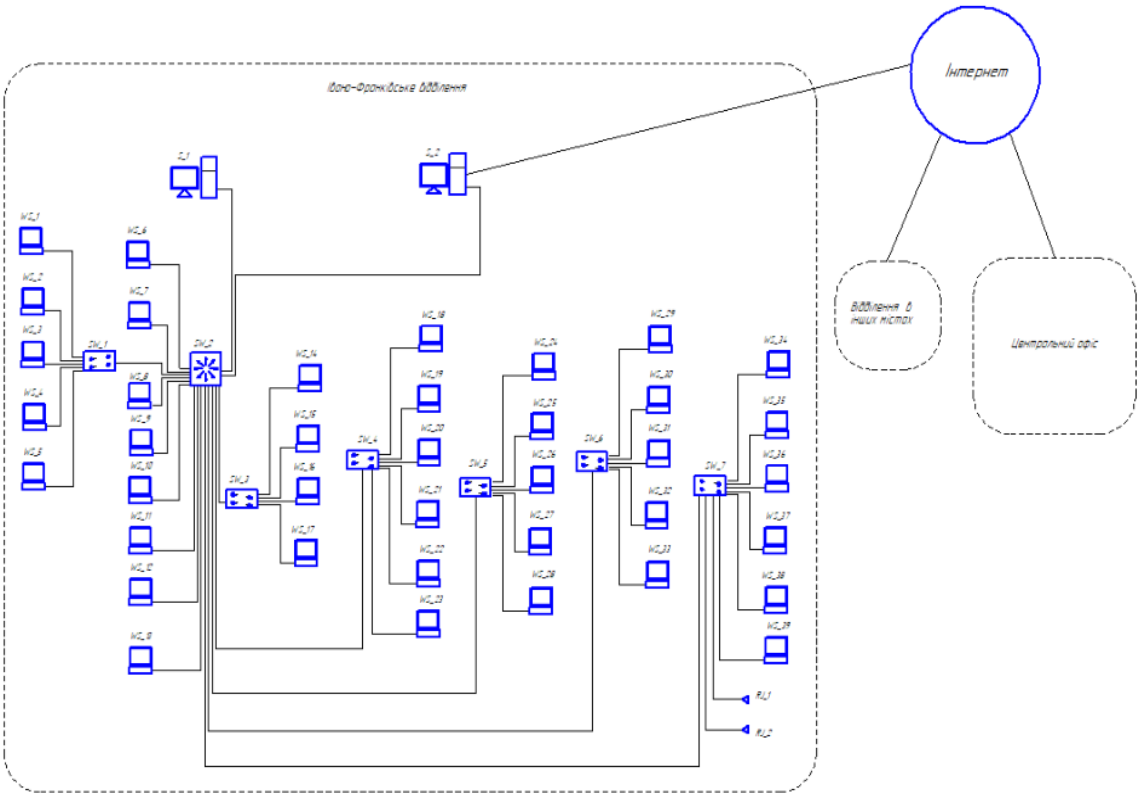


Рисунок 2.1 – Логічна тополія мережі

Впровадження стандартів Gigabit Ethernet, керованих VLAN та шифрованих тунелів OpenVPN дозволяє створити монолітну, захищену від зовнішніх та внутрішніх загроз інфраструктуру, що повністю відповідає нормативним стандартам безпеки банківського сектору.

2.2 Розробка схеми фізичного розташування кабелів та вузлів

2.2.1 Типи кабельних з'єднань та їх прокладка

Для побудови локальної комп'ютерної мережі Івано-Франківського відділення Львівської філії АБ «Експрес-Банк» можуть використовуватись оптичні та мідні кабельні лінії зв'язку. Оптоволоконний кабель забезпечує високу швидкість передачі даних на значні відстані та стійкість до електромагнітних завад, проте його використання в межах одного офісного приміщення є економічно недоцільним через вищу вартість обладнання та монтажу.

Для підключення робочих станцій, мережевих принтерів, IP-телефонів та іншого обладнання обрано неекрановану виту пару категорії 6 (UTP Cat 6). Даний кабель підтримує швидкість передачі даних до 1 Гбіт/с на відстані до 100 м та відповідає вимогам стандарту Gigabit Ethernet IEEE 802.3ab. Кабель категорії 6 характеризується підвищеною завадостійкістю порівняно з кабелями попередніх категорій та забезпечує необхідний запас пропускної здатності для розвитку мережі.

Прокладання кабельних ліній передбачається у пластикових кабельних коробах уздовж стін приміщень із дотриманням вимог структурованих кабельних систем. Завершення кабельних ліній здійснюється за допомогою інформаційних розеток RJ-45 та комутаційних панелей. Таке рішення забезпечує надійність функціонування мережі, зручність обслуговування та можливість подальшої модернізації мережевої інфраструктури.

Для забезпечення гнучкості банківської інфраструктури, можливості підключення мобільних пристроїв персоналу (планшетів, ноутбуків) та організації зони самообслуговування для клієнтів, у проєкті передбачено інтеграцію бездротової точки доступу (Wi-Fi маршрутизатора). Внаслідок поєднання класичної кабельної структури СКС та радіоканалів, результуюча архітектура мережі філії набуває ознак гібридної фізичної топології.

Гібридна топологія у межах фінансової установи являє собою інтегровану комбінацію деревоподібної кабельної підсистеми та бездротової комірчастої або радіальної структури. Таке рішення дозволяє зберегти максимальний рівень безпеки й відмовостійкості для стаціонарних критично важливих вузлів (серверів, касових терміналів, робочих місць операціоністів) за допомогою дротових ліній, одночасно надаючи необхідну мобільність для гостьового та адміністративного бездротових сегментів.

2.2.2 Будова вузлів та необхідність їх застосування

Функціонування телекомунікаційної інфраструктури банківського відділення забезпечується комплексом взаємопов'язаних апаратних компонентів. Відповідно до класичної трирівневої ієрархічної моделі проектування мереж, структурні вузли розподіляються за своїм функціональним призначенням на комутатори доступу (рівень периферійних відділів), центральний комутатор ядра (рівень агрегації) та прикордонний шлюз безпеки (периметр мережі).

Комутатори робочих груп (рівень доступу) призначені для фізичної консолідації кінцевого обладнання (робочих станцій персоналу, мережевих принтерів, касових терміналів, IP-телефонів) окремих структурних підрозділів філії в єдині локальні сегменти. Вони забезпечують комутацію трафіку на канальному рівні (L2) у межах відповідного відділу. Головне завдання комутаторів доступу гарантувати високошвидкісний безперешкодний обмін

даними між локальними клієнтами та первинне тегування пакетів ідентифікаторами віртуальних мереж (VLAN ID).

Центральний комутатор (ядро мережі та рівень агрегації) виступає головним високопродуктивним комутаційним центром, що інтегрує всі периферійні сегменти ЛОМ філії та серверне обладнання в монолітну систему. Завдяки використанню комутатора 3-го рівня (L3) з розширеними функціями маршрутизації, реалізується логічне розбиття єдиного фізичного простору на ізольовані широкомовні домени (VLAN). Такий підхід суттєво мінімізує циркуляцію паразитних широкомовних пакетів (Broadcast Storms), знижує обчислювальне навантаження на процесори мережевих карт хостів та кардинально підвищує загальну пропускну здатність і швидкісні параметри корпоративної мережі.

Шлюз доступу до Інтернту (периметр безпеки) забезпечує санкціоновану взаємодію локальної мережі банку з публічним середовищем Інтернет та побудову VPN-тунелів до Головного офісу. На цей апаратний вузол покладено завдання трансляції мережевих адрес (NAT), динамічного розподілу та шейпінгу смуги пропускання, а також stateful-фільтрації вхідних і вихідних інформаційних потоків за допомогою міжмережевого екрана (Firewall) для захисту інформаційного контуру банку від зовнішніх кібератак.

Центральним елементом фізичної структури ЛОМ є головний комутаційний вузол, розташований у спеціалізованому, технічно укріпленому приміщенні - серверній кімнаті. Тут зосереджено все активне обчислювальне та пасивне комутаційне обладнання, що монтується у закриту підлогову комутаційну шафу (19-дюймову стійку).

Конструкція комутаційної шафи містить такі елементи інфраструктури:

1. Серверна група, що включає апаратні платформи під керуванням спеціалізованих ОС (FreeBSD), що забезпечують роботу критично важливих банківських служб, файлового сховища та сервісів автентифікації.

2. Центральний комутатор мережі 3-го рівня (L3) забезпечує комутацію та внутрішню саршрутизацію пакетів між віртуальними підмережами та зв’язок з корпоративним сераерами .

3. Комутаційні патч-панелі (крос-панелі). Пасивне обладнаня, яке виступає кінцевою точкою термінування всіх магістральних і горизонтальних кабельних ліній СКС, що прокладені від робочих місць співробітників. Використання патч-панелей забезпечує високу гнучкість комутації, зручність під час реконфігурації мережевих портів за допомогою патч-кордів, а також захищає безпосередні порти активних комутаторів від фізичного зносу.

4. Блоки безперебійного живлення (ДБЖ / UPS), які гарантують безперервну роботу серверів, комутаторів та шлюзу у разі аварійних збоїв чи повної відсутності напруги в первинній електромережі, здійснюючи додаткову фільтрацію високочастотних перешкод та стрибків напруги.

Така системна організація вузлів мережі дозволяє побудувати надійне, легкокероване та відмовостійке середовище, яке відповідає суворим стандартам безпеки й архітектурної побудови банківських систем.

2.3 Обґрунтування вибору комунікаційного обладнання

Формування апаратної архітектури комп'ютерної мережі філії банку передбачає комплексний підбір активного та пасивного телекомунікаційного обладнання. Вибір конкретних технічних засобів здійснюється на основі аналізу їхньої відповідності сучасним мережевим стандартам, сумісності з протоколами передачі даних, показників відмовостійкості, а також вимог замовника щодо продуктивності та безпеки фінансових операцій.

З метою оптимізації обчислювальної потужності серверної зони було проведено детальний техніко-економічний аналіз рішень від провідних світових виробників. Зведені аналітичні дані та порівняльні параметри

представлені в Таблиці В.1 «Порівняльна характеристика апаратних платформ серверів» додатка В.

На основі зіставлення критично важливих критеріїв - обчислювальної спроможності процесорів, максимального обсягу оперативної пам'яті та вартості придбання і обслуговування як базову апаратну платформу для шлюзу доступу до мережі Інтернет обрано сервер ARTLINE Business R33. Поряд із високими індексами надійності та відмовостійкості, цей сервер має конструктивне виконання типу Rackmount для монтажу в стандартну 19-дюймову комутаційну стійку, що забезпечує високу ергономіку, зручність адміністрування та ефективне охолодження обладнання в умовах серверної кімнати.

Аналогічна високопродуктивна конфігурація платформи ARTLINE Business R33 застосовується і для розгортання централізованого файлового сервера філії. Для задоволення потреб установи в збереженні великих масивів банківської документації та щоденних резервних копій (бекапів), дискову підсистему файлового сервера додатково укомплектовано спеціалізованими жорсткими дисками (HDD) корпоративного класу ємністю 4 ТБ кожен, об'єднаними в відмовостійкий масив для забезпечення надійсності. Внутрішню будову серверу навдеено на риснку 2.2

Рисунок 2.2 – Сервер ARTLINE Business R33

Побудова комутаційної матриці ЛОМ, що забезпечує високошвидкісний обмін пакетами даних між кінцевими хостами та розподіл широкомовних доменів, базується на дворівневій ієрархічній структурі.

Для вибору оптимальних пристроїв рівня доступу в робочих групах (відділах) філії було виконано дослідження ринку мережевого обладнання. Результати цього аналізу викладено в Таблиці В.2 «Порівняльний аналіз 16-ти портових комутаторів робочих груп» додатка В, де порівнюються технічні параметри керованих комутаторів другого рівня (L2).

Вибір центрального вузла агрегації та ядра мережі здійснювався на основі жорстких вимог до пропускної здатності комутаційної фабрики, підтримки статичної та динамічної маршрутизації (L3), а також можливості стекування.

Аналітичні дані для обґрунтування цього вибору наведено в Таблиці В.3 «Порівняльний аналіз центральних комутаторів» додатка В.

За сукупністю технічних переваг та експлуатаційних характеристик для локальної мережі філії банку обрано керований комутатор третього рівня TP-Link T3700G-24TQ.

Вибраний комутатор застосовуватиметься як магістральне ядро мережі для агрегації трафіку з усіх периферійних підрозділів, забезпечення міжвекторної маршрутизації між VLAN (Inter-VLAN Routing), реалізації апаратних політик безпеки (ACL) та гарантування мінімальних затримок під час звернення користувачів до критично важливих серверних ресурсів банку.

Загальний вигляд комутатора зображено на риснку 2.3

Використання комутатора третього рівня в ролі центрального вузла мережі забезпечує можливість подальшого масштабування локальної інфраструктури без необхідності суттєвої модернізації апаратного забезпечення. Наявність високошвидкісних висхідних портів, розширених механізмів керування трафіком та підтримки сучасних мережевих протоколів дозволяє підтримувати високу продуктивність мережі навіть за умови

збільшення кількості користувачів, серверів і мережевих сервісів, що особливо важливо для безперебійного функціонування банківської інформаційної системи.

Рисунок 2.3 - Керований комутатор третього рівня TP-Link T3700G-24TQ

З метою забезпечення однорідності мережевої інфраструктури, спрощення процесу адміністрування та гарантії стовідсоткової сумісності протоколів, на рівні доступу (Access Layer) було прийнято рішення використовувати комутатори компанії TP-Link, аналогічно до обраного комутатора ядра мережі. Це дозволяє побудувати моновендорну систему з можливістю подальшої інтеграції в єдину платформу централізованого моніторингу та керування.

Для забезпечення апаратної реалізації розробленого проєкту, систематизації компонентів СКС та оптимізації процесу закупівлі технічних засобів було сформовано відомість специфікації.

В таблиці 2.1 наведено вичерпний перелік активного та пасивного телекомунікаційного обладнання, а також програмного забезпечення, що інтегрується в локальну обчислювальну мережу філії банку.

Таблиця 2.1 – Специфікація активного та пасивного обладнання комп'ютерної мережі

№	Найменування обладнання та матеріалів	Од. вим.	Кількість	Ціна, грн.	Вартість, грн.
1	Магістральний комутатор третього рівня TP-Link T3700G-24TQ	шт.	1	30670	30670
2	Керований комутатор робочої групи TP-Link TL-SG2008	шт.	6	3200	19200
3	Керований комутатор доступу TP-Link TL-SG2216	шт.	1	4500	4500
4	Сервер файлових ресурсів ARTLINE Business R33	шт.	1	38000	38000
5	Сервер доступу до зовнішніх мереж ARTLINE Business R33	шт.	1	33000	33000
6	Джерело безперебійного живлення APC Smart-UPS 1500VA	шт.	1	16500	16500
7	Телекомунікаційна шафа 24U для центрального вузла мережі	шт.	1	15800	15800
8	Настінна комутаційна шафа 7U	шт.	6	4500	27000
9	Комутаційна панель на 24 порти Cat.6	шт.	1	4000	4000
10	Комутаційна панель на 16 портів Cat.6	шт.	6	3100	18600
11	Інформаційна розетка RJ-45 категорії 6	шт.	41	130	5330
12	З'єднувальний комутаційний шнур UTP Cat.6	шт.	45	60	2700
13	Кабель «вита пара» UTP Cat.6	м	610	26	15860
14	Кабельний канал пластиковий	м	123	70	8610
	Загальна вартість проєкту				**239770**

2.4 Особливості монтажу мережі

Технологічний процес розгортання структурованої кабельної системи (СКС) на базі неекранованої витої пари U/UTP категорії 6 в Івано-Франківському відділенні банку має суворо відповідати вимогам міжнародного галузевого стандарту ANSI/TIA/EIA-568-C.2, а також нормам чинного законодавства з охорони праці та електробезпеки.

Організація та специфіка виконання монтажних робіт передбачає врахування таких ключових технологічних особливостей:

1. Матеріально-технічне забезпечення, тобто перед початком робіт готується повний комплект інструментарію та розхідних матеріалів. До нього входять: сертифікований кабель U/UTP Cat.6, мережеві модулі RJ-45 (Keystone Jacks) для крос-панелей та розеток, інструмент для зачистки ізоляції (Stripper), спеціалізований ніж для забивання та обрізки контактів (Punch down tool), обтискні кліщі (Crimper) для формування патч-кордів, а також цифровий кабельний аналізатор (тестер).

2. Підготовка та мірна нарізка кабелю передбачає розкроювання кабельних трас здійснюється з урахуванням архітектурних особливостей приміщень філії. Нарізання провідників на технологічні сегменти виконується з обов'язковим нормативним запасом довжини (не менше 1–2 метрів з кожного боку) для забезпечення можливості подальшого перепідключення, обслуговування чи ремонту лінії.

3. Трасування та захист від перешкод ліній зв'язку реалізується всередині кабельних каналів (коробів, гофротруб). Для нівелювання впливу низькочастотних та високочастотних електромагнітних наведень (EMI) слабострумні траси ЛОМ розміщуються на регламентованій стандартами відстані від ліній силового електроживлення, люмінесцентних світильників та розподільних щитів.

4. Фіксація та контроль радіуса вигинупередбачає закріплення провідників у лотках чи кабель-каналах виконується за допомогою пластикових стяжок-хомутів. Категорично забороняється надмірне затягування хомутів, що може призвести до деформації оболонки. Під час поворотів ліній мінімальний радіус вигину кабелю має становити не менше чотирьох його зовнішніх діаметрів для збереження геометрії пар і запобігання внутрішнім наведенням (Next-talk).

5. Термінування та комутація інтерфейсів. На відміну від побутових мереж, магістральні та горизонтальні лінії банківської СКС не обтискаються конекторами, а розшиваються у крос-панелі серверної шафи та внутрішні модулі інформаційних розеток робочих місць. Термінування жил виконується за єдиною затвердженою схемою розведення контактів TIA/EIA-568B за допомогою забивного інструменту, що гарантує надійний ножовий контакт (IDC).

6. Діагностика та сертифікація ліній виконується ісля завершення монтажу кожна кабельна лінія підлягає обов'язковому інструментальному контролю за допомогою кабельного тестера. Процедура тестування верифікує правильність розведення пар, відсутність коротких замикань, обривів, а також відповідність затухання сигналу та перехресних завад критеріям стандарту Cat. 6.

Дуже важливим є дотримання правил техніки безпеки під час монтажу. Усі операції з прокладання кабельних ліній поблизу елементів силової електромережі банку виконуються виключно за умови повного знеструмлення відповідного сектора живлення.

Монтажники зобов'язані використовувати сертифікований інструмент з діелектричними ручками, захисні окуляри під час штроблення або свердління стін, а також не допускати механічних перевантажень, розривів чи критичних заломів кабельної продукції, що може погіршити загальні параметри надійності ЛОМ фінансової установи.

2.5 Обґрунтування вибору програмного забезпечення

Формування програмного комплексу мережі філії банку базується на комбінуванні комерційних ліцензій для користувачів та безкоштовного ПЗ з відкритим кодом для серверного периметра.

Робочі станції передбачають інсталяцію ОС Windows 11 Pro (постачається за OEM-ліцензією разом з апаратним забезпеченням). Вибір зумовлений повною сумісністю з профільним банківським софтом (наприклад, АБС «БАРС-MMFO»), відсутністю витрат на перенавчання персоналу та високим рівнем кінцевої безпеки.

На шлюзі доступу та файловому сервері розгорнуто ОС FreeBSD 14. Ця UNIX-платформа обрана завдяки монолітній безпеці ядра, високій стійкості до кібератак, наявності потужного штатного брандмауера IPFW та нульовій вартості ліцензування й оновлень.

Захист транзитного трафіку між віддаленими підрозділами банку через Інтернет реалізовано засобами пакету OpenVPN, який функціонує у середовищі FreeBSD. Пакет забезпечує надійне шифрування даних (AES-256) та захист від перехоплення інформації на шляху до головного офісу.

2.6 Обґрунтування вибору засобів захисту мережі

Забезпечення належного рівня безпеки всередині інформаційного контуру банківської установи потребує впровадження комплексної ешелонованої системи захисту. У розробленому проєкті безпека даних реалізується одночасно на трьох технологічних рівнях: периметральному (шлюз), мережевому (L3-комутатор) та хостовому (робочі станції).

Як базовий інструмент міжмережевого екранування на межі з публічною мережею Інтернет обрано штатний брандмауер IPFW, інтегрований у ядро ОС FreeBSD. Його використання є повністю

безкоштовним і не потребує додаткових витрат на ліцензування. IPFW здійснює глибокий аналіз пакетів із врахуванням стану з'єднань (Stateful Inspection), захищаючи внутрішні ресурси філії від зовнішніх кібератак. Детальний лістинг правил фільтрації та конфігурацію брандмауера наведено у третьому розділі роботи.

Для додаткового розмежування внутрішніх інформаційних потоків між ізольованими віртуальними підмережами (VLAN) використовуються можливості операційної системи центрального комутатора TP-Link T3700G-52TQ. На ньому реалізуються апаратні списки контролю доступу (ACL Access Control Lists), які фільтрують міжмережевий трафік безпосередньо на рівні комутації, блокуючи несанкціоновані запити між різними відділами банку.

Безпека безпосередньо на робочих місцях персоналу забезпечується штатним засобом Windows Firewall, інтегрованим в операційну систему Windows 11 Pro. Цей вбудований засіб здійснює локальний контроль мережевої активності додатків, блокує шкідливий трафік на рівні окремого комп'ютера та ізолює хост у разі виникнення внутрішніх загроз.

Такий трирівневий підхід (IPFW + ACL + Windows Firewall) гарантує високу відмовостійкість захисту та унеможливлює компрометацію банківських даних як із зовнішньої мережі, так і внаслідок можливих внутрішніх інцидентів.

2.7 Тестування та налагодження мережі

Комплексна верифікація та пусконалагоджувальні роботи для розгорнутої мережевої інфраструктури банківського відділення реалізуються у кілька послідовних етапів. Це дозволяє гарантувати відповідність фізичних та логічних параметрів системи критеріям надійності, відмовостійкості та безпеки, які висуваються до фінансових установ.

Діагностика локальної обчислювальної мережі розподіляється на два базові рівні:

Апаратне тестування кабельної системи: Передбачає інструментальний контроль створеної структурованої кабельної системи (СКС) за допомогою цифрових кабельних аналізаторів (тестерів). На цьому етапі кожна кабельна лінія перевіряється на відсутність фізичних дефектів (обривів, коротких замикань, перехресних наведень) та на повну відповідність специфікаціям стандарту Gigabit Ethernet (Cat. 6).

Програмно-логічне тестування вузлів: Спрямоване на перевірку коректності функціонування мережевих служб, інтерфейсів операційних систем та конфігураційних параметрів активного обладнання на мережевому й транспортному рівнях моделі OSI.

Після успішного завершення локальних випробувань окремим критично важливим етапом є тестування розподіленої корпоративної мережі, об'єднаної за допомогою захищених криптографічних тунелів на базі технології VPN (OpenVPN). На цьому кроці перевіряється стабільність маршрутизації та безпека обміну даними між Івано-Франківським відділенням та серверами Головного офісу.

Програмна діагностика та моніторинг параметрів з'єднання здійснюються за допомогою штатного інструментарію операційних систем через такі мережеві утиліти:

- ping виконує перевірку базової доступності віддалених хостів та вимірювання затримок (RTT) під час проходження пакетів;

- tracert (або traceroute) для визначення точного маршруту слідування даних, аналізу проміжних вузлів маршрутизації та виявлення точок деградації каналу;

- netstat використовується для моніторингу активних мережевих підключень, аналізу відкритих портів та збору статистики за мережевими протоколами;

- ipconfig (або ifconfig у FreeBSD) застосовується для контролю та відображення поточних параметрів налаштування інтерфейсів (IP-адрес, масок підмереж, шлюзів за замовчуванням);

- route, засіб для перевірки, модифікації та аналізу таблиць маршрутизації на серверах і робочих станціях.

Оперативний пошук, локалізація та усунення неполадок в архітектурі ЛОМ здійснюються адміністраторами за допомогою інтегрованих засобів керування та журналювання операційних систем, встановлених на серверах (FreeBSD) та керованих комутаторах ядра (TP-Link CLI). Такий системний підхід забезпечує мінімальний час відновлення мережі у разі виникнення позаштатних ситуацій і гарантує безперервність банківських процесів.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкції з налаштування програмного забезпечення серверів

3.1.1 Інструкції з налаштування шлюза та служби OpenVPN

Для об'єднання територіально розподілених підрозділів банківської установи в єдиний інформаційний простір виникла необхідність побудови захищеної віртуальної приватної мережі (VPN) через публічну мережу Інтернет. На сучасному ринку телекомунікацій існує широкий спектр рішень для організації VPN-тунелів, які регулярно порівнюються за критеріями вартості, рівня криптографічного захисту та загальної відмовостійкості.

З огляду на вимоги до гнучкості архітектури та відсутності додаткових витрат на ліцензування пристроїв, у цьому дипломному проєкті впроваджено програмний комплекс OpenVPN. Дане рішення дозволяє розгорнути надійну топологію типу «точка-мультиточка» (Point-to-Multi-Point) із використанням інфраструктури відкритих ключів (PKI) та сертифікатів взаємної автентифікації TLS/SSL замість менш безпечних статичних ключів.

Центральний VPN-сервер розгортається на базі операційної системи FreeBSD, яка безпосередньо обслуговує мережевий периметр Головного офісу банку. Клієнтами системи є дві віддалені філії (де на шлюзах також встановлено ОС FreeBSD) та портативна робоча станція системного адміністратора під керуванням ОС Windows 10.

Впроваджена схема адресації та маршрутизації передбачає наступну логічну структуру сегментів:

Центральний офіс (Серверна зона): логічна підмережа 172.16.14.0/24.

Івано-Франківське відділення (Клієнт 1): логічна підмережа 172.16.1.0/24.

Віддалений офіс (Клієнт 2): логічна підмережа 172.16.2.0/24.

Адміністратор (Клієнт 3): мобільний клієнт з індивідуальним IP-виділенням із пулу VPN.

Політика організації тунелю визначає маршрутизований тип зв'язку (Routed VPN на базі логічних інтерфейсів tun), що виключає трансляцію широкомовного трафіку між філіями задля економії пропускної здатності каналів. Схема взаємодії вузлів реалізує таку матрицю доступу: з підмережі Головного офісу забезпечується повна прозорість до хостів обох філій і навпаки; при цьому комп'ютер віддаленого адміністратора має санкціонований доступ до всіх трьох локальних сегментів банківської інфраструктури.

Опишемо процедуру інсталяції та первинного конфігурування сервера OpenVPN. Перед початком розгортання сервісу у FreeBSD необхідно переконатися в наявності підтримки віртуальних тунельних інтерфейсів на рівні операційної системи. Для цього до конфігураційного файлу ядра додається відповідна директива:

pseudo-device tun

Примітка: якщо у збірці ядра за замовчуванням дана опція була відсутня, виконується процедура перекомпіляції ядра та перезавантаження шлюзу.

Встановлення програмного пакета OpenVPN здійснюється безпосередньо з офіційного дерева портів FreeBSD:

```
# cd /usr/ports/security/openvpn
# make install clean
```

Стандартним місцем зберігання конфігураційних файлів та елементів криптографічного захисту в ОС FreeBSD є каталог /usr/local/etc/openvpn. Наступний набір команд ініціалізує ієрархію робочих директорій та файлів внутрішньої бази даних Центру сертифікації (CA):

```
# mkdir -p /usr/local/etc/openvpn/ccd
# mkdir -p /usr/local/etc/openvpn/certs
```

```
# mkdir -p /usr/local/etc/openvpn/crl
# mkdir -p /usr/local/etc/openvpn/keys
# mkdir -p /usr/local/etc/openvpn/private
# mkdir -p /usr/local/etc/openvpn/req
# chmod 700 /usr/local/etc/openvpn/keys /usr/local/etc/openvpn/private
# echo "01" > /usr/local/etc/openvpn/serial
# touch /usr/local/etc/openvpn/index.txt
```

Налаштування підсистеми OpenSSL для генерації PKI

Для ізоляції банківського центру сертифікації від загальносистемних налаштувань OpenSSL, створюється локальний конфігураційний файл /usr/local/etc/openvpn/openssl.cnf із таким вмістом:

Ini, TOML

```
[ ca ]
default_ca = Ca_default
[ Ca_default ]
dir = /usr/local/etc/openvpn
crl_dir = $dir/crl
database = $dir/index.txt
new_certs_dir = $dir/certs
certificate = $dir/ca_cert.pem
serial = $dir/serial
crl = $dir/crl/crl.pem
private_key = $dir/private/ca_key.pem
RANDFILE = $dir/private/.rand
default_days = 3650
default_crl_days = 365
default_md = sha256
unique_subject = yes
policy = policy_any
```

```
x509_extensions = user_extensions
[ policy_any ]
organizationName = match
organizationalUnitName = optional
commonName = supplied
[ req ]
default_bits = 2048
default_keyfile = privkey.pem
distinguished_name = req_distinguished_name
x509_extensions = Ca_extensions
[ req_distinguished_name ]
organizationName = Organization Name (must match CA)
organizationName_default = Bank_Branch
organizationalUnitName = Location Name
commonName = Common User or Org Name
commonName_max = 64
[ user_extensions ]
basicConstraints = CA:false
[ Ca_extensions ]
basicConstraints = CA:true
default_days = 3650
[ server ]
basicConstraints = CA:false
nsCertType = server
```

Генерація кореневого самопідписного сертифіката (CA) та відповідного закритого ключа виконується у робочій директорії за допомогою утиліти openssl:

```
# cd /usr/local/etc/openvpn
```

openssl req -new -nodes -x509 -keyout private/ca_key.pem -out ca_cert.pem -days 3650 -config openssl.cnf

Під час виконання команди адміністратор послідовно вносить легітимні реквізити установи (код країни, назву регіону, найменування фінансової організації, назву IT-підрозділу, Common Name та контактний e-mail).

Наступним кроком є формування цифрової пари безпосередньо для самого сервера VPN:

openssl req -new -nodes -keyout keys/server.pem -out req/server.pem -config openssl.cnf

Валідація створених сертифікатів та запитів проводиться за допомогою діагностичних команд:

openssl req -noout -text -in req/server.pem

openssl rsa -noout -text -in keys/server.pem

Для завершення створення серверного сертифіката виконується його підписаня кореневим ключем банку:

openssl ca -batch -config openssl.cnf -extensions server -out certs/server.pem -infiles req/server.pem

Формування основного конфігураційного файла сервера OpenVPN

Підсумковий файл конфігурації сервісу /usr/local/etc/openvpn/openvpn.conf набуває такого вигляду:

```
dev tun
local <Зовнішня_IP_адреса_шлюзу_головного_офісу>
port 1194
proto udp
server 10.0.0.0 255.255.255.0
push "route 10.0.0.0 255.255.255.0"
route 172.16.1.0 255.255.255.0
route 172.16.2.0 255.255.255.0
client-config-dir ccd
```

```
client-to-client
tls-server
dh          /usr/local/etc/openvpn/dh2048.pem
ca          /usr/local/etc/openvpn/ca_cert.pem
cert        /usr/local/etc/openvpn/certs/server.pem
key         /usr/local/etc/openvpn/keys/server.pem
crl-verify  /usr/local/etc/openvpn/crl/crl.pem
tls-auth    /usr/local/etc/openvpn/ta.key 0
keepalive   10 120
tun-mtu     1500
mssfix      1450
persist-key
persist-tun
user        openvpn
group       openvpn
verb        3
```

Директива client-config-dir ccd посилається на однойменну директорію, де створюються персональні текстові файли налаштувань для кожного клієнта. Назви файлів повинні суворо відповідати значенню поля Common Name (CN) індивідуального сертифіката філії:

```
# cd /usr/local/etc/openvpn/ccd
# touch client1 client2 client3
```

Вміст індивідуального конфігураційного файла client1 (Івано-франківська філія):

```
push "route 172.16.14.0 255.255.255.0"
iroute 172.16.1.0 255.255.255.0
```

Вміст індивідуального конфігураційного файла client2 (Віддалена філія):

push "route 172.16.14.0 255.255.255.0"

iroute 172.16.2.0 255.255.255.0

Вміст індивідуального конфігураційного файла client3 (Робоче місце адміністратора):

push "route 172.16.14.0 255.255.255.0"

push "route 172.16.1.0 255.255.255.0"

push "route 172.16.2.0 255.255.255.0"

Для забезпечення автоматичного запуску демона OpenVPN під час ініціалізації операційної системи FreeBSD, до конфігураційного файла системних служб /etc/rc.conf вноситься відповідний рядок:

openvpn_enable="YES"

Конфігурування правил міжмережевого екрана IPFW

Для забезпечення легітимного проходження інкапсульованого трафіку та захисту шлюзу, підсистема міжмережевого екрана IPFW налаштовується відповідно до таких правил безпеки:

Безперешкодний пропуск пакетів через віртуальні інтерфейси тунелювання OpenVPN (tun).

Дозвіл вхідних UDP-пакетів на зовнішній інтерфейс і порт 1194, які забезпечують роботу самого тунелю.

Дозвіл спрямованого руху трафіку із захищеної VPN-мережі у внутрішній банківський LAN-сегмент.

Взаємний дозвіл ініціалізації сесій із локальних мереж у напрямку віртуального VPN-простору.

У конфігураційний скрипт ipfw додаються такі правила фільтрації:

/sbin/ipfw -q add pass ip from any to any via ${vif}

/sbin/ipfw -q add pass udp from any to ${oip} 1194 in via ${oif}

/sbin/ipfw -q add pass ip from ${vnet} to ${inet} out via ${iif}

/sbin/ipfw -q add pass ip from ${inet} to ${vnet} in via ${iif}

/sbin/ipfw -q add pass ip from 172.16.1.0/24 to ${inet} out via ${iif}

/sbin/ipfw -q add pass ip from ${inet} to 172.16.1.0/24 in via ${iif}

/sbin/ipfw -q add pass ip from 172.16.2.0/24 to ${inet} out via ${iif}

/sbin/ipfw -q add pass ip from ${inet} to 172.16.2.0/24 in via ${iif}

Контекст використання вказаних системних змінних оболонки Shell:

oip актуальна зовнішня статична IP-адреса шлюзу;

inet локальний мережевий сегмент Головного офісу (172.16.14.0/24);

vnet віртуальний адресний пул VPN-тунелю (10.0.0.0/24);

iif внутрішній системний мережевий інтерфейс шлюзу (наприклад, em1 або rl1);

oif зовнішній мережевий інтерфейс (наприклад, em0 або rl0);

vif логічний інтерфейс служби OpenVPN (tun0).

Зі сторони клієнтських шлюзів конфігурування правил міжмережевого екрана реалізується дзеркально. Правила фільтрації для першої філії (Клієнт 1) набувають наступного вигляду, де змінна inet вказує на внутрішню підмережу 172.16.1.0/24:

/sbin/ipfw -q add pass ip from any to any via ${vif}

/sbin/ipfw -q add pass udp from any to ${oip} 1194 in via ${oif}

/sbin/ipfw -q add pass ip from ${vnet} to ${inet} out via ${iif}

/sbin/ipfw -q add pass ip from ${inet} to ${vnet} in via ${iif}

/sbin/ipfw -q add pass ip from 172.16.14.0/24 to ${inet} out via ${iif}

/sbin/ipfw -q add pass ip from ${inet} to 172.16.14.0/24 in via ${iif}

Аналогічна структура правил застосовується і для Клієнта 2, з адаптацією локальної змінної inet під підмережу 172.16.2.0/24.

Безпечне транспортування ключів та завершення налаштування

Для мінімізації ризиків компрометації та перехоплення створених закритих ключів у публічних мережах, їх перенесення на кінцеві клієнтські шлюзи виконується виключно за допомогою фізичних зашифрованих носіїв.

Копіювання криптографічного набору для віддаленого вузла на змонтований накопичувач реалізується через командний рядок:

```
 # mount -t msdosfs /dev/da0s1 /mnt
# cd /usr/local/etc/openvpn
# cp certs/client1.pem /mnt/
# cp keys/client1.pem /mnt/
# cp ca_cert.pem /mnt/
# cp ta.key /mnt/
# umount /mnt
```

У результаті процедури на цільовий пристрій копіюється клієнтський сертифікат, закритий приватний ключ, публічний кореневий сертифікат безпеки (CA) та додатковий ключ аутентифікації заголовків HMAC (ta.key) для захисту від DOS-атак.

Після завершення інтеграції та запуску тунелів у всіх структурних підрозділах, персонал банку отримує захищений, низьколатентний канал для стабільного функціонування підсистем «Клієнт-Банк», сервісів термінального доступу (Windows Terminal Services), віддаленого адміністрування та внутрішніх закритих баз даних.

3.1.2 Інструкції з налаштування файлового сервера

Організація централізованого обміну документацією та збереження резервних копій у межах локальної обчислювальної мережі банківської філії реалізується за допомогою розгортання виділеної служби файлового обміну. Як базовий технологічний стек у проєкті використано протокол передачі файлів FTP (File Transfer Protocol), який функціонує на прикладному рівні моделі OSI та забезпечує високу швидкість обробки великих масивів даних. В ролі програмної платформи обрано безпечний, легковагий та стійкий до навантажень демон vsftpd (Very Secure FTP Daemon), який інтегрується в операційну систему FreeBSD на сервері S_1 з виділеною IP-адресою 172.16.14.10.

Управління політиками доступу та безпекою файлового сховища базується на розподілі прав користувачів, ізоляції їхніх робочих каталогів та веденні детальних логів транзакцій. Для цього в системі розгортається така структура конфігураційних файлів:

- user_list містить вичерпний перелік облікових записів персоналу банку, яким санкціоновано доступ до FTP-сервера.

- chroot_list визначає список користувачів, які підлягають безумовній ізоляції у своїх домашніх директоріях без права виходу в кореневу файлову систему сервера (технологія chroot-ізоляції).

Для гнучкого розмежування повноважень між різними відділами банку (наприклад, кредитним, депозитним чи юридичним) у системі створюється спеціалізований каталог /usr/local/etc/vsftpd/vusers/. У цій директорії формуються індивідуальні конфігураційні файли для кожного працівника або робочої групи, де прописуються персональні права на читання, запис та модифікацію даних.

Наприклад, для авторизованого співробітника юридичного відділу з логіном user113 створюється однойменний файл /usr/local/etc/vsftpd/vusers/user113, у який вноситься директива визначення індивідуального кореневого каталогу:

local_root=/var/ftp/user113

У межах цієї директорії адміністратор мережі вибудовує чітку деревоподібну структуру папок із відповідними правами доступу, що унеможливлює несанкціоноване ознайомлення персоналу з конфіденційною інформацією суміжних підрозділів фінансової установи.

Нижче наведено конфігураційний файл файлового сервера.

Головний файл налаштувань служби /usr/local/etc/vsftpd.conf, оптимізований під архітектуру мережі філії банку та вимоги безпеки, має такий вигляд:

```
! Основні системні параметри запуску
listen=YES
listen_address=172.16.14.10
pam_service_name=vsftpd
! Контроль автентифікації та політика анонімного доступу
anonymous_enable=NO
local_enable=YES
write_enable=YES
! Сувора заборона для неавторизованих завантажень
anon_upload_enable=NO
anon_mkdir_write_enable=NO
anon_other_write_enable=NO
anon_root=/var/ftp/anonymous
! Налаштування підключень та портів
dirmessage_enable=YES
connect_from_port_20=YES
chown_uploads=YES
chown_username=ftp
! Логування та аудит операцій з файлами (вимога безпеки банку)
xferlog_enable=YES
xferlog_file=/var/log/vsftpd.log
! Оптимізація сесій та тайм-аутів
idle_session_timeout=600
data_connection_timeout=12000
nopriv_user=ftp
! Заборона вразливого ASCII режиму передачі для бінарних файлів
ascii_upload_enable=NO
ascii_download_enable=NO
ftpd_banner=Welcome to Bank Branch Secure FTP Server.
```

```
! Розмежування прав за допомогою індивідуальних конфігурацій
user_config_dir=/usr/local/etc/vsftpd/vusers
! Налаштування chroot-ізоляції локальних користувачів
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/usr/local/etc/vsftpd/chroot_list
! Активація білих списків доступу
userlist_file=/usr/local/etc/vsftpd/user_list
userlist_enable=YES
userlist_deny=NO
```

Ініціалізація та керування службою у FreeBSD

На відміну від ОС Linux, керування демонами та сервісами в операційній системі FreeBSD реалізовано через підсистему rc.d. Для активації автоматичного старту файлового сервера під час завантаження апаратної платформи S_1 до системного конфігуратора /etc/rc.conf додається такий параметр:

```
vsftpd_enable="YES"
```

Запуск файлової служби у поточному сеансі роботи без перезавантаження операційної системи виконується адміністратором за допомогою штатної утиліти керування сервісами:

```
# service vsftpd start
```

Для оперативного внесення змін у конфігураційні файли або оновлення списків користувачів перезапуск демона здійснюється командою:

```
# service vsftpd restart
```

Впровадження сервера vsftpd із зазначеним рівнем конфігурування дозволяє повністю задовольнити потреби філії банку у захищеному, підконтрольному та високошвидкісному обміні службовою інформацією, мінімізуючи ризики витоку комерційних даних через внутрішні канали ЛОМ.

3.2 Інструкції з налаштування активного комутаційного обладнання

3.2.1 Інструкції з налаштування центрального комутатора ядра філії

Перейдемо безпосередньо до налаштування віртуальних локальних мереж (VLAN) та міжвекторної маршрутизації (Inter-VLAN Routing) на центральному комутаторі ядра філії, використовуючи інтерфейс командного рядка (CLI). На початковому етапі конфігурування задається максимальна кількість підтримуваних VLAN, що відповідає технічним характеристикам обраного комутатора TP-Link T3700G-52TQ:

```
SW_2(config)# max-vlans 64
```

Наступним кроком є створення ідентифікаторів віртуальних мереж та конфігурування фізичних портів доступу (Access Ports) для пристроїв, які підімкнені до комутатора ядра напряму (сервери, керівництво, секретар, відділ цінних паперів):

```
! Налаштування портів для серверної групи (VLAN 14)
SW_2(config)# interface range gigabitEthernet 1/0/1-2
SW_2(config-if-range)# switchport mode access
SW_2(config-if-range)# switchport access vlan 14
SW_2(config-if-range)# exit
! Налаштування порту секретаня (VLAN 15)
SW_2(config)# interface gigabitEthernet 1/0/3
SW_2(config-if)# switchport mode access
SW_2(config-if)# switchport access vlan 15
SW_2(config-if)# exit
! Налаштування порту директора філії (VLAN 16)
SW_2(config)# interface gigabitEthernet 1/0/4
```

SW_2(config-if)# switchport mode access

SW_2(config-if)# switchport access vlan 16

SW_2(config-if)# exit

! Налаштування портів відділу цінних паперів (VLAN 17)

SW_2(config)# interface range gigabitEthernet 1/0/5-9

SW_2(config-if-range)# switchport mode access

SW_2(config-if-range)# switchport access vlan 17

SW_2(config-if-range)# exit

Оскільки архітектура мережі побудована за ієрархічним принципом, комутатор ядра з'єднується з периферійними комутаторами поверхів та робочих груп за допомогою магістральних транкових портів (Trunk Ports). На цих інтерфейсах дозволяється проходження відповідного тегованого трафіку:

! Конфігурування магістральних лінків (Trunk) до SW_1, SW_3, SW_4, SW_5, SW_6, SW_7

SW_2(config)# interface range gigabitEthernet 1/0/11-16

SW_2(config-if-range)# switchport mode trunk

SW_2(config-if-range)# switchport trunk allowed vlan all

SW_2(config-if-range)# exit

Для забезпечення високошвидкісної апаратної маршрутизації пакетів між різними підрозділами банку (Inter-VLAN) на базі комутатора 3-го рівня (L3), створюються віртуальні інтерфейси керування (SVI). Кожному інтерфейсу присвоюється унікальна IP-адреса, яка виступає як шлюз за замовчуванням (Default Gateway) для кінцевих робочих станцій відповідного відділу:

SW_2(config)# interface vlan 11

SW_2(config-if)# ip address 172.16.11.1 255.255.255.0

SW_2(config-if)# exit

SW_2(config)# interface vlan 13

SW_2(config-if)# ip address 172.16.13.1 255.255.255.0

```
SW_2(config-if)# exit
SW_2(config)# interface vlan 14
SW_2(config-if)# ip address 172.16.14.1 255.255.255.0
SW_2(config-if)# exit
SW_2(config)# interface vlan 15
SW_2(config-if)# ip address 172.16.15.1 255.255.255.0
SW_2(config-if)# exit
SW_2(config)# interface vlan 16
SW_2(config-if)# ip address 172.16.16.1 255.255.255.0
SW_2(config-if)# exit
SW_2(config)# interface vlan 17
SW_2(config-if)# ip address 172.16.17.1 255.255.255.0
SW_2(config-if)# exit
SW_2(config)# interface vlan 18
SW_2(config-if)# ip address 172.16.18.1 255.255.255.0
SW_2(config-if)# exit
SW_2(config)# interface vlan 19
SW_2(config-if)# ip address 172.16.19.1 255.255.255.0
SW_2(config-if)# exit
SW_2(config)# interface vlan 20
SW_2(config-if)# ip address 172.16.20.1 255.255.255.0
SW_2(config-if)# exit
SW_2(config)# interface vlan 21
SW_2(config-if)# ip address 172.16.21.1 255.255.255.0
SW_2(config-if)# exit
SW_2(config)# interface vlan 22
SW_2(config-if)# ip address 172.16.22.1 255.255.255.0
SW_2(config-if)# exit
SW_2(config)# interface vlan 23
```

SW_2(config-if)# ip address 172.16.23.1 255.255.255.0

SW_2(config-if)# exit

SW_2(config)# interface vlan 24

SW_2(config-if)# ip address 172.16.24.1 255.255.255.0

SW_2(config-if)# exit

! Налаштування захищеного сегмента керування комутаторами (Management)

SW_2(config)# interface vlan 100

SW_2(config-if)# ip address 172.16.100.1 255.255.255.0

SW_2(config-if)# exit

Для активації функцій маршрутизатора та об'єднання всіх ізольованих сегментів у загальну інфраструктуру філії, вмикається глобальний режим маршрутизації IP-пакетів. Після цього задається статичний маршрут за замовчуванням (маршрут останньої надії), який перенаправляє весь зовнішній Інтернет-трафік та запити до корпоративної мережі банку на внутрішній інтерфейс програмного шлюзу безпеки під керуванням операційної системи FreeBSD (сервер S_2):

! Активація функції L3 маршрутизації

SW_2(config)# ip routing

! Задання статичного шлюзу за замовчуванням на IP-адресу сервера FreeBSD

SW_2(config)# ip route 0.0.0.0 0.0.0.0 172.16.14.254

Перегляд повної інформації про стан створених віртуальних мереж, прив'язку фізичних портів та активні транкові з'єднання здійснюється за допомогою діагностичної команди:

SW_2# show vlan

Крім вищеописаних базових налаштувань комутації, обов’язковими для банківської установи є створення локальних облікових записів адміністраторів із високим рівнем привілеїв, задання точних параметрів дати

та синхронізації часу за протоколом NTP, а також увімкнення логування повідомлень комутатора на віддалений Syslog-сервер для оперативного відстеження нештатних подій інформаційної безпеки.

3.2.2 Інструкції з налаштування комутаторів робочих груп

Конфігурування комутаторів рівня доступу (периферійних комутаторів робочих груп та поверхів) є критично важливим етапом для забезпечення кінцевої ізоляції користувацького трафіку та безпеки точок підключення до ЛОМ банку. У межах проєкту на цьому рівні розгортаються керовані комутатори серій TP-Link TL-SG2008 та TL-SG2216.

Процес їхнього системного налаштування реалізується через інтерфейс командного рядка (CLI) і розподіляється на такі послідовні технічні етапи:

Забезпечення безпеки та адміністрування (Management): Створення локального облікового запису системного адміністратора з максимальним рівнем привілеїв, призначення статичної IP-адреси управління з виділеного сегмента Management VLAN 100, а також активація захищеного протоколу віддаленого доступу SSH (із паралельним вимкненням вразливого протоколу Telnet).

Виконаємо конфігурування магістральних та користувацьких інтерфейсів:

Режим Trunk (Магістральний порт): Один із гігабітних аплінк-портів кожного комутатора (згідно з розробленою топологією та таблицею комутації портів) переводиться в режим магістрального каналу для передачі тегованого трафіку між периферією та комутатором ядра SW_2. На ньому дозволяється проходження лише необхідних клієнтських VLAN та обов’язково тегованого VLAN 100 для управління.

Режим Access (Порти доступу): Створення локальної бази даних ідентифікаторів VLAN, що функціонують у межах конкретного поверху чи

відділу. Фізичні порти, до яких підключаються робочі станції персоналу, банкомати або термінали, переводяться в режим доступу (Access) із чіткою прив'язкою до одного конкретного нетегованого віртуального сегмента.

Синхронізація та моніторинг системи: Налаштування внутрішнього системного годинника пристроїв, визначення часового поясу та конфігурування автоматичної синхронізації часу за протоколом NTP (Network Time Protocol) з локальним сервером банку для коректного ведення журналів подій інформаційної безпеки.

Нижче наведено типовий базовий лістинг команд CLI для конфігурування комутатора доступу (на прикладі пристрою кредитного та депозитного відділів SW_4):

```
! 1. Обліковий запис, параметри безпеки та управління
SW_4(config)# username admin privilege 15 password strong_secure_pass
SW_4(config)# ip ssh server
SW_4(config)# ip telnet server disable
! Створення необхідних VLAN у базі даних комутатора
SW_4(config)# vlan 19
SW_4(config-vlan)# name Credit_Dept
SW_4(config-vlan)# exit
SW_4(config)# vlan 20
SW_4(config-vlan)# name Deposit_Dept
SW_4(config-vlan)# exit
SW_4(config)# vlan 100
SW_4(config-vlan)# name Management
SW_4(config-vlan)# exit
! Призначення IP-адреси управління у VLAN 100 та шлюзу
SW_4(config)# interface vlan 100
SW_4(config-if) # ip address 172.16.100.4 255.255.255.0
SW_4(config-if) # exit
```

```
SW_4(config)# ip default-gateway 172.16.100.1
! 2. Конфігурування портів доступу (Access Ports)
! Робочі станції кредитного відділу (VLAN 19)
SW_4(config)# interface range gigabitEthernet 1/0/1-4
SW_4(config-if-range)# switchport mode access
SW_4(config-if-range)# switchport access vlan 19
SW_4(config-if-range)# exit
! Робочі станції депозитного відділу (VLAN 20)
SW_4(config)# interface range gigabitEthernet 1/0/5-6
SW_4(config-if-range)# switchport mode access
SW_4(config-if-range)# switchport access vlan 20
SW_4(config-if-range)# exit
! 3. Конфігурування магістрального порту (Trunk Uplink до ядра)
SW_4(config)# interface gigabitEthernet 1/0/7
SW_4(config-if)# switchport mode trunk
SW_4(config-if)# switchport trunk allowed vlan 19,20,100
SW_4(config-if)# exit
! 4. Синхронізація часу та збереження конфігурації
SW_4(config)# ntp server 172.16.14.10 prefer
SW_4(config)# exit
SW_4# copy running-config startup-config
```

Аналогічним чином, відповідно до розроблених таблиць логічної адресації та конфігурування портів (Таблиці Б.1 та Б.2), адаптуються та застосовуються індивідуальні конфігураційні файли для решти комутаторів робочих груп (SW_1, SW_3, SW_5, SW_6, SW_7).

Такий підхід забезпечує уніфікацію конфігурації активного мережевого обладнання, спрощує його подальше адміністрування та мінімізує ймовірність виникнення помилок під час введення локальної мережі в експлуатацію.

3.3 Інструкція з використання тестових наборів та тестових програм

Верифікація працездатності та оцінка продуктивності розгорнутої банківської ЛОМ реалізується у два послідовні етапи:

Перший етап - апаратний контроль, тобто тестування цілісності та характеристик фізичних ліній зв'язку (структурованої кабельної системи) за допомогою цифрових кабельних тестерів.

Другий етап це програмно-логічний контроль, який передбачає перевірку коректності функціонування мережевих протоколів, активного комутаційного обладнання та операційних систем за допомогою вбудованого інструментарію (ping, netstat) та спеціалізованого кросплатформного ПЗ.

Для прецизійного вимірювання максимальної пропускної здатності та оцінки реальної місткості каналів зв'язку між сегментами філії у проєкті застосовано утиліту iperf. Дане програмне забезпечення функціонує за клієнт-серверною архітектурою і дозволяє генерувати синтетичний трафік для аналізу мережевих затримок і втрат пакетів.

Процедура тестування передбачає інсталяцію утиліти на два контрольні вузли мережі, один з яких ініціалізується як ресивер (сервер), а інший як генератор трафіку (клієнт). Клієнтський вузол здійснює спрямовану передачу потоку пакетів на сервер, який фіксує швидкість прийому та виводить підсумкові метрики в консоль обох пристроїв.

Для запуску утиліти на стороні сервера (наприклад, на файловому сервері S_1) виконується команда:

```
iperf -s
```

Для старту вимірювань із боку клієнтської робочої станції (наприклад, з кредитного відділу) у терміналі вказується IP-адреса хоста-ресивера:

```
iperf -c 172.16.14.10
```

Гнучке моделювання умов навантаження та детальний аналіз параметрів мережі забезпечується комбінуванням базових ключів конфігурації iperf

3.4 Інструкції по налаштуванню засобів захисту мережі

Для забезпечення цілісності, конфіденційності та доступності інформаційних ресурсів банківської установи, а також для здійснення глибокої фільтрації мережевого трафіку на периметрі, у проєкті розгорнуто штатний підсистемний міжмережевий екран операційної системи FreeBSD IPFW (IP Firewall). Цей засіб захисту функціонує на рівні ядра ОС і дозволяє реалізувати політику безпеки за принципом «stateful inspection» (фільтрація з урахуванням стану з'єднань).

Основним концептуальним підходом під час формування набору правил є архітектурний принцип «Default Deny» (заборонено все, що чітко не дозволено). Це мінімізує вектор атак на внутрішні сервери банку та захищає шлюз від несанкціонованого сканування чи спроб впровадження шкідливого коду.

Нижче наведено повністю вивірений та оптимізований конфігураційний скрипт захисту периметра шлюзу:

Bash

```
#!/bin/sh
# Визначення системних змінних для автоматизації конфігурації
fwcmd="/sbin/ipfw"
oif="em0"                 # Зовнішній мережевий інтерфейс шлюзу
iif="em1"                 # Внутрішній мережевий інтерфейс (LAN)
oip="194.44.15.2"         # Умовна зовнішня статична IP-адреса банку
lan="172.16.14.0/24"      # Логічний сегмент серверної зони філії
vpn_net="10.0.0.0/24"     # Діапазон віртуальної мережі OpenVPN
```

```
# Очищення поточної таблиці правил перед завантаженням нових
${fwcmd} -q flush
# 1. Перевірка динамічних станів (Stateful інспекція)
# Якщо з'єднання вже ініційоване та схвалено, пакет пропускається миттєво
${fwcmd} -q add 1 check-state
# 2. Локальний інтерфейс зворотного зв'язку (Loopback)
# Дозвіл внутрішнього трафіку для стабільної роботи системних служб шлюзу
${fwcmd} -q add 2 allow all from any to any via lo0
${fwcmd} -q add 3 deny all from any to 127.0.0.0/8
${fwcmd} -q add 4 deny all from 127.0.0.0/8 to any
# 3. Контроль цілісності пакетів
# Автоматичне повторне збирання фрагментованих IP-пакетів для запобігання DOS-атакам
${fwcmd} -q add 10 reass all from any to any in
# 4. Фільтрація вхідного трафіку на зовнішньому інтерфейсі (Inbound)
# Дозвіл захищеного віддаленого адміністрування по SSH (порт 22) лише для авторизованих вузлів
${fwcmd} -q add 100 allow tcp from any to ${oip} 22 in via ${oif} setup keep-state
# Дозвіл безпечного веб-доступу по HTTPS (порт 443) до публічних сервісів філії
${fwcmd} -q add 110 allow tcp from any to ${oip} 443 in via ${oif} setup keep-state
# Дозвіл вхідного UDP-трафіку для функціонування раніше налаштованого тунелю OpenVPN
${fwcmd} -q add 120 allow udp from any to ${oip} 1194 in via ${oif} keep-state
```

5. Фільтрація вихідного трафіку шлюзу та внутрішньої мережі (Outbound)

Дозвіл вихідних DNS-запитів (порт 53 UDP) для трансляції доменних імен

${fwcmd} -q add 200 allow udp from ${oip} to any 53 out via ${oif} keep-state

Дозвіл вихідних сесій по протоколах HTTP/HTTPS для оновлення ПЗ та зв'язку з НБУ

${fwcmd} -q add 210 allow tcp from ${oip} to any 80,443 out via ${oif} setup keep-state

Дозвіл вихідної синхронізації точного часу за протоколом NTP

${fwcmd} -q add 220 allow udp from ${oip} to any 123 out via ${oif} keep-state

6. Обробка службового трафіку ICMP (Діагностика мережі)

Дозвіл проходження пакетів ехо-запиту, ехо-відповіді та повідомлень про недоступність

${fwcmd} -q add 300 allow icmp from any to any icmptypes 0,3,8,11

7. Взаємодія між внутрішніми інтерфейсами

Безперешкодний пропуск легітимного трафіку з локальної мережі банку та VPN до шлюзу

${fwcmd} -q add 400 allow all from ${lan} to any via ${iif}

${fwcmd} -q add 410 allow all from any to ${lan} via ${iif}

${fwcmd} -q add 420 allow all from ${vpn_net} to any via ${iif}

8. Фінальне блокування (Реалізація політики Default Deny)

Усі інші пакети, які не підпали під жодне з вищевказаних правил, відкидаються

${fwcmd} -q add 999 deny log all from any to any

Пояснення архітектурних рішень скрипту:

Параметр keep-state: Під час реєстрації первинного пакета (наприклад, запиту до веб-сервера) брандмауер динамічно створює тимчасове правило у таблиці станів. Усі наступні пакети в межах цієї сесії обробляються першим правилом check-state, що значно знижує навантаження на центральний процесор шлюзу.

Логування (deny log): Фінальне правило не просто блокує несанкціоновану активність, а й заносить інформацію про порушника (IP-адресу, порт, час атаки) у системний журнал /var/log/security. Це дозволяє адміністраторам безпеки банку оперативно виявляти спроби несанкціонованого проникнення у внутрішній периметр.

Така конфігурація IPFW забезпечує надійний захист інформаційного контуру філії банку від зовнішніх кіберзагроз, зберігаючи високу пропускну здатність для корпоративних додатків.

3.5 Інструкції з експлуатації та моніторингу в мережі

Ефективне адміністрування, підтримка високого рівня відмовостійкості та оперативне усунення позаштатних ситуацій у локальній обчислювальній мережі філії банку потребують наявності актуального комплексу експлуатаційної документації. До базового пакета обов'язкових технічних документів, які передаються службі IT-підтримки, належать:

1. Схема логічної топології мережі, яка відображає взаємозв'язок між віртуальними підмережами (VLAN), межі маршрутизації, розподіл IP-адрес та логічну структуру інформаційних потоків.

2. Схема фізичної топології, що деталізує архітектуру укладання кабельних трас, траєкторії магістральних каналів, а також специфікацію та точне розміщення активного й пасивного комутаційного обладнання в серверних шафах.

План архітектурно-кабельного розміщення прив'язує елементи структурованої кабельної системи (СКС) та кінцеві інформаційні розетки до конкретних кабінетів, операційних кас та зон самообслуговування на плані поверхів будівлі.

Реєстр (таблиця) логічної адресації містить вичерпну інформацію про закріплені статичні та динамічні IP-адреси серверів, мережевих інтерфейсів комутаторів, шлюзів безпеки та шлюзів за замовчуванням для кожного робочого місця підрозділу банку.

Враховуючи динамічний розвиток фінансової установи та ймовірне розширення штату працівників, на етапі проектування СКС було закладено архітектурний резерв надійності. Для кожної робочої групи (відділів кредитування, депозитів, касової зони тощо) передбачено додаткові надлишкові точки підключення (резервні порти доступу на комутаторах та вільні лінії у комутаційних панелях). Це дозволяє масштабувати мережу та вводити в експлуатацію нові робочі станції користувачів без модернізації базової кабельної інфраструктури та зупинки бізнес-процесів філії.

Під час експлуатації мреежі важлива організація комплексного моніторингу мережевих процесів. Регулярний технічний моніторинг є невід'ємною частиною забезпечення інформаційної безпеки та безперервності функціонування банківських сервісів. Система моніторингу в розробленій ЛОМ базується на трьох основних технологічних рівнях:

1. Аналіз канального та мережевого рівнів активного обладнання. Цей рівень передбачає збір і моніторинг статистики роботи інтерфейсів, контроль пакетних помилок (CRC errors), моніторинг завантаження портів та стану магістральних транкових лінків здійснюється безпосередньо через вбудовану операційну систему центрального комутатора ядра SW_2 (TP-Link T3700G-52TQ).

2. Діагностика за допомогою інструментарію ОС та аудит лог-файлів. Застосування штатних утиліт моніторингу на серверних платформах під

керуванням FreeBSD та аналіз системних журналів подій для виявлення аномальної активності чи спроб несанкціонованого доступу.

3. Контроль метрик дискового сховища передбачає неперервний збір статистичних даних щодо інтенсивності операцій введення-виведення (IOPS), доступного дискового простору та швидкості обміну даними на файловому сервері S_1 (vsftpd), що запобігає збоям у процесі збереження банківської документації.

Детальніше опишемо структуру та локалізацію системних журналів (логів). Для проведення поточного та архівного аналізу мережевих подій та розслідування інцидентів безпеки, програмне забезпечення шлюзу формує деталізовані звіти. Конфігурацією передбачено ведення відокремленого журналу подій віртуальної приватної мережі openvpn-status.log, який локалізовано в системній директорії /var/log/. Цей файл оновлюється в режимі реального часу та містить інформацію про поточні активні тунелі з віддаленими філіями, автентифікованих користувачів, обсяги переданого трафіку та точний час сесій.

У цьому ж каталозі шлюзу на базі FreeBSD консолідуються ключові системні журнали операційної системи:

- messages загальносистемний журнал, куди записуються повідомлення від демонів, інформація про стан мережевих інтерфейсів, збої в роботі служб та загальні повідомлення ядра.

- secure спеціалізований журнал реєстрації подій підсистеми безпеки (фіксація успішних та неуспішних спроб авторизації по SSH, транзакцій підвищення привілеїв через команду su, робота механізмів PAM).

- dmesg буфер повідомлень ядра операційної системи, який відображає інформацію про виявлення апаратних компонентів шлюзу, ініціалізацію мережевих карт та низькорівневі системні події під час завантаження платформи.

Організація моніторингу за наведеною схемою дозволяє IT-персоналу банку здійснювати проактивне управління інфраструктурою, вчасно реагувати на деградацію каналів зв'язку та гарантувати високу доступність сервісів для клієнтів.

3.6 Моделювання роботи локальної обчислювальної мережі

Імітаційне моделювання розробленої телекомунікаційної інфраструктури є обов'язковим етапом проєктування, який дозволяє верифікувати коректність топологічних рішень, перевірити логічну сумісність інтерфейсів та підтвердити правильність налаштування політик маршрутизації до моменту фізичного розгортання мережі на об'єкті.

На сучасному етапі розвитку інформаційних технологій для аналізу архітектури ЛОМ застосовується спеціалізоване програмне забезпечення, зокрема:

- Netcracker Professional орієнтований на високорівневе бізнес-моделювання та візуалізацію кошторисів інфраструктури.

- OPNET Modeler (Riverbed Modeler) важкий аналітичний комплекс для дискретно-подієвого моделювання великих операторських мереж.

- Cisco Packet Tracer інтерактивний інструмент симуляції та емуляції мережевих процесів, який підтримуєstateful-інспекцію протоколів та детальне конфігурування систем через CLI.

У межах цього проєкту кваліфікаційної роботи для відтворення архітектури банківської філії було обрано програмний комплекс Cisco Packet Tracer, оскільки він надає повний спектр функціональних можливостей для емуляції мережевих протоколів прикладного, мережевого та канального рівнів моделі OSI. Зважаючи на те, що інтерфейс командного рядка (CLI) обраних у проєкті комутаторів ядра та доступу компанії TP-Link є синтаксично сумісним із загальноприйнятим промисловим стандартом Cisco

IOS, середовище Packet Tracer дозволяє з високою точністю відтворити роботу створених конфігураційних файлів, віртуальних інтерфейсів (SVI) та транкових магістралей.

Програма забезпечує повну емуляцію активного обладнання, стеків серверних платформ (DHCP, DNS, HTTP, FTP), кінцевих робочих станцій, а також фізичних середовищ передачі даних. Головною метою імітаційного моделювання є комплексна перевірка наявності зв'язку (Network Connectivity) між ізольованими сегментами VLAN та підтвердження працездатності міжвекторної маршрутизації (Inter-VLAN Routing) за допомогою протоколу керуючих повідомлень ICMP.

Спроектована та інтегрована у середовище Packet Tracer логічна структура локальної обчислювальної мережі філії представлена на рисунку 3.1.

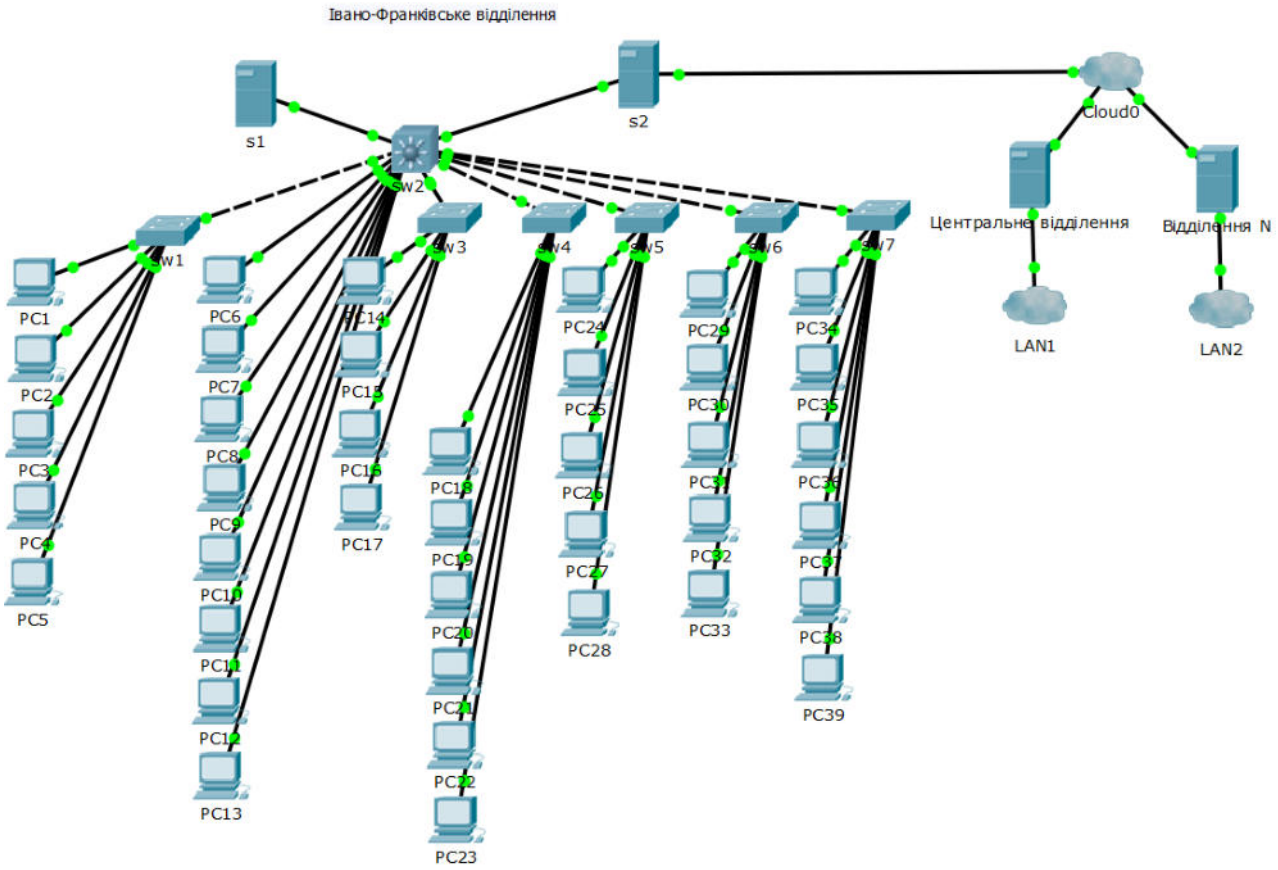


Рисунок 3.1 – Вигляд моделі мережі

Для проведення тестових випробувань виконано базове конфігурування параметрів стеку TCP/IP для двох контрольних точок мережі: робочої станції кредитного відділу PC1 (WS_1 у загальній топології) та центрального файлового сервера філії S_1.

Конфігураційні параметри вузла PC1 (VLAN 11), внесені в інтерфейс симулятора:

IP-адреса хоста: 172.16.11.2

Маска підмережі: 255.255.255.0

Шлюз за замовчуванням (інтерфейс ядра SW_2): 172.16.11.1

Адреса DNS-сервера: 172.16.14.10

Конфігураційні параметри файлового сервера S_1 (VLAN 14), внесені в інтерфейс симулятора:

IP-адреса хоста: 172.16.14.10

Маска підмережі: 255.255.255.0

Шлюз за замовчуванням (інтерфейс ядра SW_2): 172.16.14.1

Адреса DNS-сервера: 172.16.14.10 (локальний хост)

Перевірка доступності та проходження пакетів між різними віртуальними мережами через комутатор 3-го рівня реалізована за допомогою утиліти ping з консолі робочої станції PC1 у напрямку сервера. Під час моделювання пакет ICMP проходить через комутатор доступу, тегується ідентифікатором VLAN 11, надходить на транковий порт комутатора ядра SW_2, де маршрутизується на рівні L3 у VLAN 14 і доставляється до сервера S_1.

Нижче наведено лістинг результатів виконання діагностичної команди в емуляційному середовищі:

```
PC1> ping 172.16.14.10
Pinging 172.16.14.10 with 32 bytes of data:
Reply from 172.16.14.10: bytes=32 time<1ms TTL=63
Reply from 172.16.14.10: bytes=32 time<1ms TTL=63
```

Reply from 172.16.14.10: bytes=32 time<1ms TTL=63

Reply from 172.16.14.10: bytes=32 time<1ms TTL=63

Ping statistics for 172.16.14.10:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

Значення TTL=63 (Time to Live) чітко вказує на те, що пакет успішно пройшов через один маршрутизуючий пристрій (L3-комутатор ядра), який зменшив початкове значення TTL=64 на одиницю.

Аналіз отриманих статистичних даних свідчить про повну відсутність втрат пакетів (0% loss) та мінімальні затримки під час комутації. Результати імітаційного моделювання експериментально доводять стовідсоткову коректність налаштування параметрів стеку TCP/IP, правильність розробки таблиць адресації та повну працездатність обраної ієрархічної структури мережі банківської установи.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини кваліфікаційної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки комп'ютерної мережі для Івано-Франківського відділення АБ «Експрес-Банк» і прийняття рішення про її подальше впровадження в роботу.

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

Для визначення загальної тривалості проведення НДР дані витрат часу по окремих операціях технологічного процесу зводяться у таблицю 4.1.

Таблиця 4.1 - Середній час виконання НДР та стадій технологічного процесу

№ п/п	Назва стадії	Виконавець	Середній час виконання операції, год.
1	Постановка задачі та збір інформації про об'єкт	Керівник проекту	10
2	Розробка проекту	Інженер	10
3	Затвердження проекту	Керівник проекту	2
4	Монтаж мережі	Технік	28
5	Налагодження мережі, запуск в експлуатацію та створення технічної документації	Інженер	50
Разом			100

Сумарний час виконання операцій технологічного процесу, які будуть виконуватись для проектування, встановлення та запуск в експлуатацію даного проекту локальної мережі складає 100 годин.

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Оплата праці - грошовий вираз вартості і ціни робочої сили, який виступає у формі будь-якого заробітку, виплаченого керівником підприємства найманому працівникові за виконану роботу.

Заробітна плата працівника залежить від кінцевих результатів його роботи, регулюється податками і максимальними розмірами не обмежується.

Основна заробітна плата розраховується за формулою:

$$З_{осн.}=Т_с \cdot К_г\,, \qquad (4.1)$$

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

Рекомендовані тарифні ставки: керівник проекту – 260 грн./год., інженер – 210 грн./год., технік – 170 грн./год.

Отже, основна заробітна плата для:

1. Керівник проекту - $З_{осн1} = 12 \cdot 260 = 3120$ грн.
2. Інженер - $З_{осн2} = 60 \cdot 210 = 12600$ грн.
3. Технік - $З_{осн3} = 28 \cdot 170 = 4760$ грн.

Сумарна основна заробітна плата становить:

$$З_{осн} = 3120 + 12600 + 4760 = 20480\ грн.$$

Додаткова заробітна плата становить 10–15 % від суми основної заробітної плати та обчислюється за формулою 4.2.

$$З_{дод.}=З_{осн.} \cdot К_{допл.}\,, \qquad (4.2)$$

де $К_{допл.}$ – коефіцієнт додаткових виплат працівникам: 0,1 – 0,15.

Отже, додаткова заробітна плата по категоріях працівників становить:

1. Керівник проекту - $З_{дод1}$= 3120 · 0,12 = 374,4 грн.
2. Інженер - $З_{дод2}$ = 12600 · 0,12 = 1512 грн.
3. Технік - $З_{дод3}$ = 4760 · 0,12 = 571,2 грн.

Загальна додаткова заробітна плата становить:

$$З_{дод} = 374,4 + 1512 + 571,2 = 2457,6 \text{ грн.}$$

Звідси загальні витрати на оплату праці розраховуються за формулою 4.3:

$$В_{о.п.}=З_{осн.}+З_{дод.}, \quad (4.3)$$

$$В_{о.п}=20480 + 2457,6 = 22937,6 \text{ грн}$$

Необхідно визначити відрахування на соціальні заходи:

1. Фонд страхування на випадок безробіття – 1,6 %;
2. Фонд по тимчасовій втраті працездатності – 1,4 %;
3. Пенсійний фонд – 33,2 %;
4. Внески на страхування від нещасного випадку на виробництві та професійного захворювання - 1,4%.

Загальна сума зазначених відрахувань становить 37,6 22%.

Отже, сума відрахувань на соціальні заходи буде становити:

$$В_{с.з.}= ФОП \cdot 0,376, \quad (4.4)$$

де ФОП – фонд оплати праці, грн.

$$В_{с.з.}= 22937,6 \cdot 0,376 = 8624,54 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 - Зведені розрахунки витрат на оплату праці

№ п/п	Категорія прац.	Основна заробітна плата, грн.			Додатк. зароб. плата, грн.	Нараху в. на ФОП грн.	Всього витрати на оплату праці, грн.
		Тариф. ставка, грн.	К-сть відпр. год.	Факт. нарах. з/пл., грн.			
1	Керівник проекту	260	12	3120	374,4	-	-
2	Інженер	210	60	12600	1512	-	-
3	Технік	170	28	4760	571,2	-	-
Разом					2457,6	*8624,54*	31562,14

Отже, загальні витрати на оплату праці становлять 31562,14 грн.

4.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни (формула 4.5):

$$M_{Bi} = q_i \cdot p_i \qquad (4.5)$$

де q_i – кількість витраченого матеріалу i-го виду;

p_i – ціна матеріалу i-го виду.

Звідси, загальні матеріальні витрати можна визначити за формулою 4.6:

$$З_{м.в.} = \sum M_{Bi} \qquad (4.6)$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

№	Найменування обладнання та матеріалів	Од. вим.	Кількість	Ціна, грн.	Вартість, грн.
1	Магістральний комутатор третього рівня TP-Link T3700G-24TQ	шт.	1	30670	30670
2	Керований комутатор робочої групи TP-Link TL-SG2008	шт.	6	3200	19200
3	Керований комутатор доступу TP-Link TL-SG2216	шт.	1	4500	4500
4	Сервер файлових ресурсів ARTLINE Business R33	шт.	1	38000	38000
5	Сервер доступу до зовнішніх мереж ARTLINE Business R33	шт.	1	33000	33000
6	Джерело безперебійного живлення APC Smart-UPS 1500VA	шт.	1	16500	16500
7	Телекомунікаційна шафа 24U для центрального вузла мережі	шт.	1	15800	15800
8	Настінна комутаційна шафа 7U	шт.	6	4500	27000
9	Комутаційна панель на 24 порти Cat.6	шт.	1	4000	4000
10	Комутаційна панель на 16 портів Cat.6	шт.	6	3100	18600
11	Інформаційна розетка RJ-45 категорії 6	шт.	41	130	5330
12	З'єднувальний комутаційний шнур UTP Cat.6	шт.	45	60	2700
13	Кабель «вита пара» UTP Cat.6	м	610	26	15860
14	Кабельний канал пластиковий	м	123	70	8610
	Загальна вартість проєкту				**239770**

Загальна сума матеріальних витрат на розробку мережі становить 239770 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію одиниці обладнання розраховуються за формулою 4.7:

$$З_е = W \cdot T \cdot S \quad (4.7)$$

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Час роботи ПК над даним проектом становить 18 годин, споживана потужність - 0,5 кВт/год, вартість 1 кВт електроенергії – 15,94 грн.

Тому витрати на електроенергію будуть становити:

$$З_е = 0,5 \cdot 18 \cdot 15.94 = 143.36 \ грн.$$

4.5 Визначення транспортних затрат

Транспортні витрати слід прогнозувати у розмірі 8 – 10 % від загальної суми матеріальних затрат. Транспортні витрати розраховуються за формулою 4.8.

$$Т_в = З_{м.в.} \cdot 0,08...0,1, \quad (4.8)$$

де $Т_в$ – транспортні витрати.

Отже, транспортні витрати будуть становити:

$$Т_в = 239770 \cdot 0,08 = 19181.6 \ грн.$$

4.6 Розрахунок суми амортизаційних відрахувань

Комп’ютери та оргтехніка належать до четвертої групи основних фонді. Мінімально допустимі строки їх використання 2 роки. Для визначення амортизаційних відрахувань використовуємо формулу:

$$A = \frac{Б_В \cdot Н_А}{150\%} \cdot Т, \quad (4.9)$$

де $А$ – амортизаційні відрахування за звітний період, грн.

$Б_В$ – балансова вартість групи основних фондів на початок звітного періоду, грн.;

$Н_А$ – норма амортизації, %;

$Т$ – кількість годин роботи обладнання, год.

Враховуючи, що ПК працює над даним проектом 18 год., балансова вартість ПК – 25400 грн., тому:

$$A = \frac{25400 \cdot 0{,}05}{150} \cdot 18 = 152{,}40 \text{ грн.}$$

4.7 Обчислення накладних витрат

Накладні витрати - це витрати, не пов'язані безпосередньо з технологічним процесом виготовлення продукції, а утворюються під впливом певних умов роботи по організації, управлінню та обслуговуванню виробництва.

В залежності від організаційно-правової форми діяльності господарюючого суб’єкта, накладні витрати можуть становити 20 – 60 % від суми основної та додаткової заробітної плати працівників, обчислюються за формулою 4.10.

$$Н_в = В_{о.п.} \cdot 0{,}2...0{,}6, \quad (4.10)$$

де, $Н_в$ – накладні витрати.

$$Н_в = 22\,937{,}60 \cdot 0{,}3 = 6881{,}28 \text{ грн.}$$

4.8 Складання кошторису витрат та визначення собівартості НДР

Кошторис витрат являє собою зведений план усіх витрат підприємства на майбутній період виробничо-фінансової діяльності.

Результати проведених вище розрахунків зведемо у таблиці 4.4.

Таблиця 4.4 - Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
Витрати на оплату праці	22937,6	7,71
Відрахування на соціальні заходи	8624,54	2,90
Матеріальні витрати	239770	80,54
Витрати на електроенергію	143,36	0,05
Транспортні витрати	19181,60	6,44
Амортизаційні відрахування	152,40	0,05
Накладні витрати	6881,*28*	2,31
Собівартість	297 690,78	100,00

Собівартість (C_B) НДР розрахуємо за формулою 4.11:

$$C_в = B_{о.п.} + B_{с.з.} + З_{м.в.} + З_в + Т_в + А + Н_в \quad (4.11)$$

Отже, собівартість дорівнює: $C_в$= 297 690,78 *грн.*

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою 4.12:

$$Ц = C_в \cdot (1 + Р_{рен}) \cdot (1 + ПДВ), \quad (4.12)$$

де $C_в$ – собівартість виконання НДР;

$P_{рен.}$ – рівень рентабельності, 30 %

ПДВ – ставка податку на додану вартість, 20 %.

$$Ц = 297\,690{,}78 \cdot (1+0{,}2) \cdot (1+0{,}2) = 428674{,}73 \text{ грн.}$$

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва - категорія, яка характеризує результативність виробництва. Вона свідчить не лише про приріст обсягів виробництва, а й про те, якими витратами ресурсів досягається цей приріст, тобто свідчить про якість економічного зростання.

Прибуток розраховується за формулою:

$$П = Ц - C_в \qquad (4.13)$$

$$П = 357228{,}94 - 297690{,}78 = 59538{,}16 \text{ грн.}$$

Економічна ефективність ($E_р$) полягає у відношенні результату виробництва до затрачених ресурсів і розраховується за формулою 4.14.

$$E_р = П / C_в, \qquad (4.14)$$

де $П$ – прибуток;

$C_в$ – собівартість.

$$E_р = 59538{,}16 / 297690{,}78 = 0{,}20$$

Поряд із економічною ефективністю розраховують (формула 4.15) термін окупності капітальних вкладень ($T_р$):

$$T_р = 1 / E_р \qquad (4.15)$$

Допустимим вважається термін окупності до 5 років. В даному випадку

$$T_р=1/0,2 =5.$$

Всі дані розрахунків внесемо в зведену таблицю 4.5 техніко-економічних показників.

Таблиця 4.5 - Техніко-економічні показники розробки мережі

№ п/п	Показник	Значення
1.	Собівартість, грн.	297 690,78 грн.
2.	Плановий прибуток, грн.	59 538,16 грн.
3.	Ціна, грн.	428 674,73 грн.
4.	Економічна ефективність	0,2
5.	Термін окупності, рік	5

Загальна вартість розробки комп'ютерної мережі становить 428 674,73 грн (з урахуванням ПДВ). Розрахунок кошторису показав, що основну частку витрат (понад 80%) формують матеріальні ресурси, необхідні для побудови інфраструктури.

Аналіз економічної ефективності проекту підтверджує його доцільність:

- коефіцієнт економічної ефективності ($E_р$) становить 0,20, що свідчить про рентабельність інвестицій на рівні 20%;

- термін окупності капітальних вкладень ($T_р$) складає 5 років, що є прийнятним показником для проектів такого масштабу, враховуючи тривалий термін експлуатації мережевого обладнання та стабільність очікуваних результатів.

Завдяки високому рівню технічного оснащення та оптимізації витрат на етапі впровадження, проект є економічно обґрунтованим і перспективним для подальшої реалізації.

5 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ ТА ОСНОВИ ОХОРОНИ ПРАЦІ

На даний час широке розповсюдження отримали персональні комп'ютери. Однак їх використання загострило проблеми збереження власного та суспільного здоров'я, вимагає удосконалення існуючих та розробки нових підходів до організації робочих місць, проведення профілактичних заходів для запобігання розвитку негативних наслідків впливу ПК на здоров'я користувачів. Відповідно до Закону України «Про охорону праці» «Охорона праці – це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих назбереження життя, здоров'я і працездатності людини в процесі трудової діяльності [2].

Заходи з охорони праці користувачів ПК необхідно розглядати в трьох основних аспектах: соціальному, психологічному та медичному. У соціальному плані розв'язання цих проблем пов'язане з оптимізацією умов життя, праці, відпочинку, харчування, побуту, розвитком культури, транспорту.

5.1 Організація пожежної безпеки на відділенні Львівської філії АБ «Експрес-Банк»

Пожежна безпека об'єкта - стан об'єкта, за якого з регламентованою імовірністю виключається можливість виникнення і розвитку пожежі та впливу на людей її небезпечних факторів, а також забезпечується захист матеріальних цінностей. Основними напрямками забезпечення пожежної безпеки є усунення умов виникнення пожежі та мінімізація її наслідків. [2].

Зокрема, цю сферу регламентують Правила пожежної безпеки в Україні, затверджені наказом Міністерства внутрішніх справ України, зі змінами, які періодично вносяться відповідними наказами [2].

Зафіксовані на законодавчому рівні вимоги пожежної безпеки зобов'язані виконувати – незалежно від приналежності та розміру статутного капіталу, обороту, кількості співробітників, форми власності, кодів ЗЕД, сфери роботи та інших аспектів – будь-які суб'єкти, що ведуть свою господарську діяльність на українській території.

Тому необхідно бути в курсі цих змін і коригувати організаційну роботу в даному секторі на виробництвах і в компаніях.

А для цього слід регулярно проводити моніторинг нормативної бази та проходити відповідне навчання, щоб оновити не лише теоретичну базу, а й практичні навички співробітників.

Пожежна безпека входить в комплекс заходів з охорони праці, і організаційна робота в цій сфері на об'єктах господарювання включає широкий спектр заходів, а саме:

- створення умов для безпечної праці,
- мінімізації ризику виникнення пожеж,
- своєчасне і повноцінне забезпечення технічними засобами для запобігання займання та усунення самих пожеж та їх наслідків,
- контроль дотримання протипожежних вимог і норм законодавства,
- розробка і впровадження регламентів по гасінню пожеж, евакуації та порятунку з місць пожежі й задимлення людей і майна (матеріальних цінностей),
- внутрішнє і зовнішнє навчання співробітників [3].

У разі, якщо підприємство орендує площі в іншої особи, сторони повинні в письмовій формі домовитися про те, хто з них і на яких умовах здійснює ці роботи.

Вимоги до пожежної безпеки на підприємстві неухильно повинен дотримуватися кожен співробітник, а організаційна складова при цьому покладається на посадових осіб за відповідним рішенням керівництва і прописується в посадових інструкціях і положеннях по структурним підрозділам.

Важливою складовою протипожежного режиму на будь-якому об’єкті є розробка і впровадження порядку дій при виникненні пожежі. Неодмінно має бути план евакуації, описано, як повинні відключатися електроустановки, що і в якій послідовності необхідно робити співробітникам.

Відповідно, для кожного об’єкта, кожного приміщення (крім коридорів, санвузлів, басейнів і подібних приміщень), окремих видів робіт складаються інструкції, за якими повинен працювати персонал, залучений на певних ділянках і в виконанні окремих видів робіт. За інструкціями проводиться навчання (інструктаж) персоналу з подальшим контролем знань.

Для ліквідації невеликих осередків пожежі, а також для гасіння пожеж на початковій стадії їх розвитку (до прибуття штатних підрозділів пожежної охорони) призначені первинні засоби пожежогасіння.

В даному випадку вибрано вогнегасники ВВК-5, які містять 5 кілограм закачаного порошку (див. рис. 5.1).

Рисунок 5.1 – Вогнегасник ВВК-5

Вогнегасники слід установлювати в легкодоступних місцях (у коридорах, біля входів або виходів із приміщень тощо) та на видноті, а також у пожежонебезпечних місцях, де найімовірнішою є поява осередків пожежі [1]. При цьому слід забезпечити їх захист від потрапляння прямих сонячних променів та безпосередньої (без загороджувальних щитків) дії опалювальних і нагрівальних приладів. Переносні вогнегасники мають розміщуватися шляхом навішування їх на вертикальні конструкції на висоті не більше 1,5 м від рівня підлоги до нижнього торця вогнегасника та на відстані од дверей, достатній для їх повного відчинення, або встановлення в пожежних шафах поряд із пожежними кранами, в спеціальних тумбах або на пожежних щитах (стендах).

З метою забезпечення пожежної безпеки персоналу та відвідувачів банківського відділення розроблено план евакуації людей на випадок виникнення пожежі, який наведено на рисунку 5.2. План містить схеми першого та другого поверхів будівлі із зазначенням основних шляхів евакуації, місць розташування первинних засобів пожежогасіння та інших елементів протипожежного захисту.

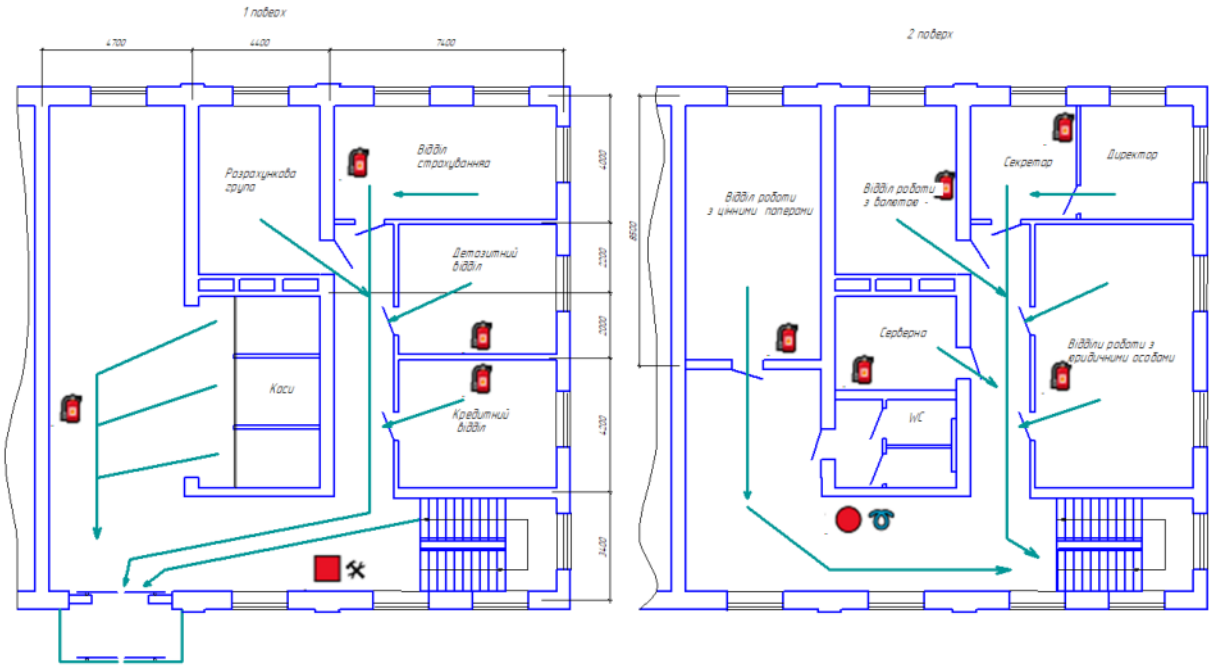


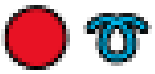
Рисунок 5.2 – План евакуації з приміщень відділення

Основним шляхом евакуації для працівників першого поверху є вихід через центральний вхід будівлі. Для персоналу другого поверху передбачено евакуацію сходовою кліткою до першого поверху з подальшим виходом через центральний евакуаційний вихід. Напрямки руху позначені стрілками, що забезпечує швидке орієнтування працівників у разі виникнення надзвичайної ситуації.

Умовні позначення на плані евакуації :

Вогнегасник ВВК-5

Пожежний щит



Пожежний рукав

У процесі розроблення плану особливу увагу приділено забезпеченню безперешкодного доступу до евакуаційних шляхів. Коридори, сходові марші та виходи повинні постійно утримуватися вільними від меблів, обладнання та інших предметів, які можуть перешкоджати евакуації людей. Двері евакуаційних виходів повинні відчинятися у напрямку виходу з будівлі та не блокуватися сторонніми предметами.

Первинні засоби пожежогасіння розміщено у найбільш доступних місцях поблизу робочих приміщень, коридорів та серверної кімнати. Таке розташування дозволяє оперативно ліквідувати осередок займання на початковій стадії його розвитку. Для гасіння електрообладнання, серверів, мережевих комутаторів та іншої комп'ютерної техніки рекомендується застосовувати вуглекислотні вогнегасники, використання яких не призводить до пошкодження електронної апаратури. В адміністративних приміщеннях можуть також використовуватися порошкові вогнегасники, призначені для ліквідації пожеж класів A, B, C та електроустановок, що перебувають під напругою.

У разі виявлення пожежі працівник повинен негайно повідомити пожежно-рятувальну службу за номером 101, поінформувати відповідальну особу банку, за можливості відключити електроживлення пошкодженої ділянки мережі та розпочати евакуацію людей відповідно до затвердженого плану. За відсутності безпосередньої загрози життю допускається використання первинних засобів пожежогасіння для ліквідації займання на початковій стадії. Після залишення будівлі працівники повинні зібратися у визначеному безпечному місці та провести перевірку присутності персоналу.

Запропонований план евакуації забезпечує організоване виведення людей із будівлі, скорочує час евакуації та сприяє підвищенню рівня пожежної безпеки банківського відділення відповідно до вимог чинних нормативних документів.

5.2 Організація безпечного виконання робіт під час монтажу структурованої кабельної системи у приміщеннях банку

Монтаж структурованої кабельної системи (СКС) є одним із найвідповідальніших етапів створення комп'ютерної мережі банківської установи, оскільки від якості виконання монтажних робіт залежить надійність функціонування інформаційної інфраструктури, безперервність роботи мережевих сервісів та безпека працівників. Під час виконання монтажу необхідно забезпечити дотримання вимог нормативних документів з охорони праці, електробезпеки, пожежної безпеки, а також рекомендацій щодо побудови структурованих кабельних систем.

До виконання монтажних робіт допускаються лише працівники, які пройшли первинний інструктаж з охорони праці, навчання безпечним методам виконання робіт, перевірку знань вимог електробезпеки та ознайомлені з особливостями експлуатації електротехнічного обладнання. Усі роботи повинні виконуватися відповідно до затвердженого плану виконання

монтажу, що визначає послідовність операцій, склад виконавців та заходи щодо мінімізації виробничих ризиків.

Перед початком монтажу необхідно провести огляд приміщень банку, визначити місця розташування телекомунікаційних шаф, комутаційних вузлів, інформаційних розеток та кабельних трас. Особлива увага приділяється перевірці технічного стану приміщень, відсутності механічних пошкоджень будівельних конструкцій, справності систем освітлення, вентиляції та електроживлення. Робоча зона повинна бути очищена від сторонніх предметів, які можуть ускладнювати виконання робіт або створювати небезпеку травмування персоналу.

Монтаж структурованої кабельної системи повинен виконуватися із застосуванням справного та сертифікованого інструменту. Для різання кабелю, зняття ізоляції, обтискання конекторів RJ-45 та монтажу комутаційних панелей використовуються спеціалізовані монтажні інструменти, що забезпечують якісне виконання з'єднань без пошкодження жил кабелю. Забороняється використовувати несправний інструмент, який має механічні пошкодження, порушену ізоляцію або дефекти ріжучих елементів.

Під час прокладання кабельних ліній необхідно дотримуватися вимог стандартів структурованих кабельних систем. Кабелі повинні прокладатися у пластикових кабельних коробах або металевих кабельних лотках із забезпеченням можливості їх подальшого технічного обслуговування. Не допускається прокладання кабелів із надмірним механічним натягом, різкими перегинами або скручуванням, оскільки це призводить до погіршення електричних характеристик кабелю та зменшення терміну його експлуатації.

Особливу увагу необхідно приділяти дотриманню мінімального радіуса вигину кабелю категорії 6. Перевищення допустимого згину може викликати порушення геометрії витих пар, збільшення перехресних наведень та погіршення параметрів передачі даних. Крім цього, необхідно уникати

надмірного розкручування витих пар під час монтажу інформаційних розеток і патч-панелей, що забезпечує відповідність лінії вимогам категорії Cat.6.

Кабельні траси повинні прокладатися окремо від силових електричних мереж. При паралельному прокладанні необхідно витримувати нормативну відстань між силовими та інформаційними кабелями або використовувати спеціальні перегородки в кабельних коробах. Таке рішення дозволяє мінімізувати вплив електромагнітних завад і забезпечити стабільність передачі інформації між мережевими пристроями.

Під час монтажу телекомунікаційних шаф необхідно забезпечити їх надійне кріплення до будівельних конструкцій та можливість безпечного доступу до встановленого обладнання. Розміщення комутаторів, патч-панелей, джерел безперебійного живлення та серверного обладнання повинно виконуватися з урахуванням допустимого тепловиділення, вентиляції та зручності проведення подальших профілактичних робіт. Електроживлення активного мережевого обладнання здійснюється через окремі захищені електричні кола із застосуванням пристроїв захисного заземлення та автоматичного захисту від перевантаження і короткого замикання.

Під час виконання монтажних робіт особлива увага приділяється дотриманню вимог електробезпеки. Установлення інформаційних розеток, комутаційних панелей, мережевих комутаторів, джерел безперебійного живлення та іншого обладнання повинно виконуватися лише після перевірки відсутності напруги на електричних колах. Підключення активного мережевого обладнання до системи електроживлення здійснюється після завершення монтажних робіт та перевірки правильності виконаних електричних з'єднань. Під час роботи із електрообладнанням працівники повинні використовувати інструмент з ізольованими ручками та дотримуватися вимог чинних правил безпечної експлуатації електроустановок.

Монтаж кабельних трас у верхній частині приміщень, над підвісними стелями або на висоті виконується із застосуванням справних драбин чи пересувних помостів. Перед початком роботи необхідно перевірити стійкість установленої драбини, справність її опор та відсутність механічних пошкоджень. Забороняється виконувати монтаж, стоячи на випадкових предметах, меблях або обладнанні, а також працювати з верхніх сходинок драбини без забезпечення стійкого положення працівника. Якщо роботи виконуються у місцях інтенсивного пересування персоналу або клієнтів банку, робочу зону необхідно огородити попереджувальними стрічками та встановити відповідні інформаційні знаки.

Для запобігання виробничому травматизму працівники повинні бути забезпечені необхідними засобами індивідуального захисту. Під час монтажу використовуються захисний спецодяг, робоче взуття з неслизькою підошвою, діелектричні рукавички при роботі поблизу електрообладнання, а також захисні окуляри під час свердління стін, монтажу кабельних каналів і виконання інших робіт, пов'язаних із можливим утворенням пилу або дрібних уламків будівельних матеріалів.

Важливою складовою безпечного виконання робіт є дотримання вимог пожежної безпеки. Кабельні траси не повинні перекривати евакуаційні виходи, пожежні проходи та доступ до первинних засобів пожежогасіння. Під час виконання монтажу необхідно використовувати кабелі та комплектуючі, що відповідають вимогам пожежної безпеки та мають відповідні сертифікати. У серверних приміщеннях і телекомунікаційних вузлах повинні бути встановлені вуглекислотні або порошкові вогнегасники, придатні для гасіння електрообладнання, що перебуває під напругою. Забороняється накопичувати легкозаймисті матеріали, пакувальну тару та відходи монтажу поблизу електротехнічного обладнання.

Після завершення монтажу проводиться комплексна перевірка структурованої кабельної системи. Контролюється правильність прокладання

кабельних ліній, якість кріплення кабельних коробів, надійність монтажу інформаційних розеток, патч-панелей і телекомунікаційних шаф. За допомогою кабельних тестерів перевіряється цілісність усіх ліній зв'язку, правильність розведення контактів відповідно до обраної схеми обтискання та відповідність основних параметрів вимогам категорії 6. Виявлені дефекти усуваються до введення мережі в експлуатацію.

Перед початком експлуатації проводиться функціональне тестування активного мережевого обладнання, перевіряється працездатність комутаторів, серверів, джерел безперебійного живлення та мережевих сервісів. Окремо контролюється правильність функціонування віртуальних локальних мереж (VLAN), доступність мережевих ресурсів і стабільність передачі даних між усіма сегментами комп'ютерної мережі. Результати перевірок оформлюються відповідною технічною документацією.

Таким чином, дотримання вимог охорони праці, електробезпеки та пожежної безпеки під час монтажу структурованої кабельної системи забезпечує безпечні умови праці для персоналу, знижує ризик виникнення аварійних ситуацій і сприяє створенню надійної мережевої інфраструктури банківської установи. Виконання монтажних робіт відповідно до нормативних вимог гарантує високу якість інсталяції структурованої кабельної системи та її безпечну й довготривалу експлуатацію.

ВИСНОВКИ

У межах виконання кваліфікаційної роботи було успішно розроблено та технічно обґрунтовано архітектуру локальної обчислювальної мережі для Івано-Франківського відділення Львівської філії АБ «Експрес-Банк». Спроектована телекомунікаційна інфраструктура охоплює як внутрішній інформаційний контур центрального офісу відділення, так і розподілену мережеву топологію, що інтегрує територіально віддалені структурні підрозділи в єдиний захищений корпоративний простір.

У роботі сформовано комплекс вичерпних інженерних інструкцій та конфігураційних лістингів для розгортання і безперебійного функціонування ключових вузлів ЛОМ, а саме:

- програмного шлюзу безпеки для контролю доступу до глобальної мережі Інтернет;

- виділеного файлового сервера для централізованого збереження даних;

- головного високопродуктивного комутатора ядра мережі;

- периферійних керованих комутаторів рівня доступу для робочих груп.

Окрему увагу приділено безпеці взаємодії філій, зокрема детально описано алгоритми криптографічного захисту та параметри налаштування VPN-тунелів для санкціонованого обміну даними з віддаленими філіями. З метою оптимізації капітальних витрат та підвищення відмовостійкості систем, у проєкті впроваджено альтернативні програмні рішення з відкритим вихідним кодом.

В економічній частині роботи проведено детальний розрахунок кошторисної вартості проєктних робіт, куди увійшли витрати на проектування, закупівлю апаратного забезпечення, монтаж кабельних систем СКС та фінальне конфігурування мережевих служб для Івано-Франківського відділення АБ «Експрес-Банк».

У розділі, присвяченому охороні праці та екології, систематизовано вимоги виробничої санітарії, електробезпеки та техніки безпеки під час експлуатації засобів обчислювальної техніки персоналом банківської установи. Крім того, відповідно до вимог нормативних документів розроблено план евакуації працівників у разі виникнення пожежі та виконано схему розміщення первинних засобів пожежогасіння в приміщеннях відділення банку, що сприяє підвищенню рівня пожежної безпеки, забезпеченню своєчасної евакуації людей і мінімізації можливих наслідків надзвичайних ситуацій.

ПЕРЕЛІК ПОСИЛАНЬ

1. Бірюков М.Л., Стеклов В.К., Костік Б.Я. Транспортні мережі телекомунікацій: системи мультиплексування: навч. посіб. Київ: Техніка, 2019. 312 с.

2. Жидецький В.Ц. Охорона праці користувачів комп’ютерів: навч. посіб. 2-ге вид., доп. Львів: Афіша, 2020. 176с.

3. Жуков І.А., Дрововозов В.І., Махновський Б.Г. Експлуатація комп’ютерних систем та мереж. Київ: НАУ. 2017. 361с.

4. Катренко Л.А., Катренко А.В., Охорона праці в галузі комп'ютингу: Підручник. За науковою редакцією В.В. Пасічника. - Львів: «Магнолія 2006» - 2026, - 544 с.

5. Методичні вказівки до виконання кваліфікаційної роботи за спеціальністю 123 Комп’ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ» 2021. 54с.

6. Оришака, О. В. Основи охорони праці : навч. посіб. / О. В. Оришака, Г. П. Горбачова, К. М. Марченко ; М-во освіти і науки України, Центрально-україн. нац. техн. ун-т. - Кропивницький : ЦНТУ, 2022. - 175 с.

7. Погорілий С.Д.. Комп'ютерні мережі. Апаратні засоби та протоколи передачі даних: навч. підр. Київ: ВПЦ "Київський університет. 2018. 138с.

8. Ткаченко В. Комп’ютерні мережі та телекомунікації: навч. посіб. Харків: НТУ “ХПІ”. 2021. 224 с.

9. Царьов Р. Ю. Структуровані кабельні системи : навч. посіб. Одеса: ОНАЗ ім. О.С. Поповаю 2023. 260 с.

10. Черкун О.М. Сучасні технології комп’ютерної безпеки. Монографія. Книга 7. Рівне: МЕГУ. 2022. 90с.

11. Швиденко М.З., Матус Ю.В.. Комп’ютерні мережні технології: Навч.-метод. посібн. Київ: ТОВ “Авета”. 2016. 264с.

12. APC 1500 VA/ URL: https://www.apc.com/shop/ua/products/APC-Smart-UPS-1500-USB-230-/P-SUA1500I?isCurrentSite=false (дата звернення: 2.06.2026)

13. Cisco Packet Tracer. URL: https://wikipedia.org/wiki/Cisco_Packet_Tracer. (дата звернення: 04.06.2026).

14. D-Link DGS-1110. URL:: http://www.dlink.com/ua/products/1/816.html. (дата звернення: 1.06.2026).

15. FreeBSD: установка і настройка OpenVPN клієнта. URL: https://rtfm.co.ua/freebsd-ustanovka-i-nastrojka-openvpn-klienta/ (дата звернення: 3.06.2026).

16. T3700G-52TQ. URL:: https://www.tp-link.com/uф/products/details/cat-39_T3700G-52TQ.html. (дата звернення: 1.06.2026)

17. Windows 11 Prof URL: https://techcommunity.microsoft.com/t5/windows-it-pro-blog/what-s-new-for-it-pros-in-windows-11-version-20h2/ba-p/1800132. (дата звернення: 3.06.2026).

18. Настройка ipfw. URL: http://system-administrators.info/?p=1287 (дата звернення: 4.06.2026).

19. Настройка vsftpd. URL: http://ashep.org/2011/nastrojka-vsftpd/#.YLklt6j7TGg. (дата звернення: 3.06.2026).

20. Огляд технологій, застосованих для побудови локальних мереж. URL: http://easy-code.com.ua/2024/05/oglyad-texnologij-zastosovuvanix-dlya-pobudovi-lokalnix-merezh-lokalni-merezhi-statti/. (дата звернення: 20.05.2026).

21. Патч панель Panduit URL: https://svit-server.com.ua/patch-paneli/ (дата звернення: 1.06.2026)

22. Сервер ArtLine Business R33 URL: https://artline.ua/uk/product/server-artline-business-r33v08 (дата звернення: 2.06.2026)

ДОДАТКИ

Додаток А. Таблиця IP-адрес

Таблиці А1 - Таблиця IP адрес

№ п/п	Назва вузла	Назва відділу / Призначення	Номер VLAN	IP Адреса / Маска	Шлюз
1	2	3	4	5	6
1	WS_1	Відділ роботи з юридичними особами	11	172.16.11.2/24	172.16.11.1
2	WS_2	Відділ роботи з юридичними особами	11	172.16.11.3/24	172.16.11.1
3	WS_3	Відділ роботи з юридичними особами	11	172.16.11.4/24	172.16.11.1
4	SW_1	Комутатор доступу юридичного відділу	100	172.16.100.2/24	172.16.100.1
5	WS_4	Відділ роботи з валютою	13	172.16.13.2/24	172.16.13.1
6	WS_5	Відділ работы з валютою	13	172.16.13.3/24	172.16.13.1
7	WS_6	Робоче місце адміністратора серверної	14	172.16.14.2/24	172.16.14.1
8	S_1	Файловий сервер банку (Artline R33)	14	172.16.14.10/24	172.16.14.1
9	S_2	Внутрішній інтерфейс Сервера-шлюзу (FreeBSD)	14	172.16.14.254/24	—
		Зовнішній інтерфейс шлюзу в Інтернет (WAN)	—	93.44.65.2/30	93.44.65.1
10	SW_2	Центральний комутатор ядра філії (L3)	100	172.16.100.1/24	172.16.14.254
11	WS_7	Робоче місце секретаря	15	172.16.15.2/24	172.16.15.1
12	WS_8	Робоче місце директора філії	16	172.16.16.2/24	172.16.16.1
13	WS_9	Відділ роботи з цінними паперами	17	172.16.17.2/24	172.16.17.1
14	WS_10	Відділ роботи з цінними паперами	17	172.16.17.3/24	172.16.17.1
15	WS_11	Відділ роботи з цінними паперами	17	172.16.17.4/24	172.16.17.1
16	WS_12	Відділ роботи з цінними паперами	17	172.16.17.5/24	172.16.17.1
17	WS_13	Відділ роботи з цінними паперами	17	172.16.17.6/24	172.16.17.1
18	WS_14	Відділ майнового та освітнього страхування	18	172.16.18.2/24	172.16.18.1
19	WS_15	Відділ майнового та освітнього страхування	18	172.16.18.3/24	172.16.18.1
20	WS_16	Відділ майнового та освітнього страхування	18	172.16.18.4/24	172.16.18.1

21	WS_17	Відділ майнового та освітнього страхування	18	172.16.18.5/24	172.16.18.1
22	SW_3	Комутатор доступу відділу страхування	100	172.16.100.3/24	172.16.100.1
23	WS_18	Кредитний відділ	19	172.16.19.2/24	172.16.19.1
24	WS_19	Кредитний відділ	19	172.16.19.3/24	172.16.19.1
25	WS_20	Кредитний відділ	19	172.16.19.4/24	172.16.19.1
26	WS_21	Кредитний відділ	19	172.16.19.5/24	172.16.19.1
27	SW_4	Комутатор доступу кредитного відділу	100	172.16.100.4/24	172.16.100.1
28	WS_22	Депозитний відділ	20	172.16.20.2/24	172.16.20.1
29	WS_23	Депозитний відділ	20	172.16.20.3/24	172.16.20.1
30	WS_24	Розрахункова група	21	172.16.21.2/24	172.16.21.1
31	WS_25	Розрахункова група	21	172.16.21.3/24	172.16.21.1
32	WS_26	Розрахункова група	21	172.16.21.4/24	172.16.21.1
33	WS_27	Розрахункова група	21	172.16.21.5/24	172.16.21.1
34	WS_28	Розрахункова група	21	172.16.21.6/24	172.16.21.1
35	SW_5	Комутатор доступу розрахункової групи	100	172.16.100.5/24	172.16.100.1
36	WS_29	Операційні каси банку	22	172.16.22.2/24	172.16.22.1
37	WS_30	Операційні каси банку	22	172.16.22.3/24	172.16.22.1
38	WS_31	Операційні каси банку	22	172.16.22.4/24	172.16.22.1
39	WS_32	Операційні каси банку	22	172.16.22.5/24	172.16.22.1
40	WS_33	Операційні каси банку	22	172.16.22.6/24	172.16.22.1
41	SW_6	Комутатор доступу касового вузла	100	172.16.100.6/24	172.16.100.1
42	WS_34	Центр комплексного обслуговування клієнтів	23	172.16.23.2/24	172.16.23.1
43	WS_35	Центр комплексного обслуговування клієнтів	23	172.16.23.3/24	172.16.23.1
44	WS_36	Центр комплексного обслуговування клієнтів	23	172.16.23.4/24	172.16.23.1
45	WS_37	Центр комплексного обслуговування клієнтів	23	172.16.23.5/24	172.16.23.1
46	WS_38	Центр комплексного обслуговування клієнтів	23	172.16.23.6/24	172.16.23.1
47	SW_7	Комутатор доступу центру обслуговування	100	172.16.100.7/24	172.16.100.1
48	WS_39	Периферійний термінал	24	172.16.24.2/24	172.16.24.1
49	RJ_1	Зовнішній банкомат (Мережева розетка)	24	172.16.24.3/24	172.16.24.1
50	RJ_2	Інформаційний термінал самообслуговування	24	172.16.24.4/24	172.16.24.1

Додаток Б. Таблиці VLAN

Таблиця Б1 – Логічний поділ на VLAN

Діапазон позначення вузлів	Робоча група / К-сть вузлів	Приміщення	Назва кабінету та його номер	Номер VLAN	Адреса підмережі / Маска
WS_1 – WS_3	3	—	Відділ роботи з юридичними особами	11	172.16.11.0/24
WS_4 – WS_5	2	—	Відділ роботи з валютою	13	172.16.13.0/24
WS_6, S_1, S_2	3	—	Серверна зона філії	14	172.16.14.0/24
WS_7	1	—	Приймальня / Секретар	15	172.16.15.0/24
WS_8	1	—	Кабінет директора філії	16	172.16.16.0/24
WS_9 – WS_13	5	—	Відділ роботи з цінними паперами	17	172.16.17.0/24
WS_14 – WS_17	4	—	Відділ майнового та освітнього страхування	18	172.16.18.0/24
WS_18 – WS_21	4	—	Кредитний відділ	19	172.16.19.0/24
WS_22 – WS_23	2	—	Депозитний відділ	20	172.16.20.0/24
WS_24 – WS_28	5	—	Розрахункова група	21	172.16.21.0/24
WS_29 – WS_33	5	—	Операційні каси банку	22	172.16.22.0/24
WS_34 – WS_38	5	—	Центр комплексного обслуговування клієнтів	23	172.16.23.0/24
WS_39, RJ_1, RJ_2	3	—	Зона самообслуговування (Периферія та банкомати)	24	172.16.24.0/24
SW_1 – SW_7, SW_2	8	—	Мережа моніторингу та управління (Management)	100	172.16.100.0/24

Таблиця Б2 - Таблиця конфігурування VLAN

№ п/п	Позначення вузла	Порт джерела	Тип джерела	Приймач	Порт прийм.	Тип прийм.	VLAN
1	2	3	4	5	6	7	8
1	WS_1	Eth0	—	SW_1	1	Access	11
2	WS_2 – WS_3	Eth0	—	SW_1	2-3	Access	11
3	WS_4 – WS_5	Eth0	—	SW_1	4-5	Access	13
4	WS_6, S_1, S_2	Eth0	—	SW_2	1-2	Access	14
5	WS_7	Eth0	—	SW_2	3	Access	15
6	WS_8	Eth0	—	SW_2	4	Access	16
7	WS_9 – WS_13	Eth0	—	SW_2	5-9	Access	17
8	WS_14 – WS_17	Eth0	—	SW_3	1-4	Access	18
9	WS_18 – WS_21	Eth0	—	SW_4	1-4	Access	19
10	WS_22 – WS_23	Eth0	—	SW_4	5-6	Access	20
11	WS_24 – WS_28	Eth0	—	SW_5	1-5	Access	21
12	WS_29 – WS_33	Eth0	—	SW_6	1-5	Access	22
13	WS_34 – WS_38	Eth0	—	SW_7	1-5	Access	23
14	WS_39, RJ_1, RJ_2	Eth0	—	SW_7	6-8	Access	24
Магістральні канали зв'язку (Trunk Uplinks)							
15	SW_1	6	Trunk	SW_2	11	Trunk	11,13,100
16	SW_3	5	Trunk	SW_2	12	Trunk	18,100
17	SW_4	7	Trunk	SW_2	13	Trunk	19,20,100
18	SW_5	6	Trunk	SW_2	14	Trunk	21,100
19	SW_6	6	Trunk	SW_2	15	Trunk	22,100
20	SW_7	9	Trunk	SW_2	16	Trunk	23,24,100

Додаток В. Характеристики обладнання

Таблиця В1 - Порівняльна характеристика апаратних платформ серверів

	ARTLINE Business R33	ProServer DL360p
Процесор	Intel Xeon E-2224G	Intel Xeon E-2136
Об’єм ОЗП	16ГБ	16ГБ
Тип ОЗП	DDR4-2666 МГц (4 слоти, макс. обсяг пам'яті 64 ГБ)	2666/2400/2133 МГц ECC DDR4 SDRAM
Дискова підсистема	HDD: 2 x 1 ТБ SSD: 2 x 250 ГБ	HDD: 2 x 1 ТБ SSD: 2 x 250 ГБ
Мережева плата	інтегрована	інтегрована
Блок живлення	650 Вт	650Вт

Таблиця В2 - Порівняльний аналіз 16-ти портових комутаторів робочих груп

Технічні характеристики/ модель комутатора	D-Link DGS-1100-16	TP-LINK TL-SG2216
Швидкість комутаційної шини, Гбіт/с	32	32
Швидкість пересилки пакетів 64 байт, млн./с	23,81	23,8
К-сть портів 10/100/1000	16 + 2SFP	16 + 2 SFP
Підтримка базових протоколів канального рівня (VLAN, Port Mirroring, Spanning Tree, IGMP, QoS)	Так	Так

Таблиця В3 - Порівняльний аналіз центральних комутаторів

Модель /Параметри	TP-Link T3700G-24TQ	Cisco 3750G-48	Dell N1548
Швидкість комутації, Гбіт/с	104	32	176
Пропускна здатність, млн. пакетів/с	77,3	38,7	164
К-сть портів	48	48	48
Додаткові слоти SFP	4	4	4
Підтримка протоколів 2 рівня моделі OSI	VLAN, Spaning Tree, QoS		
Статична маршрутизація	+	+	+
Динамічна маршрутизація	На базі протоколів: RIP, OSPF, IGRP, BGP		
Списки фільтрації	+	+	+
Моніторинг	SNMP, RMON, PortMirroring		
Підтримка Jumbo pack	+	+	+