Міністерство освіти і науки України
Криворізький національний університет
Факультет інформаційних технологій
Кафедра комп’ютерних систем та мереж

Пояснювальна записка
до кваліфікаційної роботи бакалавра
за спеціальністю 123 «Комп’ютерна інженерія»

на тему: Комп’ютерна мережа для фінансових установ

Проектував _____ Д. О. Коваленко

Керівник роботи _____ В. А. Чубаров

Нормоконтроль _____ Д. І. Кузнєцов

Завідувач кафедри _____ А. І. Купін

Кривий Ріг
2024

РЕФЕРАТ

Пояснювальна записка: 60 сторінок, 27 рисунків, 8 таблиць, 21 використаних джерел.

Об’єкт аналізу – локальна комп’ютерна мережа фінансової установи.

Проект складається з чотирьох розділів.

Перший розділ присвячений опису об’єкта проектування.

У другому розділі піднімаються питання безпеки та захисту в локальних мережах.

Третій розділ складається з проектування та опису локальних комп’ютерних мереж, обирається топологія, обладнання. Будується структура кабельної системи.

У четвертому розділі моделюється мережа, впроваджуються параметри налаштувань, та тестується працездатність.

КОМП’ЮТЕРНА МЕРЕЖА, МАРШРУТИЗАТОР, КОМУТАТОР КОМУТАЦІЯ, ТЕЛЕКОМУНІКАЦІЯ, PACKET TRACER.

Explanatory note: 60 pages, 27 figures, 8 tables, 21 used sources.

The object of analysis is a local computer network of a financial institution.

The project consists of four sections.

The first section is devoted to the description of the design object.

The second chapter raises issues of security and protection in local networks.

The third section consists of the design and description of local computer networks, the topology and equipment are selected. The structure of the cable system is being built.

In the fourth section, the network is modeled, configuration parameters are implemented, and performance is tested.

COMPUTER NETWORK, ROUTER, SWITCH, TELECOMMUNICATION, PACKET TRACER.

ЗМІСТ

Перелік скорочень

ТКВ – телекомунікаційний вузол;
ЛКМ – локальна комп’ютерна мережа;
TCP/IP – мережева модель передачі даних;
OSI – Open System Interconnection (взаємодія відкритих систем);
NAT – Network Address Translation (механізм перетворювання IP-адреси транзитних пакетів)
VPN – Virtual private network (віртуальна приватна мережа);
IDS – Intrusion detection system (система виявлення вторгнень);
IPS – Intrusion prevention system (система запобігання вторгнень);
DDoS – Distributed denial of service (розподілена відмова в обслуговуванні)
LAN – Local Area Network (локальна обчислювальна мережа);
WAN – Wide Area Network (глобальні обчислювальні мережі);
MDF – Main Distribution Frame (ПТКВ, первинний телекомунікаційний вузол);
SDF – Secondary Distribution Frame (ВТКВ, вторинний телекомунікаційний вузол);
LDF – Local Distribution Frame (ЛТКВ, локальний телекомунікаційний вузол).

					КНУ.КП.123.24.09.ПС		
Змн.	Арк.	№ документа	Підпис	Дата			
Розробив		Коваленко			ПЕРЕЛІК СКОРОЧЕНЬ	Літера	Аркуш	Аркушів
Перевірив		Чубаров						
						КІ-20		
Н.контроль		Кузнєцов						
Затвердив		Купін						

Вступ

Сучасний світі інформаційних технологій, де швидкість обробки та передавання даних має високе значення, надійність та безпека комп'ютерних мереж стають критичними факторами для успішного функціонування фінансових установ. Фінансові організації, такі як банки, страхові компанії, інвестиційні фонди та інші установи, потребують високопродуктивних, стабільних та безпечних мережевих інфраструктур для забезпечення безперебійної роботи своїх інформаційних систем, захисту конфіденційних даних та надання якісних послуг клієнтам.

Актуальність обраної теми зумовлена необхідністю фінансових установ мати надійну та захищену мережеву інфраструктуру для збереження та обробки великих масивів даних. Неправильне налаштування або використання застарілого обладнання призводить до збоїв у роботі мережі, втрати важливої інформації та фінансових збитків. Враховуючи зростаючу кількість кібератак на фінансові установи, забезпечення безпеки мережі стає однією з найважливіших задач.

Метою цієї кваліфікаційної роботи є розробка ефективної та безпечної комп'ютерної мережі для фінансової установи, яка б відповідала сучасним стандартам та вимогам. У роботі буде детально розглянуто фізичну топологію мережі, обрано відповідне мережеве обладнання, розроблено та змодельовано конфігураційні параметри налаштувань, а також проведено тестування працездатності мережі.

Для досягнення поставленої мети в роботі будуть використовуватись такі методи дослідження: аналіз літератури та нормативних документів щодо побудови та забезпечення безпеки комп'ютерних мереж, використання програмного забезпечення для моделювання та тестування мережевих рішень, емпіричні методи для оцінки ефективності та надійності мережевої інфраструктури.

Таким чином, дана кваліфікаційна робота має практичну значимість та сприятиме покращенню мережевих рішень у фінансових установах, що, в свою чергу, підвищить ефективність їхньої роботи та рівень обслуговування клієнтів.

Очікується, що результати цієї роботи дозволять створити ефективну та надійну комп'ютерну мережу для фінансової установи, яка забезпечуватиме високу швидкість передачі даних, надійність, масштабованість та безпеку. Отримані знання та досвід можуть використовуватись для подальшого розвитку та вдосконалення мережевої інфраструктури фінансових установ.

1. Огляд об'єкта проектування

1.1 Вимоги до проектованої ЛКМ

В якості об'єкта проектування було обрано страхову компанію. Страхова компанія є фінансовою установою, що надає послуги страхування різних ризиків фізичним та юридичним особам. Основними напрямками діяльності компанії є страхування життя, здоров'я, майна, відповідальності, а також інші види страхування, які відповідають потребам ринку. Для забезпечення безперебійної роботи та високої продуктивності інформаційних систем, компанія потребує надійної та масштабованої комп'ютерної мережі, яка забезпечить ефективну взаємодію між усіма підрозділами та забезпечить швидкий доступ до інформації.

Однією з ключових вимог до мережі є висока надійність та безпека, оскільки страхова компанія обробляє велику кількість конфіденційних даних клієнтів. Для захисту інформації необхідно використовувати сучасні методи шифрування, аутентифікації та захисту від кібератак.

Для забезпечення безпечного документообміну, підвищення захищеності та зручності передачі інформації між робочими станціями створюється локальна мережа LAN. Вона є комп’ютерною мережею, яка охоплює невелику територію, наприклад будівлю.

LAN складається з набору комп’ютерного обладнання, яке може взаємодіяти з іншими пристроями цієї ж мережі для обміну інформацією. Підключення здійснюється за допомогою звитої пари, коаксіального, оптоволоконного кабелю або інших типів кабелів, які використовуються при будівництві LAN-мережі. Основні пристрої комп’ютерної мережі, крім магістралей зв’язку, включають персональні комп’ютери, принтери, факси, IP-телефони.

Проста мережа може складатися з кількох комп’ютерів, з'єднаних між собою одним кабелем. У таких випадках використовувалися порти, причому один з комп’ютерів називався майстром, а інший - підлеглим. Комп'ютер-майстер міг створювати копії файлів чи цілих каталогів зі свого комп’ютера на інший, а також виконувати різні операції з інформацією на іншому комп’ютері – видаляти, додавати, редагувати. Таким чином, інформація, використовувана під час такого з'єднання, була спільною для цих комп’ютерів. Цей принцип поділу функцій у мережі став основоположним для побудови мереж будь-якої складності.

Підключення комп’ютера чи сервера до мережі здійснюється за допомогою зовнішньої чи внутрішньої плати – мережевого адаптера. Адаптери перетворюють коди, що використовуються всередині комп’ютера, на потужні сигнали, які потім передаються по мережі. Крім того, адаптери

мають бути сумісні з кабельною системою, шиною передачі інформації всередині комп’ютера та операційною системою, яка використовується на ПК

Дана мережа повинна задовільняти наступні потреби страхової компанії:

- Мережа повинна забезпечувати швидкий доступ до інформаційних систем для оформлення страхових полісів, обробки заявок на відшкодування та вирішення інших питань клієнтів.
- Компанія потребує централізованої системи управління даними, яка дозволить ефективно зберігати, обробляти та аналізувати великі обсяги інформації.
- Для мінімізації простоїв та підвищення відмовостійкості мережа повинна включати резервні канали зв’язку та механізми автоматичного переключення на резервні ресурси у випадку відмови основних.
- Мережа повинна бути достатньо гнучкою, щоб легко адаптуватися до змін у бізнес-процесах і вимогах компанії.

Таким чином, комп'ютерна мережа страхової компанії повинна відповідати сучасним вимогам до надійності, безпеки, продуктивності та масштабованості, забезпечуючи безперебійну роботу всіх підрозділів та високий рівень обслуговування клієнтів.

1.2 Вибір технології для побудови ЛКМ

З моменту створення перших локальних мереж було розроблено безліч різних мережевих технологій, але, тим не менш, лише деякі з них набули широкого поширення, що в основному пов'язано з високим рівнем стандартизації мережевих принципів і підтримкою відомих компаній. Але при всьому цьому стандартна мережа не завжди володіє кращими характеристиками і може забезпечити оптимальний режим обміну. Але найбільшою перевагою і основною перевагою технології є обсяг масового виробництва і низька вартість обладнання. Важливим фактором є те, що розробники програмного забезпечення в основному звертають увагу на найпопулярніші мережі.

Технологія Ethernet

Технологія Ethernet, створена компанією Xerox у 1972 році, є найпопулярнішою серед мережевих технологій. Проєкт став настільки успішним, що в 1980-х роках його підтримали провідні IT-компанії світу, такі як DEC та Intel. Згодом Ethernet стала міжнародним стандартом мережевої технології, отримавши назву IEEE 802.3.

Основні особливості стандарту IEEE 802.3 включають використання топологій «шина» або «зірка»; коаксіальний кабель або виту пару як середовище передачі; бітову швидкість передачі даних до 10 Мбіт/с; максимальну протяжність мережі близько 5 км; кількість кінцевих вузлів до 1024; довжину одного сегмента мережі до 500 м; кількість кінцевих вузлів у сегменті до 100; і метод доступу Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

Ця технологія не обмежується стандартною топологією «шина» і може використовувати топології типу «зірка» або «дерево», які передбачають

використання концентраторів для об'єднання сегментів мережі(Рисунок 1.1). [1]

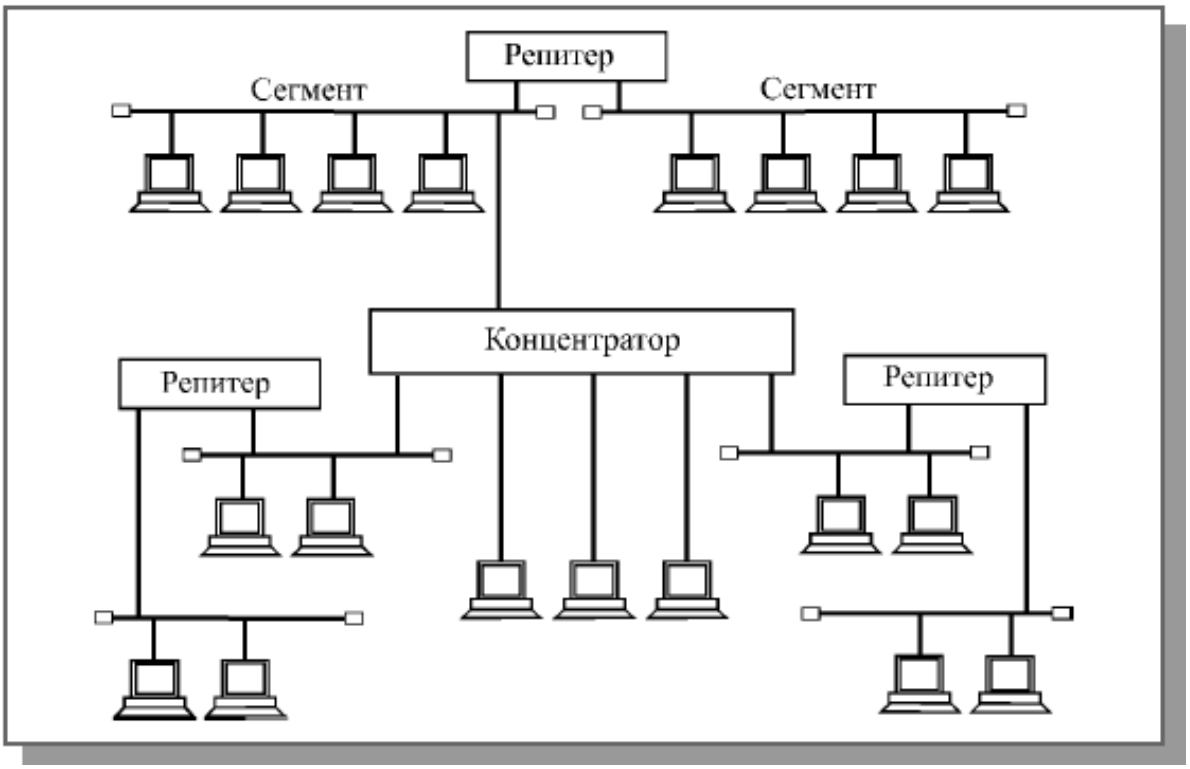

Рисунок 1.1 – Фізична топологія мережі Ethernet [1]

Такі сегменти мережі використовують коаксіальний кабель, а для їх з'єднання застосовують виту пару або оптоволоконний кабель. Крім того, у мережі неприпустима поява петель, оскільки це може перешкоджати її роботі. Теоретично довжина кабелю може сягати 6,5 км, але зазвичай не перевищує 2,5 км.

10Base-5	• коаксіальний кабель, відомий як «товстий» коаксіал
10Base-2	• коаксіальний кабель, відомий як «тонкий» коаксіал
10Base-T	• кабель на основі неекранованої витої пари
10Base-F	• оптоволоконний кабель, з кількома варіантами специфікації: FOIRL, 10Base-FL, 10Base-FB

Рисунок 1.2 – Фізичні специфікації Ethernet

Бітова швидкість передачі даних цих фізичних стандартів досягає 10 Мбіт/с, а слово Base вказує на метод передачі на одній базовій частоті – 10 МГц. Кодування здійснюється за допомогою лінійного манчестерського коду.

На сьогоднішній день технологія Ethernet використовує такі модифікації, як Fast Ethernet і Gigabit Ethernet.

Технологія Fast Ethernet

У 1992 році було створено об'єднання Fast Ethernet Alliance, яке розпочало розробку нової мережевої технології, що передбачала підвищення бітової швидкості передачі даних, зберігаючи при цьому особливості технології Ethernet. З 1992 по 1993 рік було розглянуто різні варіанти переходу на швидкість 100 Мбіт/с. У 1995 році комітет IEEE 802.3 ухвалив технологію Fast Ethernet як стандарт 802.3u, який доповнив стандарт 802.3.

Було встановлено такі фізичні специфікації для середовища передачі даних (рис. 1.2.):

Рисунок 1.3 – Фізичні специфікації Fast Ethernet

Специфікація 100Base-FX працює з використанням оптоволоконного кабелю, де кодування здійснюється за допомогою лінійного коду 4B/5B.

Специфікація 100Base-TX використовує кабель витої пари UTP 5-ої категорії або STP 1-го типу і застосовує кодування MLT-3. Ця специфікація також підтримує функцію автоналагодження, яка дозволяє пристроям, що підтримують кілька стандартів фізичного рівня з різною бітовою швидкістю та числом витих пар, узгоджувати свою роботу.

Специфікація 100Base-T4 працює на основі кабелю UTP 3-ої категорії та використовує лінійне кодування 8B/6T.

Технологія Gigabit Ethernet

У 1996 році була створена група 802.3z для розробки мережевого протоколу на базі технології Ethernet з бітовою швидкістю 1000 Мбіт/с, названого Gigabit Ethernet. Сам стандарт 802.3z був прийнятий у 1998 році. Група 802.3ab займалася роботою над використанням витої пари 5-ої категорії. Незважаючи на те, що цей тип кабелю був створений для передачі даних зі швидкістю 100 Мбіт/с, група 802.3ab успішно впоралася із завданням, і версія Gigabit Ethernet була розроблена для витої пари 5-ої категорії.

Для багатомодового оптоволоконного кабелю стандарт 802.3z має фізичні специфікації 1000Base-SX (коротка хвиля), яка використовує довжину хвилі 850 нм, та 1000Base-LX (довга хвиля), яка використовує довжину хвилі 1300 нм. Специфікація 1000Base-SX може працювати лише на багатомодовому оптоволоконному кабелі з максимальною довжиною до 500 м.

Фізичні специфікації Gigabit Ethernet використовують кабель витої пари 5-ої категорії. Кожна пара кабелю має смугу пропускання до 100 МГц. Для передачі даних зі швидкістю до 1000 Мбіт/с по цьому кабелю необхідно організувати одночасну передачу по всіх чотирьох парах кабелю, що дозволяє знизити бітову швидкість передачі даних по кожній парі до 250 Мбіт/с.

Технологія FDDI

Технологія FDDI (Fiber Distributed Data Interface) була однією з перших мережевих технологій, де використовувалися оптоволоконні кабелі для передачі даних. У 1980-х роках оптоволоконні кабелі почали використовуватися в промисловості, і водночас почалося створення стандарту для їх застосування в локальних мережах. Тоді ж було створено обладнання для підтримки цього стандарту, включаючи мережеві адаптери, концентратори, маршрутизатори та інші пристрої та компоненти.

На сьогоднішній день багато технологій підтримують використання оптоволоконних кабелів на фізичному рівні, але FDDI вважається однією з найбільш перевірених і актуальних мережевих технологій. Вона має високий рівень сумісності з обладнанням від різних виробників, що робить її привабливою для різноманітних застосувань.

Технологія FDDI заснована на ідеях Token Ring, але розвинула їх, спрямовуючись на наступні цілі:

- Підвищення бітової швидкості передачі до 100 Мбіт/с.
- Підвищення рівня відмовостійкості завдяки стандартним процедурам відновлення мережі.
- Ефективне використання пропускної здатності мережі для синхронних та асинхронних потоків трафіку.

Мережа FDDI базується на використанні двох оптоволоконних кілець, які створюють два шляхи передачі даних (основний і резервний) між вузлами мережі. Цей підхід є основним засобом підвищення відмовостійкості мережі. Кожен новий вузол, доданий до мережі, підключається до обох кілець одночасно. В нормальному режимі дані передаються через перше кільце, тоді як друге залишається неактивним.

Таблиця 1.1 Порівняння мережевих технологій.

Параметр	Ethernet	Fast Ethernet	Gigabit Ethernet	FDDI
Максимальна бітова швидкість передачі даних	10 Мбіт/с	100 Мбіт/с	1000 Мбіт/с (1 Гбіт/с)	100 Мбіт/с
Топологія мережі	Зірка, Шина	Зірка, Шина	Зірка, Шина	Кільце
Середовище передачі	Коаксіальний кабель, вита пара	Коаксіальний кабель, вита пара	Вита пара, оптоволокно	Оптоволокно

Продовження Таблиці 1.1

Максимальна довжина кабелю	До 500 м (вита пара)	До 100 м (вита пара)	До 100 м (вита пара)	До 2000 м (оптоволокно)
Макс. відстань між вузлами	2500 м	200 м	200 м	2 км
Кількість вузлів на сегменті	До 1024	До 1024	До 1024	До 500
Метод доступу	CSMA/CD	CSMA/CD	CSMA/CD, Gigabit Ethernet має інші методи	Token Ring
Кодування	Манчестерське	Манчестерське	Манчестерське, 4B/5B, 8B/6T	4B/5B
Сумісність з обладнанням	Широкий спектр	Широкий спектр	Широкий спектр	Висока
Використання в сучасних мережах	Значно менше	Значно менше	Широко використовується	Менше, але в деяких спеціалізованих мережах

В даний час більшість робочих станцій підключаються до мережі за допомогою з'єднання зі швидкістю 100 Мбіт/сек, вищі канали зазвичай працюють зі швидкістю 1 Гбіт/сек.

Тому виходячи з об’єкту проектування та проаналізованого матеріалу, краще обрати технологію Fast Ethernet для проектування ЛКМ банківської установи.

1.3 Пропозиції щодо топології комп’ютерної мережі

Топологія комп'ютерної мережі визначає розміщення і конфігурацію фізичного з'єднання між взаємопов'язаними кінцевими пристроями. Вона відображає структуру зв'язку між основними функціональними елементами мережі.

Залежно від компонентів, топологію мережі можна розділити на логічну і фізичну структури. Логічна структура визначається логічною взаємодією між кінцевими пристроями, тоді як фізична структура визначає фізичний зв'язок через безпосереднє з'єднання пристроїв один з одним.

Варто зазначити, що фізична топологія явно залежить від використовуваної технології та стандартів.

Всього існує 3 основні топології. Нижче описані 3 основні використовувані топології.

"Шина даних" - це тип топології мережі, реалізований за допомогою

одного спільного кабелю, до якого підключений кінцевий пристрій. Кабелі в цій топології називаються шинами або магістралями. В кінці такого кабелю використовується поглинач сигналу, званий Термінатором, для запобігання відбиття сигналу.

Цей тип топології мережі використовує один кабель, до якого підключені всі комп'ютери в мережі. Повідомлення, надіслані з будь-якої робочої станції, поширюються на всі комп'ютери в мережі. Кожен пристрій перевіряє, хто є одержувачем повідомлення, і обробляє, хто є одержувачем повідомлення. Ця топологія вважається застарілою і сьогодні не дуже практичною. Приклад такої топології показан на рисунку 1.4.

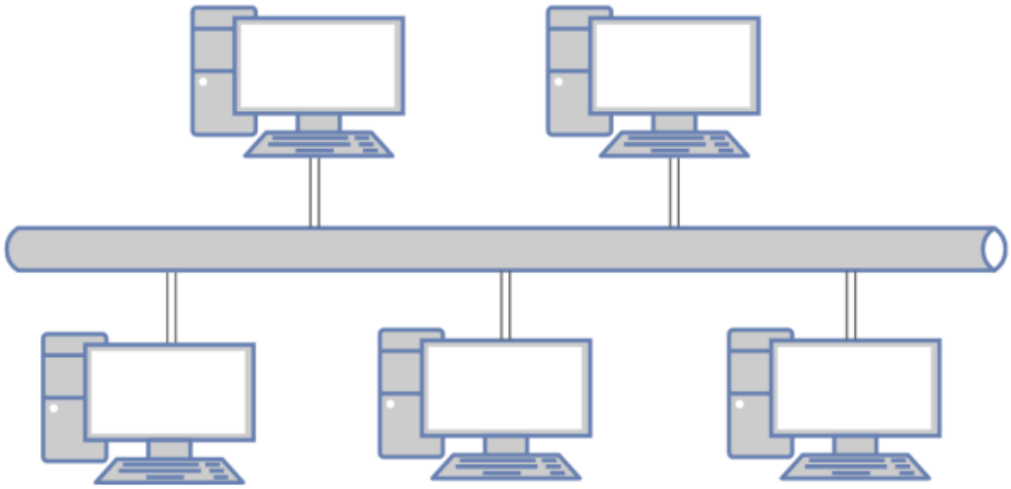

Рисунок 1.4 – Шинна топологія[3]

"Кільце" - це топологія мережі, в якій кінцевий пристрій підключений до замкнутого кабелю по колу. Цей варіант топології вирішує проблему топології шини і не вимагає встановлення спеціального кінцевого пристрою сигналу на кінці кабелю. Сигнал передається по кільцю в одному напрямку, послідовно проходячи через кожен пристрій в мережі, причому останній одночасно діє як підсилювач сигналу.

Один із методів передачі потоків даних по кільцевій мережі відомий як проходження маркера. Цей метод передачі називається Token Ring і передбачає використання спеціального концентратора. Фізично мережа має зірково-кільцеву топологію, але насправді пристрої пов'язані в кільце. Концепція цього методу передачі даних полягає в тому, що виділений центр переміщує невеликі блоки даних, які називаються маркерами, по мережі. Token передаються по черзі по колу. Така архітектура широко не використовується через низку проблем, пов'язаних з обмеженням швидкості (до 16 Мбіт / сек) і складністю фізичної реалізації. Кільцева топологія показана на рисунку 1.5.

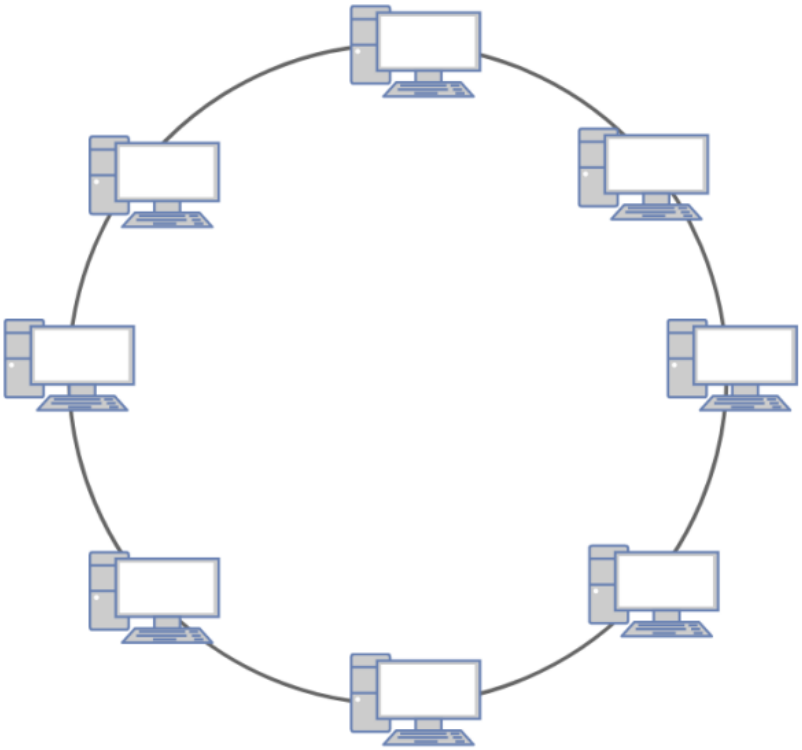

Рисунок 1.5 – Топологія кільце[3]

"Зірка" - це топологія мережі, що характеризується виділеним центром, до якого підключені інші пристрої. Обмін інформацією здійснюється через центральний пристрій у мережі.

Використання такої топології має важливу перевагу у стійкості до збоїв або аварій, пов'язаних з кінцевими пристроями. Якщо один з пристроїв вийде з ладу, інші можуть продовжувати працювати без зниження продуктивності. Однак ця перевага виносить на поверхню недолік: якщо вийде з ладу центральний пристрій, через який здійснюється передача даних, це може призвести до зупинки обміну інформацією. Для мінімізації таких ситуацій вживаються превентивні заходи. З такою топологією можна легко контролювати роботу мережі і локалізувати збої, відключаючи певних абонентів від центру. В даний час" зірка", крім іншого, є найпопулярнішим рішенням для компонування локальних комп'ютерних мереж всіх типів і напрямків. Застосування такої топології показано на рисунку 1.6.

Рисунок 1.6 – Топологія зірка[3]

Проаналізувавши матеріал, можна відзначити, що використання топології зірка є найбільш оптимальним, тому саме ця топологія буде використовуватись у подальшій розробці мережі для БА.

1.4 Висновок за розділом

У першому розділі було детально розглянуто основні аспекти побудови та функціонування локальних мереж. Спочатку було проведено огляд мережевих технологій ЛКМ, та обрано необхідну технологію, для її впровадження у проектовану систему. Було розглянуто різні топології комп'ютерних мереж, такі як шинна, зіркоподібна, кільцева, топології, а також висвітлено їхні недоліки та переваги.

2. Характеристика безпеки в ЛКМ

2.1 Передумови створення захисту в комп’ютерній мережі

Основне завдання створення багаторівневої системи захисту локальних мереж – захистити інформаційне середовище від навмисних або випадкових перешкод, спроб знищення її компонентів, отримання несанкціонованого доступу та забезпечення роботи системи в непередбачених ситуаціях.

У сучасному світі інформаційні системи займають одне з важливих місць у функціонуванні організацій і підприємств. Метою інформаційної системи є задоволення потреб користувачів у процесі виконання своїх посадових обов'язків.[10] Комп'ютерні мережі дозволяють співробітникам підприємства швидко і ефективно обмінюватися інформацією, зберігати і створювати файли віддалено, спілкуватися поштою, отримувати доступ до всесвітньої мережі Інтернет і її ресурсів, а також безпосередньо взаємодіяти з виробничим процесом. Тобто функція включає основні аспекти життя кожної компанії.

Ефективність використання мережі без перебільшення має основоположне значення для сучасної реальності. Якщо мережа скомпрометована або сталася dos-атака або вірусний спалах, під загрозою опиниться діяльність всієї організації. Це пов'язано з підвищеним ризиком для операційних ресурсів, даних користувачів, приватних фондів та технологій. Інтелектуальна власність може бути вкрадена і використана третіми особами.

Підтримка локальної мережі компаній з кожним роком стає все більш складним завданням і є одним з ключових факторів, з якими стикаються компанії сьогодні. Нові загрози з'являються регулярно, і організація не застрахована від них. Варто відзначити, що з кожною появою нових видів небезпечних загроз концепція "захищеної мережі" змінюється.[4]

Створення захищеної комп'ютерної мережі, це найкращий спосіб організувати єдине інформаційне середовище для компанії. Таким чином, користувачі отримають доступ до спільних ресурсів і зможуть спільно використовувати принтери та інші мережеві пристрої. Правильно налаштувавши мережу, адміністратори можуть забезпечити належний рівень конфіденційності та запобігти витоку даних, що становлять комерційну таємницю. Важливість і актуальність питань інформаційної безпеки обумовлені факторами, які зображені на рисунку 2.1.[5]

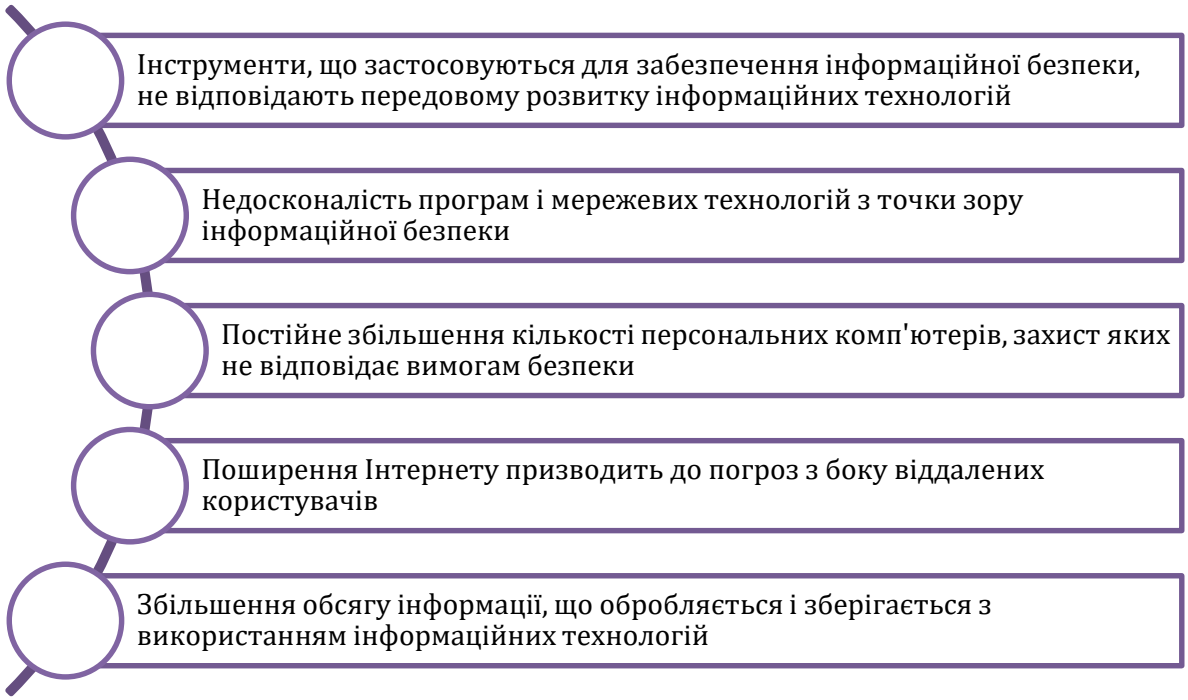

Рисунок 2.1 – Фактори, які впливають на інформаційну безпеку[5]

Впровадження єдиної корпоративної інформаційної системи є найбільш поширеною практикою серед сучасних компаній. Це дозволяє централізувати управління та об'єднувати всі пристрої в єдине середовище для ефективної декомунікації та взаємодії між відділами. З іншого боку, зі зростанням ролі інформаційних систем у корпоративних операціях зростає і загроза незаконного втручання, атак та інших методів несанкціонованого доступу, спотворення або знищення інформації в системі.

Діапазон шкідливих наслідків може варіюватися від збоїв системи і фінансових втрат для комерційних компаній, таких як розголошення державної таємниці. грудень. З цієї причини інформаційної безпеки завжди відводилося особливо важливе місце в дизайні будь-якого бізнесу.[6]

2.2 Принципи захисту інформації у мережі, підключеної до інтернету

Надсилаючи конфіденційну інформацію через Інтернет, важливо використовувати безпечні протоколи, такі як HTTPS. Це забезпечує шифрування даних і запобігає несанкціонованому доступу. Ви можете налаштувати надійні паролі та 2-факторну автентифікацію, щоб запобігти несанкціонованому доступу до мережевих ресурсів. Необхідно використовувати унікальний пароль для кожного облікового запису і регулярно його оновлювати. Налаштування брандмауер, допоможе відстежувати трафік, що надходить і виходить з мережі.[7] Це запобігає несанкціонованому доступу та забезпечує безпеку мережі. Якщо антивірусне програмне забезпечення встановлено і оновлено правильно, ваш комп'ютер може бути захищений від вірусів і троянів. Один з підходів до захисту інформації зображений на рисунку 2.2.[8]

Рисунок 2.2 – Ієрархічний підхід до забезпечення безпеки інформації[9]

До основних принципів захисту, можна віднести:

- Конфіденційність, яка передбачає захист інформації від несанкціонованого доступу. Для забезпечення конфіденційності використовуються різноманітні методи шифрування, які гарантують, що дані можуть бути прочитані лише авторизованими користувачами. Протоколи SSL/TLS, які використовуються для захисту веб-трафіку, є прикладом таких методів. Крім того, для захисту конфіденційності важливо впроваджувати політики доступу, які визначають, хто має право доступу до певних даних та ресурсів.
- Цілісність, що забезпечує захист даних від несанкціонованих змін. Для цього використовуються хеш-функції та цифрові підписи, які дозволяють перевірити, чи не було змінено дані під час передачі. Протоколи, такі як IPSec, забезпечують цілісність та автентичність даних при їх передачі через Інтернет. Важливо також впроваджувати регулярні резервні копії даних, щоб мати можливість відновити їх у випадку втрати або пошкодження.
- Доступність, яка передбачає забезпечення безперебійного доступу до інформації та ресурсів для авторизованих користувачів. Для цього використовуються різноманітні методи захисту від атак, спрямованих на виведення системи з ладу, такі як атаки типу "відмова в обслуговуванні" (DoS). Важливим аспектом забезпечення доступності є використання механізмів відмовостійкості, таких як дублювання критичних систем та використання резервних каналів зв'язку.[10]

Моніторинг і управління інцидентами безпеки є невід'ємною частиною захисту інформації. Постійний моніторинг мережевого трафіку та системних журналів дозволяє виявляти підозрілі активності та оперативно реагувати на інциденти. Використання систем виявлення та запобігання вторгнень (IDS/IPS) допомагає автоматично визначати та блокувати потенційні загрози.

Навчання та підвищення обізнаності користувачів також є важливим елементом захисту інформації. Більшість успішних атак спрямовані на соціальну інженерію та фішинг, які використовують людський фактор як слабку ланку. Регулярні тренінги та інформаційні кампанії допомагають підвищити рівень обізнаності працівників щодо потенційних загроз та методів їх уникнення.

Таким чином, захист інформації при підключенні до мережі Інтернет вимагає комплексного підходу, що включає використання технічних засобів, розробку політик безпеки, навчання користувачів та регулярний моніторинг системи. Виконання цих принципів дозволяє значно знизити ризики та забезпечити безпеку даних у мережі.[11]

2.3 Види мережевих атак

Зловмисне програмне забезпечення зазвичай потрапляє в систему через те, що користувач натискає на шкідливе посилання або відкриває шкідливий електронний лист. Воно може бути доставлене кількома способами. Після встановлення шкідливе програмне забезпечення може блокувати доступ до критичних компонентів мережі, завдавати шкоди системі та збирати конфіденційну інформацію.[12]

Найбільш поширеними прикладами мережевих атак є наступні типи впливів:

– *Використання нестандартних протоколів*. Тип протоколу пакета даних визначається вмістом настроюваних полів в ньому. Якщо зловмисник змінює значення цього поля, він надсилає дані, які система не може ідентифікувати.

– *Пінг-флуд*. Така атака застосовується лише в тому випадку, якщо у вас є доступ до високошвидкісного Інтернету. Для цього потрібно, щоб замість стандартної команди управління пінгом використовувалася команда затоплення. В результаті виникає перевантаження мережі, яка перериває її роботу.

– *Фрагментація даних*. При відправці по IP пакети даних розбиваються на частини і збираються на стороні одержувача. У разі атаки значна частина таких фрагментів відправляється, забиваючи плату і руйнуючи мережу.

У зв'язку з швидким розвитком інформаційних технологій і технічних засобів механізми статичного захисту від мережевих загроз часто виявляються неефективними. Динамічні методи, які можуть швидко виявляти і усувати загрози, забезпечують ефективний захист інформації. Робота динамічної технології заснована на оцінці рівня підозрілості до дій в мережі конкретною службою або процесом.

Алгоритм дій, спрямованих на усунення атак, спрямований на виявлення підозрілих об'єктів. Після цього система реагує на активність таких об'єктів, які при необхідності можуть бути націлені на мережеві ресурси або комп'ютерне обладнання.[13]

На сьогоднішній день відомі наступні види мережевих атак:

Рисунок 2.3 – Види мережевих атак

2.4 Методи виявлення атак та захисту інформації

Міжмережеві екрани, або брандмауери - це апаратні або програмні засоби, які відстежують інформацію, що надходить і виходить з інформаційної системи. Залежно від вашої конфігурації, брандмауер дозволяє або забороняє трафік, шифрує дані та діє як інтерпретатор мережевих адрес (NAT).[14]

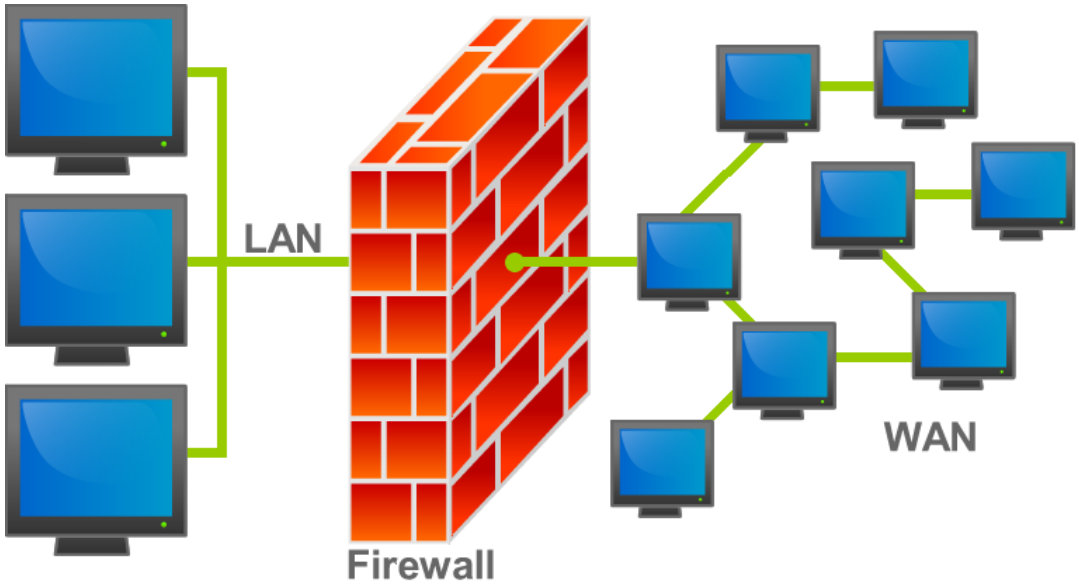

Рисунок 2.4 – Принцип роботи міжмережевого екрану[14]

Існує 2 типи брандмауерів: апаратні та програмні:

- Апаратний брандмауер-це спеціальний пристрій, фізично підключений до комп'ютерної мережі. Щоб налаштувати цей тип брандмауера, ви можете використовувати консольний порт пристрою або з віддаленого комп'ютера з виділеним допоміжним хостом по протоколу Telnet або SSH. Прикладами таких пристроїв є Cisco PIX, Cisco ASA, брандмауер ZL1 та Watchguard Firebox.;
- Програмний брандмауер це програмне забезпечення, яке працює на окремих кінцевих пристроях, таких як ПК, сервери та маршрутизатори. Завдання такого брандмауера аналізувати вміст інформаційних пакетів у зовнішній мережі і виконувати відповідні дії в залежності від поточної конфігурації. Він діє як захисний бар'єр між внутрішньою мережею підприємства та зовнішньою обчислювальною мережею.

Всього існує 3 покоління брандмауерів з різними типами фільтрації трафіку.

Брандмауер першого покоління діє як фільтр пакетів, порівнюючи основну інформацію, таку як джерело, призначення, порт та протокол пакета, з визначеним списком правил.

Брандмауер другого покоління містить додаткові параметри конфігурації фільтра-стан підключення. Використовуючи цю інформацію, технологія може відстежувати дані про поточне з'єднання, його початок і завершення.

Брандмауер наступного покоління створений для фільтрації інформації за допомогою всіх рівнів моделі OSI, включаючи прикладний рівень.[15]

На основі цієї інформації брандмауер може виявляти атаки, спрямовані на спроби обійти несанкціоноване використання авторизованих портів або протоколів.

NAT-Перетворення

У локальній мережі використовуються приватні IP-адреси з визначених для цього діапазонів. Найбільш поширені серед них — 10.0.0.0/8, 172.16.0.0/12 і 192.168.0.0/16. Ці адреси не маршрутизуються через Інтернет і є унікальними в межах локальної мережі.

Компанія має обмежену кількість публічних IP-адрес, які використовуються для зв'язку з Інтернетом. Завдяки NAT можна замаскувати приватні IP-адреси під публічні, що дозволяє пристроям в локальній мережі виходити в Інтернет через одну або кілька публічних IP-адрес.

У локальних мережах NAT змінює IP-адресу вихідних пакетів, використовуючи таблицю перетворення IP-адрес. Ця таблиця містить відповідності між приватними та публічними IP-адресами, тому при відправленні пакету з локальної мережі в Інтернет приватна IP-адреса замінюється на відповідну публічну.

Трансляція NAT включає зміну як IP-адреси, так і порту. Кожен пакет має унікальний номер порту, що відповідає певній програмі або службі. NAT зв'язує публічні та приватні порти, забезпечуючи передачу даних між локальною мережею та Інтернетом.

NAT є корисним для онлайн-захисту, оскільки фільтрує трафік і забезпечує безпеку локальної мережі. Використовуючи публічну IP-адресу для зовнішнього зв’язку, приватні IP-адреси залишаються недоступними для прямого підключення з Інтернету, що додає додатковий рівень захисту від зовнішніх загроз.

Використання NAT у корпоративних мережах має важливе значення, оскільки дозволяє ефективно використовувати обмежену кількість публічних IP-адрес і забезпечує захист та ізоляцію локальної мережі при підключенні до Інтернету. [14]

IDS / IPS

У сучасному світі системи виявлення та запобігання вторгненням IDS / IPS є важливим елементом захисту від мережевих атак. Основне завдання цих систем-виявляти факти несанкціонованого доступу або несанкціонованого управління мережею і застосовувати відповідні заходи (наприклад, повідомляти адміністратора про факт вторгнення, відключати або переналаштувати брандмауер для запобігання інших дій зловмисника).

Система IPS призначена для запобігання атак (рис. 2.5). Така системи відстежує трафік і блокують підозрілі потоки даних. ЇЇ мета виявити і запобігти несанкціоновану активність в мережі. Система використовує набір правил для блокування трафіку. Таким чином, він закриває вразливості, IP-адреси можуть застосовуватися до межі мережі або до окремих хостів. Також вона може дублювати трафік, не маючи при цьому IP-адреси.[16]

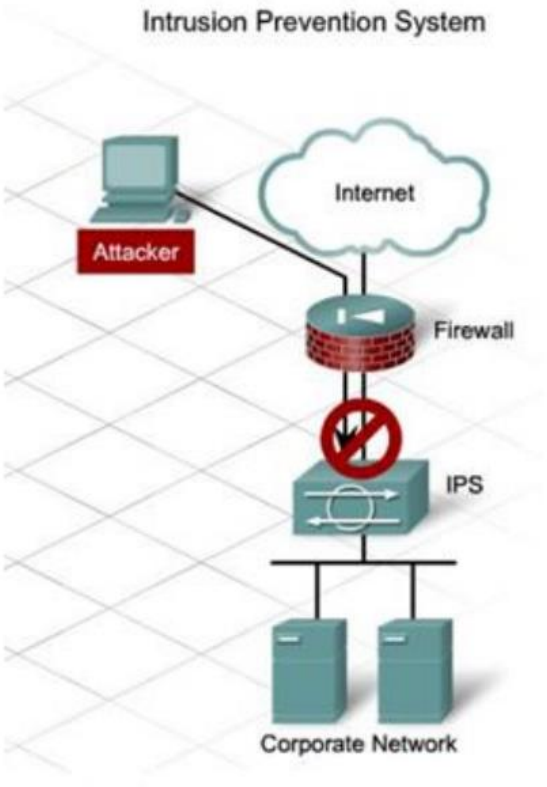

Рисунок 2.5 – Система запобігання вторгненням[17]

IPS можна розділити на 2 класи. Перший аналізує трафік і порівнює його з відомими характеристиками загроз. Другий аналізує протокол і шукає заборонений трафік у базі даних раніше виявлених вразливостей. Саме цей клас забезпечує захист від несанкціонованих атак. Система IDS використовується для виявлення незвичайної поведінки в мережі і попередження про неї фахівців з інформаційної безпеки (рис. 2.6).[16]

Повідомлення з'являється на панелі керування або може бути надіслано на електронну пошту, телефон тощо. Метою системи є моніторинг трафіку, виявлення мережевих атак та виявлення порушень політики безпеки користувачами. Система виявлення вторгнень IDS допомагає контролювати стан безпеки.[17]

Системні функції IDS:

- реєстрація інформації, відправка в систему збору журналів;
- попередження про інциденти
- підсумовування даних подій

Архітектура IDS зазвичай включає:

- сенсорні підсистеми, призначені для збору подій в різних областях захисту системи;
- підсистему аналізу, призначену для виявлення і класифікації атак і підозрілих дій на основі даних датчиків;
- репозиторій, що забезпечує накопичення первинних подій і результатів аналізу;

– консоль управління, яка дозволяє встановлювати ідентифікатор, відстежувати стан системи та переглядати звіти про події, виявлені системою.[16]

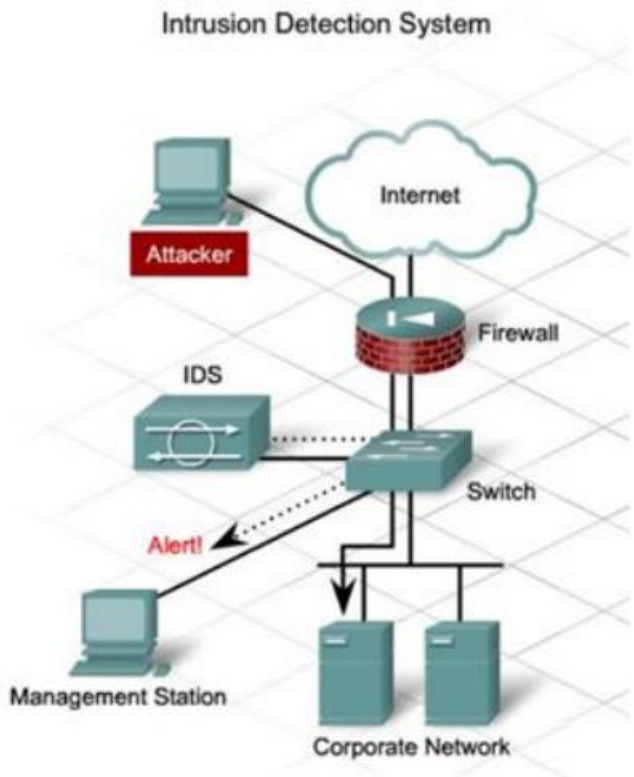

Рисунок 2.6 – Система виявлення вторгнень[27]

2.5 Висновок за розділом

У другому розділі було розглянуто ключові аспекти забезпечення захисту в комп'ютерних мережах. Спочатку були проаналізовані передумови створення захищеної мережі. Були розглянуті принципи захисту інформації при підключенні до Інтернету. Аналіз видів мережевих атак, таких як мережева розвідка, IP-спуфинг, DDOS-атаки, та ін., дозволив зрозуміти різноманітність загроз, з якими може зіткнутися мережа. На завершення, були розглянуті методи виявлення атак та захисту інформації, включаючи використання систем виявлення вторгнень (IDS/IPS), та міжмережевих екранів. Усі ці аспекти формують комплексний підхід до захисту мережі, що дозволяє ефективно протидіяти загрозам та забезпечити безпеку інформаційних ресурсів.

3. Проектування та опис ЛКМ, фінансової установи

3.1 План приміщення, структура компанії

Обрана фінансова установа представляє собою страхову компанію.

Для створення схем ЛКМ страхової будуть використовуватися онлайн-версія програмного забезпечення draw.io.[24] Вона дозволяє графічно відобразити обладнання в приміщенні.

Будівля страхової складається з двох поверхів. Всього в будівля 10 кабінетів. Макети 1 і 2 поверхів відповідно зображені у Додатку А, Рис.А.1, Рис.А.2.

Організаційна структура компанії
1 поверх:
Кабінет 1-1: відділ обслуговування клієнтів;
Кабінет 1-2: кімната відпочинку;
Кабінет 1-3: адміністратор мережі;
Кабінет 1-4: приміщення для надання страхових виплат;
2 поверх:
Кабінет 2-5: юридичний відділ;
Кабінет 2-6: відділ кадрів;
Кабінет 2-7: кабінет директора;
Кабінет 2-8: бухгалтерія;
Кабінет 2-9: архів;
Кабінет 2-10: відділ андеррайтингу.

3.2 Розташування обладнання в приміщенні

Мережа має наступне обладнання:
1 поверх:
Кабінет 1-1 – 6 комп’ютерів, 1 принтер, 1 комутатор, 6 ip-телефонів, 2 камери;
Кабінет 1-2 – 1 бездротова точка доступу, 3 смартфони, 1 телевізор;
Кабінет 1-3 – 1 комп’ютер, 1 комутатор рівня 3, 2 сервери, 1 пригранічний маршрутизатор, 1 міжмережевий екран;
Кабінет 1-4 – 3 комп’ютери, 2 принтери, 1 комутатор, 3 ip-телефони, 1 камера.
2 поверх:
Кабінет 2-5 – 3 комп’ютери, 1 принтер, 1 комутатор, 3 ip-телефони;
Кабінет 2-6 – 2 комп’ютери, 2 принтери, 1 комутатор, 1 ip-телефон, 1 камера;
Кабінет 2-7 – 1 комп’ютер, 1 ноутбук;
Кабінет 2-8 – 2 комп’ютери, 1 комутатор, 1 бездротова точка доступу, 1 камера;
Кабінет 2-9 – 1 комп’ютер, 1 маршрутизатор;

Кабінет 2-10 – 2 принтери, 3 ноутбуки, 1 точка доступу Wi-fi.

Обладнання розміщене безпосередньо на місцях використання, що відображено на Рис.А.3, Рис.А.4 (додаток А). В якості робочих станцій обрані персональні комп’ютери та ноутбуки. Для друку використовуються принтери. Зв'язок налагоджений завдяки ір-телефонам, та смартфонам.

3.3 Визначення телекомунікаційних вузлів

Телекомунікаційні вузли є важливим компонентом інфраструктури комп'ютерних мереж, що забезпечує зв'язок і передачу даних між різними сегментами мережі. Вони забезпечують централізоване управління мережею, розподіл трафіку, а також високу надійність і стійкість мережевого підключення.

TKV можна класифікувати за наступними критеріями:

- Головний телекомунікаційний вузол, або МДФ, є центральним вузлом мережевої інфраструктури друкарського верстата. Він діє як головний вузол, через який проходить весь зв'язок між різними сегментами мережі та зовнішніми мережами, такими як Інтернет. МДФ є життєво важливим елементом для забезпечення надійних і швидких з'єднань.

Основні компоненти МДФ включають в себе всі інші мережеві комутатори, маршрутизатори, що відповідають за маршрутизацію трафіку між внутрішньою мережею та Інтернетом, сервери управління базами даних, сховище файлів, управління принтерами та інші мережеві ресурси, а також інші мережеві і протокольні служби. До них відносяться шлюзи для підключення до протоколу, брандмауери для захисту мережі від несанкціонованого доступу та атак, а також патч-панелі для декомунізації та підключення кабелів. Основні телекомунікаційні вузли зазвичай розташовані в спеціальних приміщеннях з контрольованими Умовами, такими як температура і вологість. Приміщення повинно бути захищене від несанкціонованого доступу і оснащене джерелом безперебійного живлення.

- Вторинний телекомунікаційний вузол або SDF є проміжним вузлом між основним телекомунікаційним вузлом і локальним телекомунікаційним вузлом.

Він забезпечує розподіл трафіку з МДФ в певні зони або великі приміщення. SDF включають комутатор доступу для підключення кінцевих пристроїв і передачі даних на, патч-панель для встановлення з'єднань між різними сегментами мережі. SDF зазвичай розміщується у великому приміщенні, наприклад, на виробничому заводі або у великому офісному приміщенні, і для його підключення потрібно багато периферійних пристроїв. Приміщення SDF також має бути захищене і оснащене системою охолодження і резервного живлення.

- Локальний телекомунікаційний вузол , або LDF, є кінцевим вузлом. Мережева інфраструктура, що забезпечує підключення кінцевих пристроїв в певній області або об'єкті. Він підключається до SDF і забезпечує доступ до мережевих ресурсів для робочих станцій, принтерів, сканерів та іншого обладнання.

Основні компоненти LDF включають комутатори доступу для підключення кінцевих пристроїв до мережі. LDF розташовують у невеликих приміщеннях або робочих зонах, таких як офіс, конструкторський відділ, виробничі приміщення та склад. Кімната LDF зручна для доступу персоналу і повинна забезпечувати можливість швидкого підключення або відключення пристроїв.

ТКВ - це основа мережевої інфраструктури. Розподілена структура, що включає первинні, вторинні і локальні вузли, забезпечує ефективну і надійну роботу мережі. Правильне планування мережі, вибір обладнання, впровадження та постійний моніторинг мають вирішальне значення для успішної роботи.

Такий підхід забезпечує високу пропускну здатність, надійність, безпеку і масштабованість мережі, сприяючи ефективній роботі і задоволенню потреб в обробці і передачі даних. Блок-схема комп'ютерної мережі, що містить наведені вище розділи, складається на основі кількості та місця розташування ТЗ, а також частин топології фізичної мережі, утвореної кінцевим обладнанням, зонами бездротового доступу, серверами обмеженого доступу, серверами загального доступу та інтернет-з'єднаннями. На блок-схемі підкреслюється прив'язка сегмента топології мережі до відповідних ТКВ.

Структурна схема проектованої комп'ютерної мережі, яка реалізує підключення 10 кабінетів зображена на Рис.3.1.[25,26]

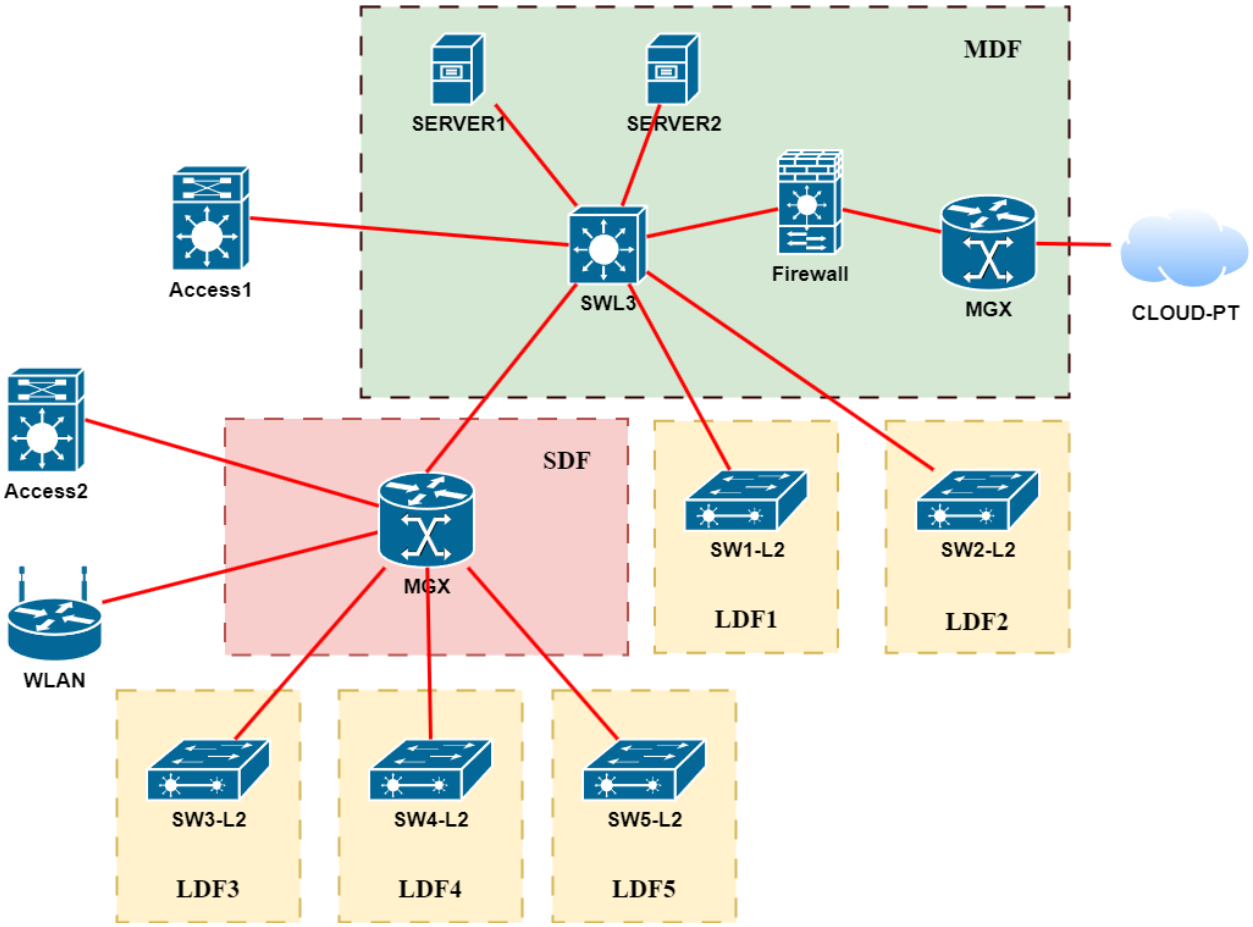

Рисунок 3.1 – Структурна схема мережі

Елементи структурної схеми комп'ютерної мережі:

- ❖ сервіс Інтернету;
- ❖ MDF:
  - пригранічний маршрутизатор: MGX;
  - міжмережевий екран: Firewall;
  - комутатор рівня 3: SWL3;
  - сервери загального та обмеженого доступу: Server1, Server2;
  - мережеві сегменти: LDF1, LDF2;
  - мережевий сегмент бездротового доступу: Access1.
- ❖ SDF:
  - мережеві сегменти: LDF3, LDF4, LDF5;
  - мережевий сегмент бездротового доступу: WLAN, Access2.

3.4 Фізична топологія, розрахунок довжини кабелю

Приєднаємо всі кінцеві пристрої до комутаторів та визначемо фізичне розташування МДФ та СДФ. Побудована кабельна підсистема зображена на Рис.А.5, Рис.А.6 (додаток А).

Для орієнтовного підрахунку кабельної системи використаємо макети 1 та 2 поверху будівлі Рис.А.1, Рис.А.2 (додаток А).

Існує кілька методів для розрахунку необхідної довжини кабеля для локальної мережі:

− Метод сумування;

− Емпіричний метод; Метод суми полягає в розрахунку довжини кабелю на окремих ділянках, які потім сумуються. До отриманого результату додається технологічний запас до 10% і запас розділки на розетках і кроссових панелях. Цей метод відзначається високою точністю, однак при великій кількості портів у локальній мережі і відсутності автоматизованих засобів для проектування стає складним у реалізації, а також може обмежувати вибір варіантів організації мережі.

Емпіричний метод використовує положення центральної граничної теореми теорії ймовірностей. Цей метод часто використовується для оцінки середньої довжини кабелю у мережі з великою кількістю робочих місць.

Тому краще скористатися методом сумування та занести дані до таблиці.

Таблиця 1.1 – Підрахунок ділянки кабелю

Поверх	Кабінет	Довжина ділянки, м
1	1-1	10,5
	1-2	5
	1-3	6
	1-4	11
2	2-5	11
	2-6	7
	2-7	4
	2-8	5
	2-9	4
	2-10	11

Отже, за результатами розрахунків, для кабельного з’єднання:
1 поверху = ±30,5 м кабелю витої пари;
2 поверху = ±41 м кабелю витої пари.

3.5 Вибір активного мережевого обладнання

Для реалізації запропонованої системи використовується широкий спектр апаратного забезпечення. До активного мережевого обладнання відносяться комутатори, маршрутизатори, міжмережеві екрани та набір різних кінцевих пристроїв. Проведемо порівняльний аналіз між такими виробниками як D-Link та Cisco. В процесі порівняння будуть обрані пристрої, які забезпечать більшу продуктивність, надійність та безпеку мережі.

Комутатор 2-го рівня

Комутатори 2-го рівня мережевої моделі OSI працюють на канальному рівні. Вони використовують MAC-адреси для передачі даних між пристроями у локальній мережі (LAN). Ці комутатори забезпечують ефективне та швидке з'єднання пристроїв, зменшують кількість колізій та забезпечують сегментацію мережі для поліпшення продуктивності. Керовані комутатори дозволяють адмініструвати, моніторити та налаштовувати мережу відповідно до потреб організації. Порівняємо комутатори 2-го рівня.

Таблиця 2.1 – Порівняння комутаторів Cisco Catalyst 2960 та D-Link DGS-1210.

Модель	Cisco Catalyst 2960	D-Link DGS-1210
Кількість портів	24 або 48 портів Gigabit Ethernet	24 або 48 портів Gigabit Ethernet
Рівень комутатора	2-й рівень	2-й рівень
Тип комутатора	Керований	Керований
Оперативна пам’ять, МБ	128 МБ	64 МБ
Флеш-пам’ять, МБ	64 МБ	16 МБ
Кількість VLAN, Тис	4,096	4,096
Розмір таблиці MAC-адрес, Тис	16	16
Комутаційна здатність, Гбіт/с	216 Гбіт/с (для моделі з 48 портами)	56 Гбіт/с
Комутація, Мпакетів/с	65.5 Мпакетів/с	41.7 Мпакетів/с
Комутаційна смуга пропускання	108 Гбіт/с (для моделі з 48 портами)	28 Гбіт/с
Робоча напруга, струм	100-240 В змінного струму, 0.5-2 А	100-240 В змінного струму, 0.5-2 А
Стандарти, що підтримуються	IEEE 802.1p, 802.1Q, 802.1s, 802.1w, 802.3ad, 802.3af, 802.3at, 802.3az	IEEE 802.1p, 802.1Q, 802.3ad, 802.3af, 802.3at, 802.3az
Напрацювання на відмову, г.	230,000 годин	250,000 годин

Cisco Catalyst 2960 має більшу оперативну та флеш-пам'ять, що може бути корисно для складніших мережевих конфігурацій та підтримки додаткових

функцій. Також він має вищу комутаційну здатність та пропускну здатність, що робить його більш підходящим для мереж з високим трафіком.

D-Link DGS-1210 має трохи вищий показник напрацювання на відмову, що робить його більш надійним у довгостроковій перспективі.

Обидва комутатори є гідним вибором. Але пріоритетом є продуктивність та розширені функції, тому для проектованої мережі варто обрати Cisco Catalyst 2960.

Рисунок 3.2 – Зовнішній вигляд комутатора Cisco Catalyst 2960 на 48 портів

Комутатор 3-го рівня

Комутатори 3-го рівня працюють як на канальному (2-му рівні), так і на мережевому (3-му рівні) моделі OSI. Вони використовують IP-адреси для направлення трафіку між різними сегментами мережі. Ці комутатори забезпечують високу швидкість комутації разом із можливостями маршрутизації, що дозволяє ефективно керувати великими та складними мережами. Порівняємо комутатори 3-го рівня.

Таблиця 2.2 – Порівняння комутаторів 3-го рівня Cisco Catalyst 3650-24 та D-Link DGS-3630-28TC.

Модель	Cisco Catalyst 3650-24	D-Link DGS-3630-28TC
Кількість портів	24 портів Gigabit Ethernet	24 портів Gigabit Ethernet + 4 SFP
Рівень комутатора	3-й рівень	3-й рівень
Тип комутатора	Керований	Керований
Оперативна пам’ять, МБ	4 ГБ	2 ГБ
Флеш-пам’ять, МБ	2 ГБ	128 МБ
Кількість VLAN, Тис	4,096	4,096
Розмір таблиці MAC-адрес, Тис	32	32
Комутаційна здатність, Гбіт/с	88 Гбіт/с	128 Гбіт/с
Комутація, Мпакетів/с	68.4 Мпакетів/с	95.23 Мпакетів/с
Комутаційна смуга пропускання	176 Гбіт/с	256 Гбіт/с

Продовження Таблиці 2.2

Робоча напруга, струм	100-240 В змінного струму, 1.2-3.0 А	100-240 В змінного струму, 1.2-3.0 А
Стандарти, що підтримуються	IEEE 802.1p, 802.1Q, 802.1s, 802.1w, 802.3ad, 802.3af, 802.3at, 802.3az	IEEE 802.1p, 802.1Q, 802.1s, 802.3ad, 802.3af, 802.3at, 802.3az
Напрацювання на відмову, г.	230,000 годин	300,000 годин

D-Link DGS-3630-28TC має вищу комутаційну здатність та пропускну здатність, що робить його більш підходящим для мереж з високим трафіком. Також має вищий показник напрацювання на відмову, що робить його більш надійним у довгостроковій перспективі. Обидва комутатори підтримують широкий спектр стандартів, але Cisco може пропонувати більш розширені функції управління та безпеки завдяки своїй більшій пам'яті.

У даному випадку слід обрати D-Link DGS-3630-28TC, який забезпечить більшу продуктивність та надійність.

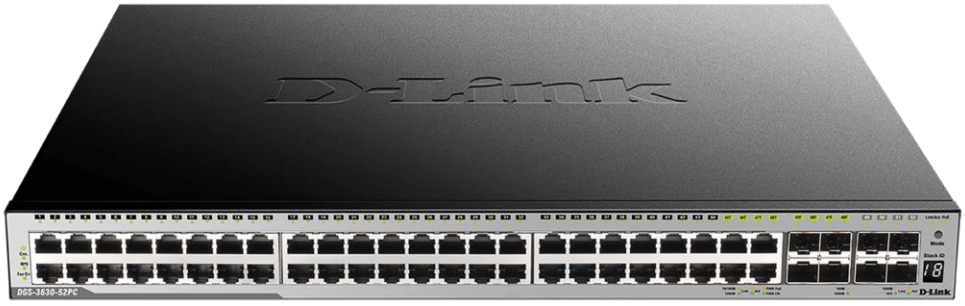

Рисунок 3.3 – Зовнішній вигляд комутатора D-Link DGS-3630-28TC

Бездротова точка доступу

Бездротові точки доступу забезпечують пристроям доступ до мережі Wi-Fi, підключаючи їх до проводової мережі. Вони використовуються для розширення зони покриття бездротової мережі та можуть підтримувати різні стандарти Wi-Fi, забезпечувати різні рівні безпеки та мати різні технічні характеристики. Порівняємо бездротові точки доступу Cisco Aironet 1832i та D-Link DAP-2680.

Таблиця 2.3 – Порівняння бездротових точок доступу.

Модель	Cisco Aironet 1832i	D-Link DAP-2680
Стандарт Wi-Fi	802.11ac Wave 2	802.11ac Wave 2
Максимальна швидкість	867 Мбіт/с на 5 ГГц, 300 Мбіт/с на 2.4 ГГц	1300 Мбіт/с на 5 ГГц, 450 Мбіт/с на 2.4 ГГц
Частотний діапазон	2.4 ГГц, 5 ГГц	2.4 ГГц, 5 ГГц
Кількість антен	3 внутрішні	4 внутрішні
MU-MIMO	Так, 2x2	Так, 3x3
Підтримка PoE	Так	Так
Порти Ethernet	1 порт Gigabit Ethernet	2 порти Gigabit Ethernet
Безпека	WPA, WPA2, 802.1X	WPA, WPA2, WPA3, 802.1X
Максимальна кількість клієнтів	200	256
Максимальна потужність передавача	23 dBm	28 dBm
Робоча температура	0°C до 40°C	-20°C до 60°C
Стандарти, що підтримуються	802.11a/b/g/n/ac	802.11a/b/g/n/ac
Напрацювання на відмову, г.	150,000 годин	200,000 годин

Cisco Aironet 1832i забезпечує стабільну продуктивність і надійність, добре підходить для підприємств з високими вимогами до безпеки та підтримки.

D-Link DAP-2680 пропонує вищу швидкість передачі даних та більшу кількість одночасних клієнтів, що робить його кращим вибором для середніх та великих мереж з великою кількістю користувачів.

Обидві точки доступу підтримують сучасні стандарти Wi-Fi і забезпечують високу продуктивність, але D-Link має перевагу в швидкості і потужності передавача.

В цьому випадку важливішою є надійність і безпека, тому Cisco Aironet 1832i буде кращим вибором.

Рисунок 3.4 – Зовнішній вигляд бездротової точки доступу Aironet 1832i

Маршрутизатор

Маршрутизатори - це мережеві пристрої, які визначають оптимальні шляхи для передачі даних між різними мережами. Вони функціонують на третьому рівні моделі OSI і використовують IP-адреси для направлення трафіку. Маршрутизатори забезпечують підключення до Інтернету, управління трафіком, забезпечення безпеки та інші функції мережевого управління. Порівняємо маршрутизатори Cisco 2811 та D-Link DSR-500.

Таблиця 2.4 – Порівняння маршрутизаторів.

Модель	Cisco 2811	D-Link DSR-500
Кількість портів Ethernet	2 порти 10/100 Ethernet	4 порти Gigabit Ethernet
WAN порти	2 порти 10/100 Ethernet	2 порти Gigabit Ethernet
Рівень маршрутизатора	3-й рівень	3-й рівень
Тип маршрутизатора	Керований	Керований
Оперативна пам’ять, МБ	256 МБ	128 МБ
Флеш-пам’ять, МБ	64 МБ	32 МБ
Підтримка VPN	Так (IPSec, PPTP, L2TP)	Так (IPSec, PPTP, L2TP)
Максимальна кількість VPN тунелів	150	75
Розширення слотів	2 слоти HWIC, 1 слот AIM	2 USB порти
Продуктивність VPN, Мбіт/с	90	50
Firewall	Так	Так
QoS	Так	Так
Надійність (MTBF), годин	150,000 годин	200,000 годин
Робоча температура	0°C до 40°C	-10°C до 55°C
Стандарти безпеки	802.1x, IPSec, SSL, SSH	802.1x, IPSec, SSL, SSH

Cisco 2811 має більшу кількість розширюваних слотів, що робить його більш гнучким для додавання нових функцій і розширення можливостей мережі. D-Link DSR-500 пропонує більше портів Gigabit Ethernet і підтримує сучасніші технології, що забезпечують вищу пропускну здатність.

Обидва маршрутизатори підтримують необхідні стандарти безпеки і мають функції QoS для управління трафіком.

Для проектованої мережі краще обрати D-Link DSR-500, який забезпечить високу пропускна здатність і надійність.

Рисунок 3.5 – Зовнішній вигляд маршрутизатора D-Link DSR-500

Міжмережевий екран

Міжмережеві екрани є важливими елементами мережевої безпеки, які контролюють та фільтрують вхідний і вихідний мережевий трафік на основі заданих правил безпеки. Вони забезпечують захист мережі від несанкціонованого доступу, атак та інших загроз, гарантують безпеку даних і збереження конфіденційності. Порівняємо міжмережеві екрани Cisco ASA 5505 та D-Link DFL-860E.

Таблиця 2.5 – Порівняння міжмережевих екранів.

Модель	Cisco ASA 5505	D-Link DFL-860E
Кількість портів Ethernet	8 портів 10/100 Ethernet	7 портів Gigabit Ethernet
WAN порти	2 порти 10/100 Ethernet	2 порти Gigabit Ethernet
Продуктивність Firewall, Мбіт/с	150 Мбіт/с	500 Мбіт/с
Продуктивність VPN, Мбіт/с	100 Мбіт/с	110 Мбіт/с
Максимальна кількість VPN тунелів	25	50
Підтримка VPN	Так (IPSec, L2TP, SSL)	Так (IPSec, L2TP, SSL)
Максимальна кількість з'єднань	10,000	20,000
Розширення слотів	0	1 слот USB
Підтримка PoE	Ні	Ні

Продовження Таблиці 2.5

Антивірус/Антиспам	Так (ліцензування додаткове)	Так (ліцензування додаткове)
QoS	Так	Так
Стандарти безпеки	802.1x, IPSec, SSL, SSH	802.1x, IPSec, SSL, SSH
Надійність (MTBF), годин	250,000 годин	200,000 годин
Робоча температура	0°C до 40°C	-10°C до 60°C

Cisco ASA 5505 має меншу кількість портів Ethernet, але забезпечує надійну продуктивність та високу безпеку для малих і середніх мереж. Також він забезпечує високу надійність з більшим MTBF, що важливо для критично важливих мереж. D-Link DFL-860E пропонує більшу кількість портів Gigabit Ethernet і вищу продуктивність Firewall, що робить його більш підходящим для мереж з високим трафіком. Обидва пристрої підтримують основні стандарти безпеки та мають функції антивірусу та антиспаму, що забезпечують додатковий рівень захисту мережі.

Краще обрати Cisco ASA 5505, який забезпечить надійність та вже перевірені технології безпеки.

Рисунок 3.6 – Зовнішній вигляд міжмережевого екрану Cisco ASA 5505

3.6 Висновок за розділом

У третьому розділі було проведено комплексний аналіз та планування комп'ютерної мережі для фінансової установи, зокрема страхової компанії. На основі плану приміщення та структури компанії було визначено оптимальне розташування обладнання в кожному приміщенні, що забезпечує ефективне використання простору та комфорт для працівників. Детально розглянуто та визначено телекомунікаційні вузли, які відіграють ключову роль у забезпеченні стабільного та безперебійного зв'язку між різними частинами

мережі. Особливу увагу приділено структурі кабельної підсистеми, де було здійснено розрахунок довжини кабелю для забезпечення оптимального покриття всіх необхідних ділянок мережі. Вибір активного мережевого обладнання був здійснений з урахуванням специфічних вимог компанії, що дозволяє досягти високої продуктивності та надійності мережевої інфраструктури.

4. Моделювання, налаштування, тестування проектованої мережі

4.1 Моделювання мережі

Перед прямим впровадженням розробленої мережі необхідно переконатися в її коректності. Для створення та перевірки роботи системи та окремих її частин було використано програмний інструмент Cisco Packet Tracer, який є симулятором для налаштування комп'ютерних мереж. Ця програма надає можливість максимально точно симулювати роботу обчислювальної мережі. На початковому етапі ми створимо таблицю адресації активного обладнання мережі. Для кожного вузла вкажемо наступні параметри мережевого налаштування:

- IP-адреса вузла;
- маска підмережі;
- шлюз за замовчуванням;
- IP-адреса сервера DNS;
- метод призначення мережевих параметрів налаштувань: автоматично (DHCP) або вручну.

Таблиця 3.1 – IP-адресація

Вузол	IP-адреса (з маскою)	Шлюз за замовчуванням	IP-адреса сервера DNS	Метод призначення
Router1	192.168.0.1/24	-	-	Вручну
Router2	192.168.6.1/24	-	-	Вручну
WLAN	192.168.7.1/24	-	-	Вручну
Access1	192.168.8.1/24	-	-	Вручну
Access2	192.168.9.1/24	-	-	Вручну
Multilayer Switch0	192.168.0.3/24	192.168.0.1	192.168.0.3	Вручну
Switch0	192.168.1.1/24	192.168.1.1	192.168.1.2	Вручну
Switch1	192.168.2.1/24	192.168.2.1	192.168.2.2	Вручну
Switch2	192.168.3.1/24	192.168.3.1	192.168.3.2	Вручну
Switch3	192.168.4.1/24	192.168.4.1	192.168.4.2	Вручну
Switch4	192.168.5.1/24	192.168.5.1	192.168.5.2	Вручну
Server1	192.168.0.4/24	192.168.0.1	192.168.0.3	Вручну
Server2	192.168.0.5/24	192.168.0.1	192.168.0.3	Вручну
Cloud0	192.168.0.6/24	192.168.0.1	192.168.0.3	Вручну
ASA5506	192.168.0.2/24	192.168.0.1	192.168.0.3	Вручну

Продовження таблиці 3.1

Printer0 - Printer10	192.168.1.13 - 192.168.4.5/24	192.168.1.1	192.168.1.2	Вручну
Laptop0 – Laptop3	192.168.4.1 - 192.168.4.4/24	192.168.5.1	192.168.5.2	DHCP
PC1 - PC10	192.168.1.2 - 192.168.1.12/24	192.168.1.1	192.168.1.2	DHCP
PC11 - PC13	192.168.2.2 - 192.168.2.4/24	192.168.2.1	192.168.2.2	DHCP
PC14 - PC17	192.168.3.2 - 192.168.3.5/24	192.168.6.1	192.168.6.2	DHCP
PC18 - PC20	192.168.4.2 - 192.168.4.4/24	192.168.7.1	192.168.7.2	DHCP

Локальна мережа, що була спроектована, використовує топологію ієрархічна зірка. Ця структура мережі включає центральний компонент - маршрутизатор. Топологія «ієрархічна зірка» відома своєю популярністю і ефективністю, оскільки полегшує обслуговування кінцевих пристроїв.

Отже створимо мереже використовуючи план схему (Додаток А, Рис.А.3, Рис.А.4). Сворена мережа зображена у Додатку Б Рис.Б.1.

4.2 Конфігураційні параметри налаштувань

Для кожного активного мережевого пристрою потрібно зробити ряд налаштувань. Налаштування маршрутизаторів та керованих комутаторів має проходити за наступною схемою:

- ім'я пристрою;
- паролі доступу (локального та віддаленого);
- пароль доступу до привілейованого режиму;
- описи інтерфейсів;
- протоколу VTP;
- протоколу STP;
- створення VLAN;
- налаштування режиму роботи порта (access або trunk);
- налаштування приналежності порта до мережі VLAN;
- налаштування IP-адреси фізичних та віртуальних (VLAN) інтерфейсів;
- протоколу динамічної маршрутизації;
- статичних маршрутів та маршруту за замовчуванням.

Для точки бездротового доступу необхідно вказати:

- ім'я точки;
- пароль доступу до налаштувань;
- IP-адресу, маску підмережі, шлюз за замовчуванням;
- ім'я бездротової мережі (SSID);
- стандарт бездротової технології;
- канал роботи;
- тип автентифікації;
- алгоритм шифрування;

- ключ доступу.

Для міжмережевого екрану були налаштовані NAT та IPS.

Всі налаштування будуть зроблені у вигляді лістінгів (Додаток Б).

4.3 Логічна топологія

Відповідно до розробленої схеми IP-адресації розробити логічну топологію комп'ютерної мережі. На логічній топології буде зобраажено:

- мережеві пристрої 2-го та 3-го рівня з прив'язкою до ТКВ;
- логічні ідентифікатори мережевих пристроїв;
- номер VLAN.

Сворена логічна топологія мережі на Рисунку.Б.2(Додаток Б).

4.4 Тестування працездатності мережі

Для перевірки працездатності мережі виконаємо команду ping між абонентами мережі.

Пропінгуємо Laptop0 з PC13

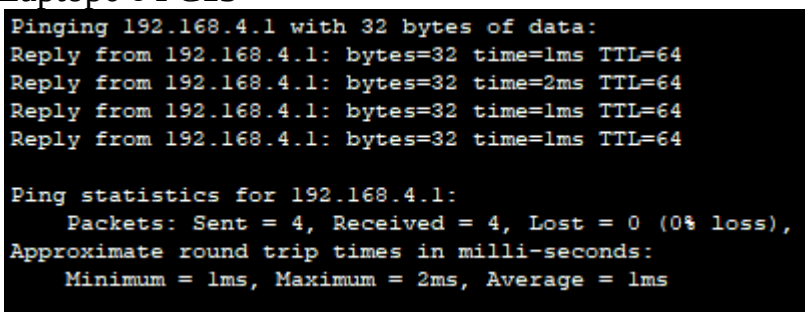

Рисунок 3.2 – Результат виконання команди ping 192.168.4.1

Пропінгуємо PC4 з PC18

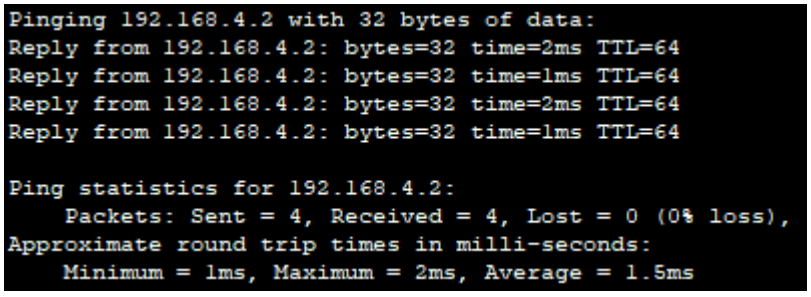

Рисунок 3.4 – Результат виконання команди ping 192.168.4.2

4.4 Висновок за розділом

У третьому розділі, було прописана IP-адресація активного обладнання. Була побудована проектована мережа у програмному застосунку Cisco Packet Trace. Для маршрутизатору, керованих комутаторів, точки бездротового доступу були зроблені всі необхідні конфігураційні налаштування. З різних пристроїв мережі було проведене пінгування, для підтвердження працездатності.

Висновки

Під час виконання кваліфікаційної роботи було проведено детальний аналіз та планування фізичної топології мережі. Було розглянуто основні концепції створення мережі, побудовано план приміщення та визначено оптимальне розташування обладнання. Проведено аналіз телекомунікаційних вузлів та зроблено вибір необхідного мережевого обладнання з урахуванням потреб та вимог проекту. Було визначено передумови створення захисту в комп’ютерних мережах, принципи захисту інформації у мережах, підключених до інтернету, види мережевих атак, методи їх виявлення та захисту. Також у Packet Tracer була створена модель мережі, налаштовано конфігураційні параметри кінцевих приладів та було зроблено тестування працездатності мережі. В результаті, була успішно реалізована локальна комп'ютерна мережа, яка відповідає всім вимогам та специфікаціям проекту. Було детально розглянуто структуру та принципи роботи мережевої моделі OSI, а також механізми комутації в локальних мережах. Одержані результати підтверджують ефективність та надійність розробленої мережі, що відповідає поставленим завданням та потребам.

Список використаних джерел

1. Комп'ютерні мережі. URL: https://e-tk.lntu.edu.ua/mod/page/view.php?id=3544 (дата звернення 06.05.2024)
2. Лекція №2. Комп’ютерні мережі та їх класифікація. URL: https://km.ptngu.com/lections/2.html (дата звернення 06.05.2024)
3. Топологія локальних мереж. URL: https://ua5.org/lan/125-topologja-lokalnikh-merezh.html (дата звернення 06.05.2024)
4. Лекція 4. Технології захисту інформації. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/4186 (дата звернення 06.05.2024)
5. Швиденко М.З., Матус Ю.В.. Комп’ютерні мережні технології. / Навч.метод. посібник. – Київ. – ТОВ “Авета”, - 2008.
6. Лозікова Г.М. Комп’ютерні мережі: Навчально-методичний посібник.– К.: Центр навчальної літератури, 2004.–128
7. Габрусєв В.Ю. Вивчаємо комп’ютерні мережі. – К.: Вид. дім "Шкільний світ", 2005. – 128 с.
8. Кім Р. "Методи захисту інформації в інтернеті", Київ: Видавництво "Політехніка", 2016. 480 с.
9. Види атак на інформацію та методи її захисту. URL: https://flashstart.com/understanding-different-kinds-of-network-attacks/ (дата звернення 06.05.2024).
10. Грайворонський М. В. Безпека інформаційно-комунікаційних систем: підруч. для студ. вищ. навч. закл., які навчаються за напрямами "Безпека інформаційних і комунікаційних систем", "Системи технічного захисту інформації", "Управління інформаційною безпекою" / М. В. Грайворонський, О. М. Новіков. – К. : Видво BHV, 2009. – 608 с
11. Види атак на інформацію та методи її захисту. URL: https://wiki.tntu.edu.ua (дата звернення 06.05.2024).
12. Advantage and Disadvantages Of Firewalls. URL: https://teleforum.ethiotelecom.et/blogs/2564/Advantage-and-Disadvantages-Of-Firewalls (дата звернення 06.05.2024).
13. Види захисту. URL:https://magistrweb.wordpress.com/home-2/protection/ (дата звернення 06.05.2024).

					КНУ.ПК.123.23.09.СВД		
Змн.	Арк.	№ документа	Підпис	Дата			
Розробив		Коваленко			СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	Літера	Аркуш / Аркушів
Перевірив		Чубаров					
Н.контроль		Кузнєцов				КІ-20	
Затвердив		Купін					

14. Маршрутизация трафика (NAT). URL: https://timeweb.cloud/docs/vpc/nat (дата звернення 06.05.2024).
15. Johnson E. "Systems for detecting and preventing attacks", New Brunswick: Publishing "ACT", 2016. 528 с.
16. Обнаружение и предотвращение атак и вторжений (IDS/IPS). URL: https://www.usergate.com/ru/products/ips (дата звернення 06.05.2024).
17. Firewalls, IDS, and IPS Explanation and Comparison. URL: https://study-ccna.com/firewalls-ids-ips-explanation-comparison/ (дата звернення 06.05.2024).
18. Офіційний сайт draw.io. URL: https://app.diagrams.net/ (дата звернення 06.05.2024).
19. Stallings, W. Data and Computer Communications. Upper Saddle River, NJ: Pearson Education. 2013. 784 p.
20. Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer Networks. Boston, MA: Pearson Education. 2011. 600 p.
21. Офіційний сайт Cisco. URL: https://www.cisco.com (дата звернення 06.05.2024).

Додаток А

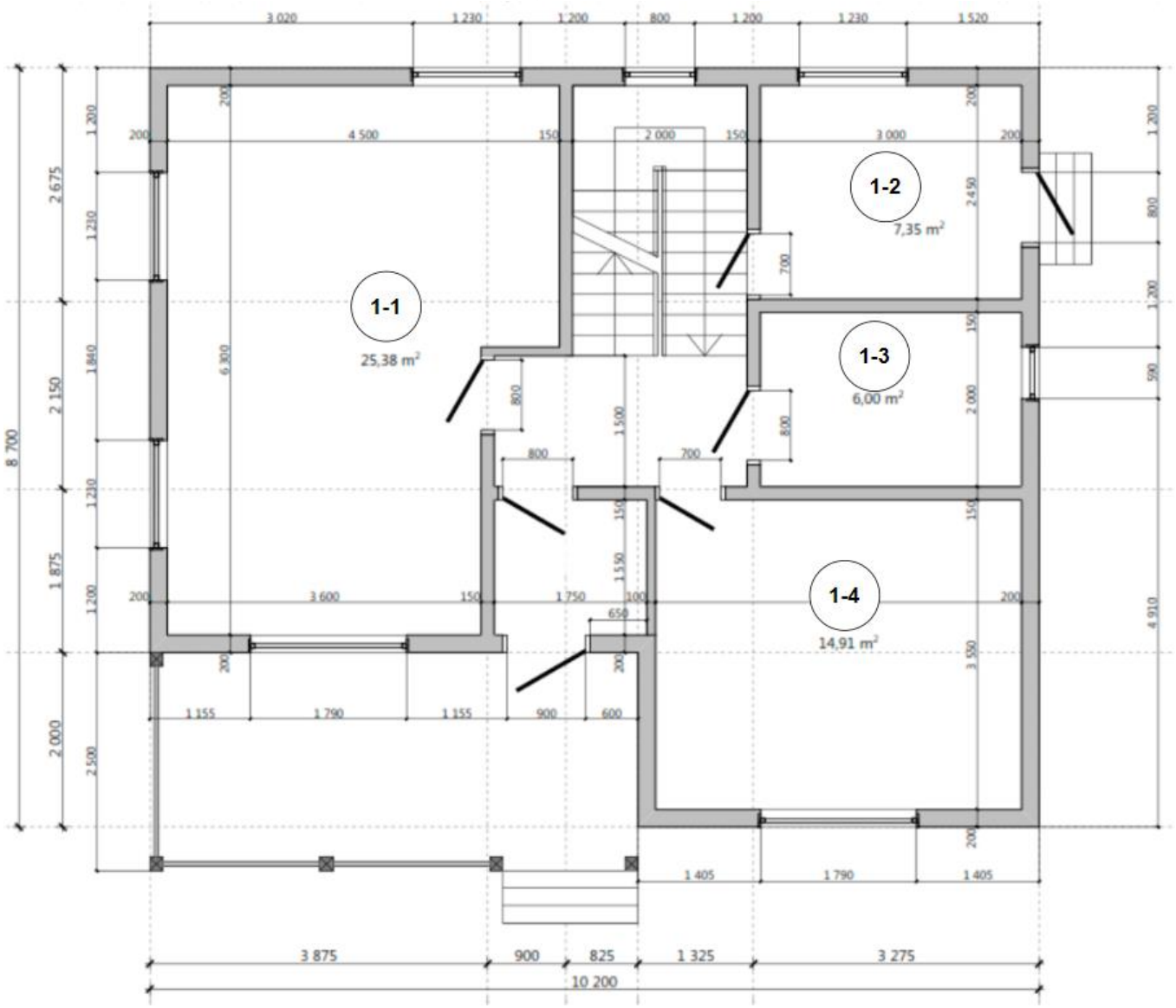

Рис.А.1 – Макет 1 поверху страхової

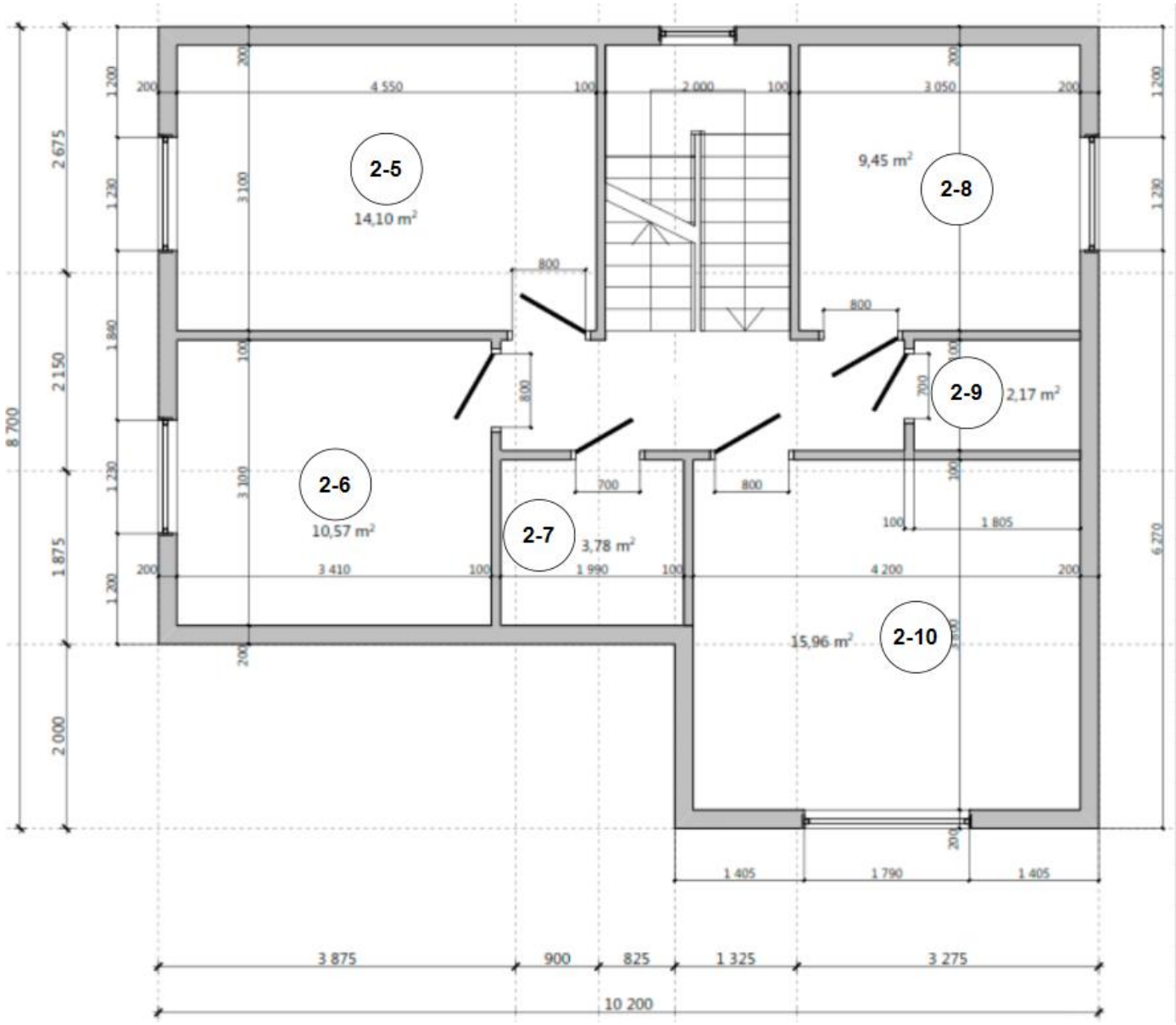

Рис.А.2 – Макет 2 поверху страхової

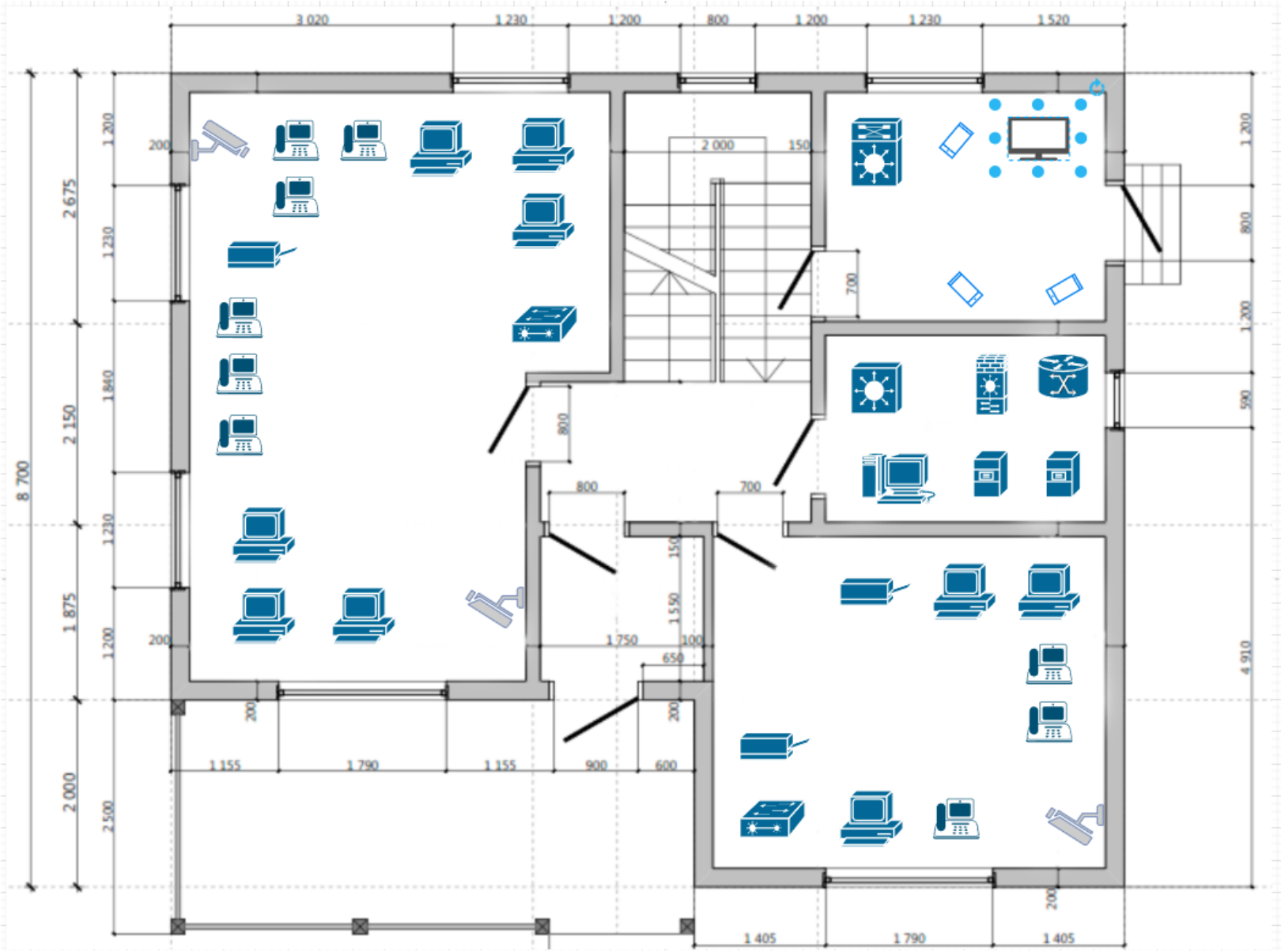

Рис.А.3 – Розташування мережевого обладнання на 1 поверсі

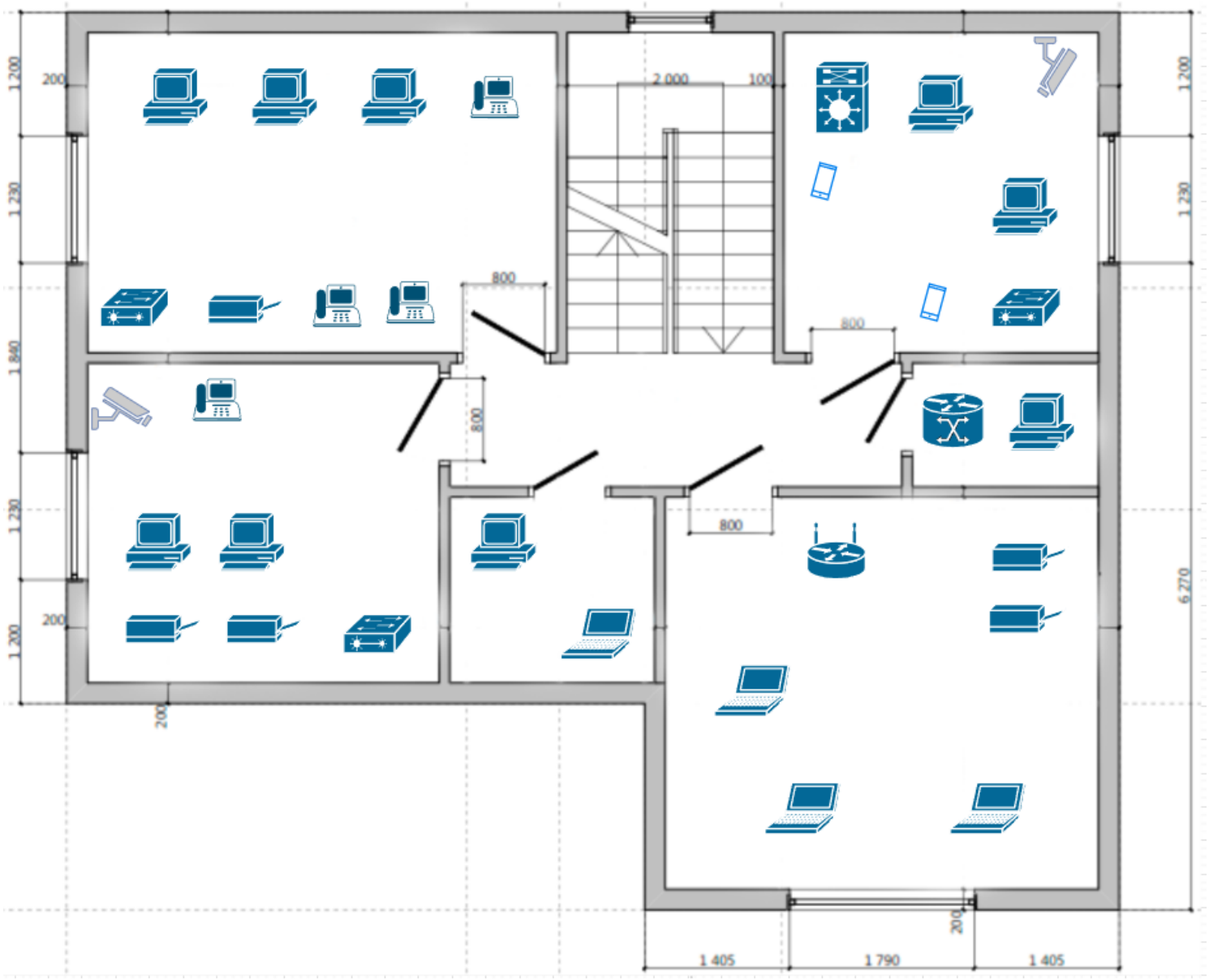

Рис.А.4 – Розташування мережевого обладнання на 2 поверсі

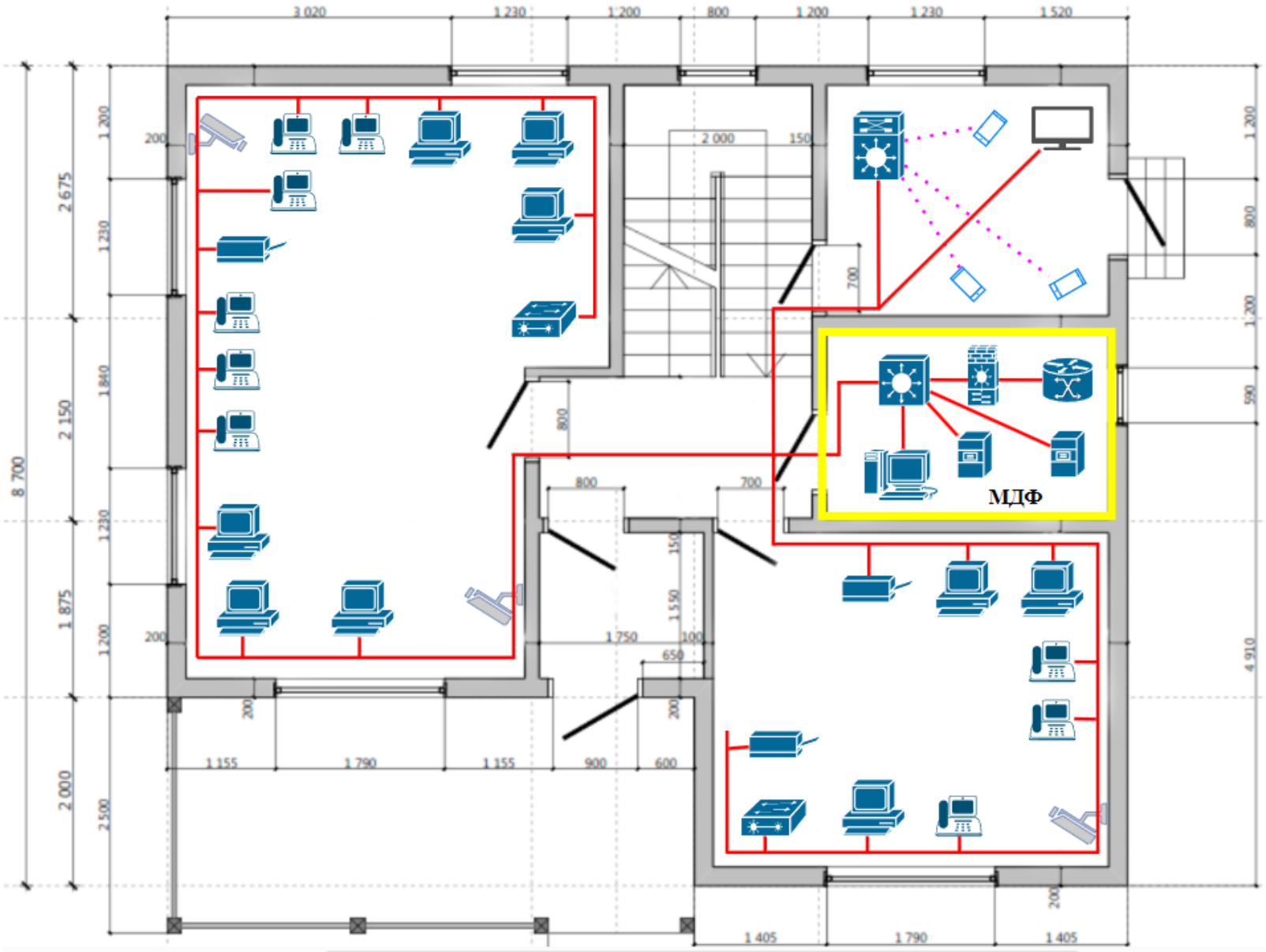

Рис.А.5 – Фізична топологія 1 поверху

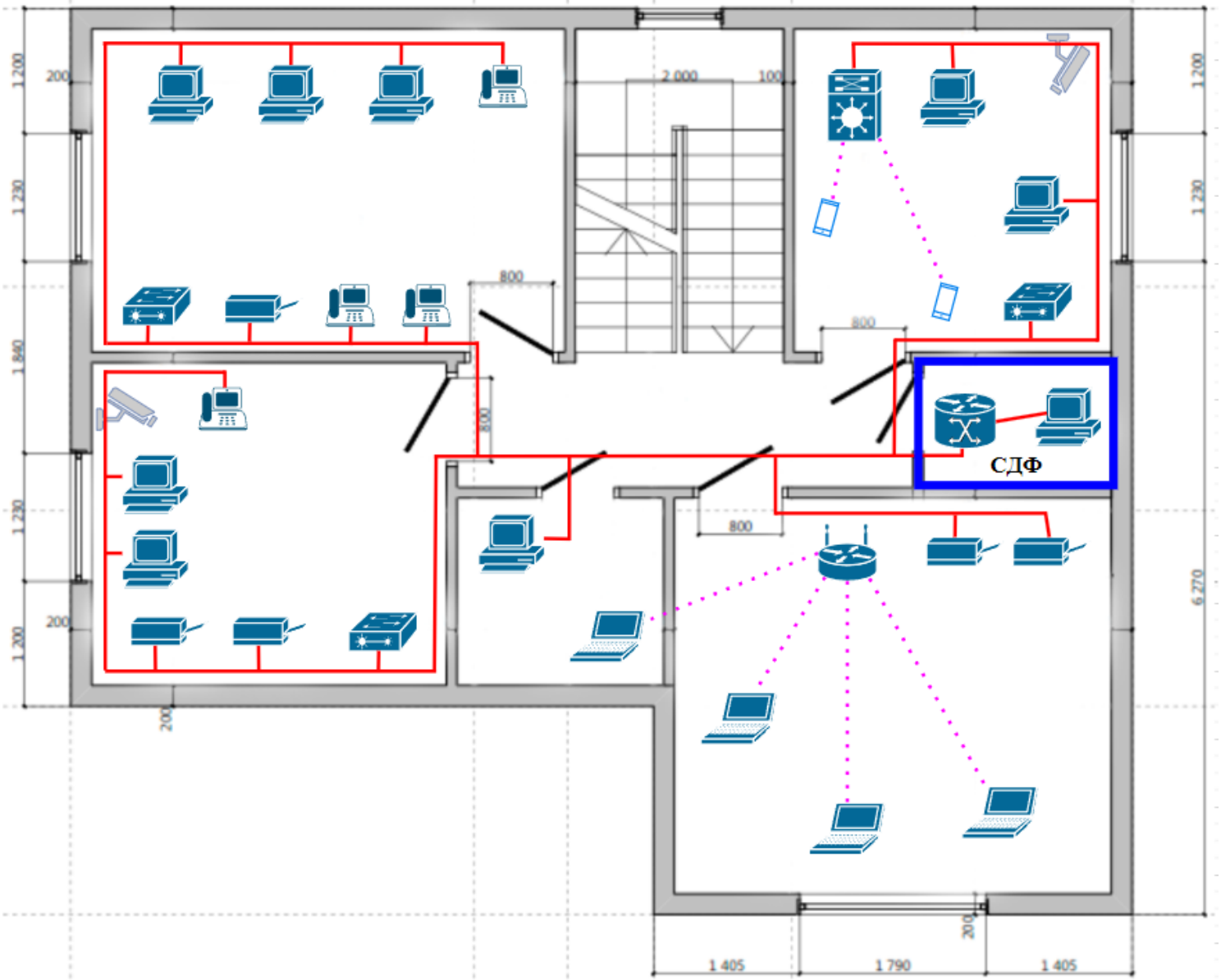

Рис.А.6 – Фізична топологія 2 поверху

Додаток Б

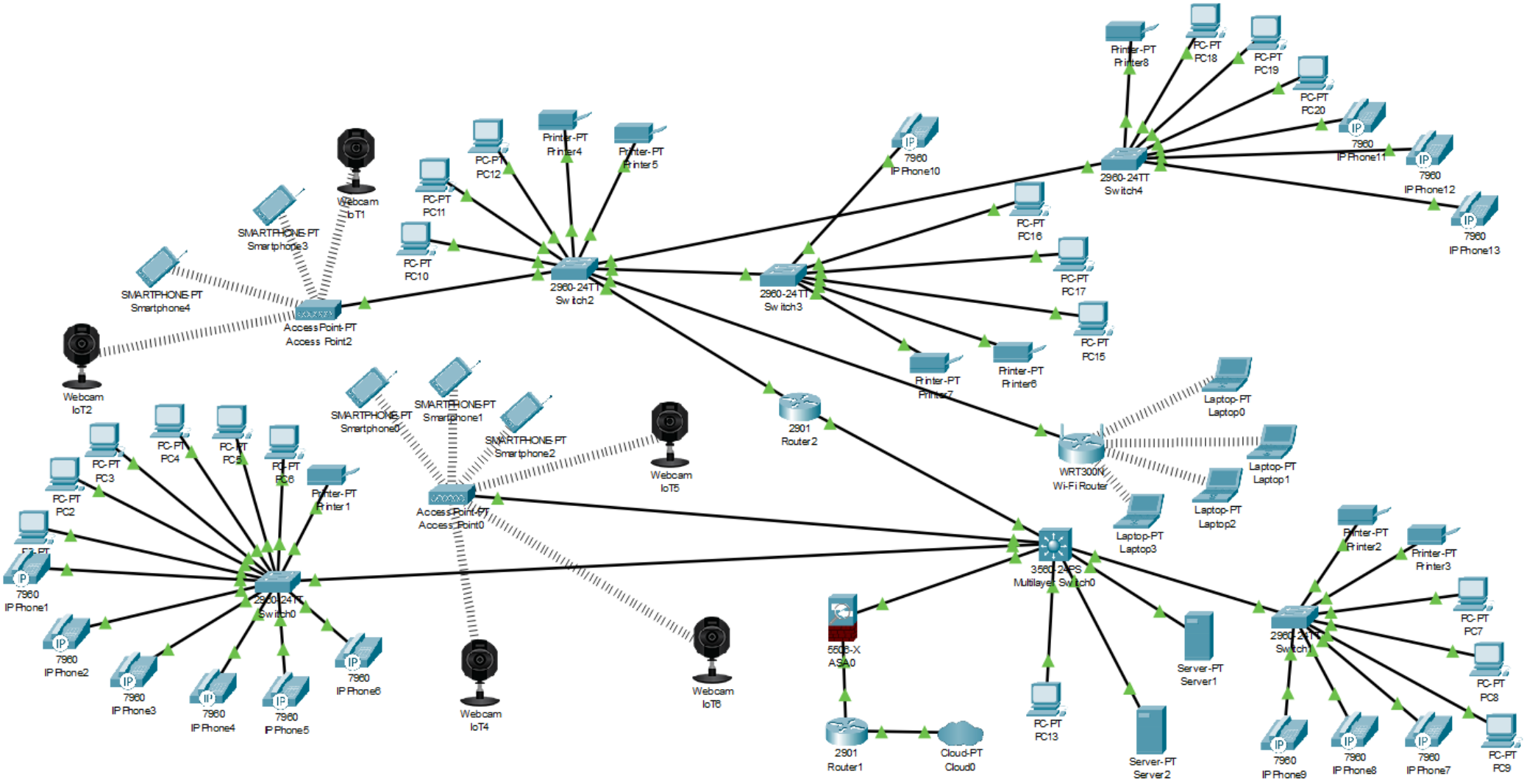

Рис.Б.1 – Модель мережі в Packet Tracer

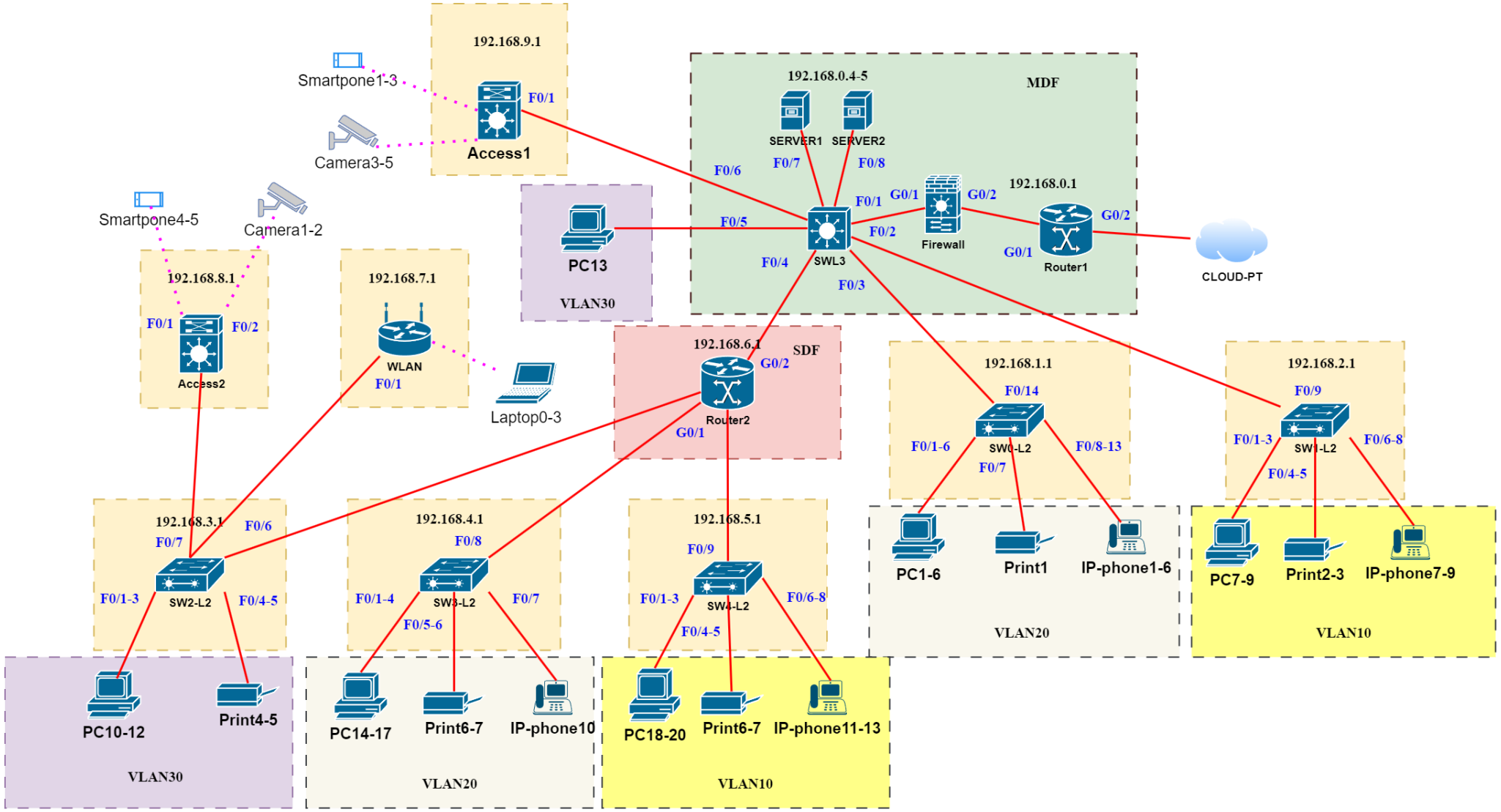

Рис.Б.2 – Логічна топологія мережі

Лістинг 3.1 – Налаштування комутатора Switch0:

```
Switch>enable
Switch#configure terminal
! Зміна імені пристрою
Switch(config)#hostname Switch0
! Встановлення паролів доступу
Switch0(config)#enable secret Cisco
Switch0(config)#line console 0
Switch0(config-line)#password Cisco
Switch0(config-line)#login
Switch0(config-line)#exit
Switch0(config)#line vty 0 15
Switch0(config-line)#password Cisco
Switch0(config-line)#login
Switch0(config-line)#exit
! Опис інтерфейсів
Switch0(config)#interface FastEthernet0/1
Switch0(config-if)#description Link to Router1
Switch0(config-if)#exit
! Налаштування протоколу VTP
Switch0(config)#vtp mode server
Switch0(config)#vtp domain mydomain
Switch0(config)#vtp password Cisco
! Налаштування протоколу STP
Switch0(config)#spanning-tree mode pvst
! Створення VLAN
Switch0(config)#vlan 10
Switch0(config-vlan)#name Sales
Switch0(config-vlan)#exit
Switch0(config)#vlan 20
Switch0(config-vlan)#name Marketing
Switch0(config-vlan)#exit
Switch0(config)#vlan 30
Switch0(config-vlan)#name Engineering
Switch0(config-vlan)#exit
! Налаштування режиму роботи порта та його приналежності до VLAN
Switch0(config)#interface FastEthernet0/1
Switch0(config-if)#switchport mode trunk
Switch0(config-if)#exit
Switch0(config)#interface FastEthernet0/2
Switch0(config-if)#switchport mode access
Switch0(config-if)#switchport access vlan 10
Switch0(config-if)#exit
Switch0(config)#interface FastEthernet0/3
Switch0(config-if)#switchport mode access
Switch0(config-if)#switchport access vlan 20
```

```
Switch0(config-if)#exit
Switch0(config)#interface FastEthernet0/4
Switch0(config-if)#switchport mode access
Switch0(config-if)#switchport access vlan 30
Switch0(config-if)#exit
! Налаштування IP-адреси для VLAN інтерфейсів
Switch0(config)#interface vlan 1
Switch0(config-if)#ip address 192.168.1.1 255.255.255.0
Switch0(config-if)#no shutdown
Switch0(config-if)#exit
! Динамічна маршрутизація (немає потреби на комутаторі, але для повноти прикладу)
! Припустимо, ми використовуємо статичні маршрути
Switch0(config)#ip routing
Switch0(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.254
! Збереження конфігурації
Switch0(config)#exit
Switch0#copy running-config startup-config
```

Лістинг 3.2 – Налаштування комутатора Switch1:

```
Switch>enable
Switch#configure terminal
! Зміна імені пристрою
Switch(config)#hostname Switch1
! Встановлення паролів доступу
Switch1(config)#enable secret Cisco
Switch1(config)#line console 0
Switch1(config-line)#password Cisco
Switch1(config-line)#login
Switch1(config-line)#exit
Switch1(config)#line vty 0 15
Switch1(config-line)#password Cisco
Switch1(config-line)#login
Switch1(config-line)#exit
! Опис інтерфейсів
Switch1(config)#interface FastEthernet0/1
Switch1(config-if)#description Link to Router1
Switch1(config-if)#exit
! Налаштування протоколу VTP
Switch1(config)#vtp mode server
Switch1(config)#vtp domain mydomain
Switch1(config)#vtp password Cisco
```

```
! Налаштування протоколу STP
Switch1(config)#spanning-tree mode pvst
! Створення VLAN
Switch1(config)#vlan 10
Switch1(config-vlan)#name Sales
Switch1(config-vlan)#exit
Switch1(config)#vlan 20
Switch1(config-vlan)#name Marketing
Switch1(config-vlan)#exit
Switch1(config)#vlan 30
Switch1(config-vlan)#name Engineering
Switch1(config-vlan)#exit
! Налаштування режиму роботи порта та його приналежності до VLAN
Switch1(config)#interface FastEthernet0/1
Switch1(config-if)#switchport mode trunk
Switch1(config-if)#exit
Switch1(config)#interface FastEthernet0/2
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 10
Switch1(config-if)#exit
Switch1(config)#interface FastEthernet0/3
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 20
Switch1(config-if)#exit
Switch1(config)#interface FastEthernet0/4
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport access vlan 30
Switch1(config-if)#exit
! Налаштування IP-адреси для VLAN інтерфейсів
Switch1(config)#interface vlan 1
Switch1(config-if)#ip address 192.168.2.1 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config-if)#exit
! Динамічна маршрутизація
Switch1(config)#ip routing
Switch1(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.254
! Збереження конфігурації
Switch1(config)#exit
Switch1#copy running-config startup-config
```

Лістинг 3.3 – Налаштування комутатора Switch2:

```
Switch>enable
Switch#configure terminal
! Зміна імені пристрою
Switch(config)#hostname Switch2
! Встановлення паролів доступу
Switch2(config)#enable secret Cisco
Switch2(config)#line console 0
Switch2(config-line)#password Cisco
Switch2(config-line)#login
Switch2(config-line)#exit
Switch2(config)#line vty 0 15
Switch2(config-line)#password Cisco
Switch2(config-line)#login
Switch2(config-line)#exit
! Опис інтерфейсів
Switch2(config)#interface FastEthernet0/1
Switch2(config-if)#description Link to Router1
Switch2(config-if)#exit
! Налаштування протоколу VTP
Switch2(config)#vtp mode server
Switch2(config)#vtp domain mydomain
Switch2(config)#vtp password Cisco
! Налаштування протоколу STP
Switch2(config)#spanning-tree mode pvst
! Створення VLAN
Switch2(config)#vlan 10
Switch2(config-vlan)#name Sales
Switch2(config-vlan)#exit
Switch2(config)#vlan 20
Switch2(config-vlan)#name Marketing
Switch2(config-vlan)#exit
Switch2(config)#vlan 30
Switch2(config-vlan)#name Engineering
Switch2(config-vlan)#exit
! Налаштування режиму роботи порта та його приналежності до VLAN
Switch2(config)#interface FastEthernet0/1
Switch2(config-if)#switchport mode trunk
Switch2(config-if)#exit
Switch2(config)#interface FastEthernet0/2
```

```
Switch2(config-if)#switchport mode access
Switch2(config-if)#switchport access vlan 10
Switch2(config-if)#exit
Switch2(config)#interface FastEthernet0/3
Switch2(config-if)#switchport mode access
Switch2(config-if)#switchport access vlan 20
Switch2(config-if)#exit
Switch2(config)#interface FastEthernet0/4
Switch2(config-if)#switchport mode access
Switch2(config-if)#switchport access vlan 30
Switch2(config-if)#exit
! Налаштування IP-адреси для VLAN інтерфейсів
Switch2(config)#interface vlan 1
Switch2(config-if)#ip address 192.168.3.1 255.255.255.0
Switch2(config-if)#no shutdown
Switch2(config-if)#exit
! Динамічна маршрутизація
Switch2(config)#ip routing
Switch2(config)#ip route 0.0.0.0 0.0.0.0 192.168.3.254
! Збереження конфігурації
Switch2(config)#exit
Switch2#copy running-config startup-config
```

Лістинг 3.3 – Налаштування комутатора Switch3:

```
Switch>enable
Switch#configure terminal
! Зміна імені пристрою
Switch(config)#hostname Switch3
! Встановлення паролів доступу
Switch3(config)#enable secret Cisco
Switch3(config)#line console 0
Switch3(config-line)#password Cisco
Switch3(config-line)#login
Switch3(config-line)#exit
Switch3(config)#line vty 0 15
Switch3(config-line)#password Cisco
Switch3(config-line)#login
Switch3(config-line)#exit
! Опис інтерфейсів
Switch3(config)#interface FastEthernet0/1
```

```
Switch3(config-if)#description Link to Router1
Switch3(config-if)#exit
! Налаштування протоколу VTP
Switch3(config)#vtp mode server
Switch3(config)#vtp domain mydomain
Switch3(config)#vtp password Cisco
! Налаштування протоколу STP
Switch3(config)#spanning-tree mode pvst
! Створення VLAN
Switch3(config)#vlan 10
Switch3(config-vlan)#name Sales
Switch3(config-vlan)#exit
Switch3(config)#vlan 20
Switch3(config-vlan)#name Marketing
Switch3(config-vlan)#exit
Switch3(config)#vlan 30
Switch3(config-vlan)#name Engineering
Switch3(config-vlan)#exit
! Налаштування режиму роботи порта та його приналежності до VLAN
Switch3(config)#interface FastEthernet0/1
Switch3(config-if)#switchport mode trunk
Switch3(config-if)#exit
Switch3(config)#interface FastEthernet0/2
Switch3(config-if)#switchport mode access
Switch3(config-if)#switchport access vlan 10
Switch3(config-if)#exit
Switch3(config)#interface FastEthernet0/3
Switch3(config-if)#switchport mode access
Switch3(config-if)#switchport access vlan 20
Switch3(config-if)#exit
Switch3(config)#interface FastEthernet0/4
Switch3(config-if)#switchport mode access
Switch3(config-if)#switchport access vlan 30
Switch3(config-if)#exit
! Налаштування IP-адреси для VLAN інтерфейсів
Switch3(config)#interface vlan 1
Switch3(config-if)#ip address 192.168.4.1 255.255.255.0
Switch3(config-if)#no shutdown
Switch3(config-if)#exit
! Динамічна маршрутизація
Switch3(config)#ip routing
```

```
Switch3(config)#ip route 0.0.0.0 0.0.0.0 192.168.4.254
! Збереження конфігурації
Switch3(config)#exit
Switch3#copy running-config startup-config
```

Лістинг 3.4 – Налаштування комутатора 3-го рівня Multilayer Switch0:

```
MultilayerSwitch0>enable
MultilayerSwitch0#configure terminal
MultilayerSwitch0(config)#hostname MultilayerSwitch0
! Налаштування паролів доступу
MultilayerSwitch0(config)#enable secret Cisco
MultilayerSwitch0(config)#line console 0
MultilayerSwitch0(config-line)#password Cisco
MultilayerSwitch0(config-line)#login
MultilayerSwitch0(config-line)#exit
MultilayerSwitch0(config)#line vty 0 4
MultilayerSwitch0(config-line)#password Cisco
MultilayerSwitch0(config-line)#login
MultilayerSwitch0(config-line)#exit
! Пароль доступу до привілейованого режиму
MultilayerSwitch0(config)#enable secret Cisco
! Описи інтерфейсів
MultilayerSwitch0(config)#interface FastEthernet 0/1
MultilayerSwitch0(config-if)#description Connected to Switch0
MultilayerSwitch0(config-if)#exit
MultilayerSwitch0(config)#interface FastEthernet 0/2
MultilayerSwitch0(config-if)#description Connected to Switch1
MultilayerSwitch0(config-if)#exit
MultilayerSwitch0(config)#interface FastEthernet 0/3
MultilayerSwitch0(config-if)#description Connected to Switch2
MultilayerSwitch0(config-if)#exit
MultilayerSwitch0(config)#interface FastEthernet 0/4
MultilayerSwitch0(config-if)#description Connected to Server0
MultilayerSwitch0(config-if)#exit
MultilayerSwitch0(config)#interface FastEthernet 0/5
MultilayerSwitch0(config-if)#description Connected to ASA0
MultilayerSwitch0(config-if)#exit
! Налаштування VTP
MultilayerSwitch0(config)#vtp mode server
MultilayerSwitch0(config)#vtp domain myVTPDomain
MultilayerSwitch0(config)#vtp password Cisco
!
```

Налаштування STP
MultilayerSwitch0(config)#spanning-tree mode pvst
! Налаштування режиму роботи порта (access або trunk)
MultilayerSwitch0(config)#interface range FastEthernet 0/1-3
MultilayerSwitch0(config-if-range)#switchport mode trunk
MultilayerSwitch0(config)#interface FastEthernet 0/4
MultilayerSwitch0(config-if)#switchport mode access
MultilayerSwitch0(config)#interface FastEthernet 0/5
MultilayerSwitch0(config-if)#switchport mode access
! Протокол динамічної маршрутизації (OSPF)
MultilayerSwitch0(config)#router ospf 1
MultilayerSwitch0(config-router)#network 10.0.0.0 0.0.0.255 area 0
MultilayerSwitch0(config-router)#network 10.0.2.0 0.0.0.255 area 0
MultilayerSwitch0(config-router)#network 10.0.3.0 0.0.0.255 area 0
MultilayerSwitch0(config-router)#exit
! Статичні маршрути та маршрут за замовчуванням
MultilayerSwitch0(config)#ip route 0.0.0.0 0.0.0.0 10.0.0.2
MultilayerSwitch0(config)#end
MultilayerSwitch0#write memory

Лістинг 3.5 – Налаштування маршрутизатора Router1:
Router1>enable
Router1#configure terminal
Router1(config)#hostname Router1
! Налаштування паролів доступу
Router1(config)#enable secret Cisco
Router1(config)#line console 0
Router1(config-line)#password Cisco
Router1(config-line)#login
Router1(config-line)#exit
Router1(config)#line vty 0 4
Router1(config-line)#password Cisco
Router1(config-line)#login
Router1(config-line)#exit
! Пароль доступу до привілейованого режиму
Router1(config)#enable secret Cisco
! Налаштування IP-адреси фізичних інтерфейсів
Router1(config)#interface FastEthernet 0/0
Router1(config-if)#ip address 10.0.4.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#interface FastEthernet 0/1
Router1(config-if)#ip address 192.168.1.1 255.255.255.0
Router1(config-if)#no shutdown

```
Router1(config-if)#exit
! Протокол динамічної маршрутизації (OSPF)
Router1(config)#router ospf 1
Router1(config-router)#network 10.0.4.0 0.0.0.255 area 0
Router1(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router1(config-router)#exit
! Статичні маршрути та маршрут за замовчуванням
Router1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.254
Router1(config)#end
Router1#write memory
```

Лістинг 3.6 – Налаштування бездротової точки доступу:

```
! Вхід у налаштування точки доступу
AP>enable
AP#configure terminal
! Ім'я точки доступу
AP(config)#hostname AP0
! Пароль доступу до налаштувань
AP(config)#enable secret Cisco
AP(config)#line console 0
AP(config-line)#password Cisco
AP(config-line)#login
AP(config-line)#exit
AP(config)#line vty 0 4
AP(config-line)#password Cisco
AP(config-line)#login
AP(config-line)#exit
! Налаштування IP-адреси, маски підмережі, шлюзу за замовчуванням
AP(config)#interface BVI1
AP(config-if)#ip address 10.0.2.3 255.255.255.0
AP(config-if)#ip default-gateway 10.0.2.1
AP(config-if)#no shutdown
AP(config-if)#exit
! Налаштування SSID
AP(config)#dot11 ssid PrintingNetwork
AP(config-ssid)#authentication open
AP(config-ssid)#authentication key-management wpa
AP(config-ssid)#wpa-psk ascii 7 Password123
AP(config-ssid)#exit
! Налаштування інтерфейсу радіо
AP(config)#interface Dot11Radio0
AP(config-if)#ssid PrintingNetwork
AP(config-if)#channel 6
AP(config-if)#encryption mode ciphers aes-ccm
AP(config-if)#exit
! Налаштування типу автентифікації та алгоритму шифрування
AP(config)#dot11 ssid PrintingNetwork
```

```
AP(config-ssid)#authentication open
AP(config-ssid)#authentication key-management wpa
AP(config-ssid)#wpa-psk ascii 7 Password123
AP(config-ssid)#exit
! Збереження конфігурації
AP(config)#end
AP#write memory
```

Лістинг 3.4 – Налаштування міжмережевого екрану ASA:
Налаштування використовує auto NAT для встановлення одностороннього перекладу адрес з внутрішньої мережі на зовнішню.

```
! Встановлення інтерфейсів
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 203.0.113.1 255.255.255.0
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
! Налаштування доступу з внутрішньої мережі на зовнішній світ
access-list inside_access_out extended permit ip any
! Налаштування NAT для внутрішніх мережевих адрес
nat (inside,outside) after-auto source dynamic any interface
! Налаштування маршрутизації
route outside 0.0.0.0 0.0.0.0 203.0.113.254
! Встановлення пароля для доступу до пристрою через SSH
aaa authentication ssh console LOCAL
username admin password MySecretPassword encrypted
ssh 192.168.1.0 255.255.255.0 outside
! Увімкнення SSH та відключення HTTP доступу до пристрою
ssh 192.168.1.0 255.255.255.0 outside
no http server enable
! Відключення відправки трафіку ICMP Unreachable повідомлень
icmp unreachable rate-limit 0 burst-size 0
! Заборона працювати з протоколом IP
no ip identd
! Відключення перевірки DNS
no dns-guard
! Включення міжмережевого екрану
no failover
! Збереження конфігурації
write memory
```

Налаштування включають IPS і визначають, які інтерфейси слід моніторити для знаходження потенційно шкідливого трафіку. Також вони включають підписи для IPS та налаштовують чутливість системи.

```
! Включення IPS та налаштування інтерфейсів
ips inline on
ips promiscuous interface outside
ips promiscuous interface inside
! Визначення внутрішньої мережі для IPS
ips promiscuous inside
! Визначення зовнішньої мережі для IPS
ips promiscuous outside
! Налаштування інтерфейсів, які слід моніторити IPS
ips interface inside
ips interface outside
! Включення підписів для IPS
ips signature-category
! Налаштування чутливості для IPS
ips inline fail-open
! Активація IPS для всього трафіку
ips promiscuous bypass-traffic
! Збереження конфігурації
write memory
```