МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Роман ОДАРЧЕНКО
“_____”_____2023 р.

КВАЛІФІКАЦІЙНА

РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВР

Тема: «Корпоративна мережа підприємства на базі обладнання Cisco»

Виконавець: _____ Іван Котеленець
(підпис)

Керівник: _____ Віталій КУРУШКІН
(підпис)

Нормоконтролер: _____ Денис БАХТІЯРОВ
(підпис)

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі» .

ЗАТВЕРДЖУЮ
Завідувач кафедри

Роман ОДАРЧЕНКО
“_____”_____2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Котеленця Івана Михайловича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Корпоративна мережа підприємства на базі обладнання Cisco»

затверджена наказом ректора від «29» березня 2023 р. № 421/ст

2. Термін виконання роботи: з 22.05.2023 р. по 25.06.2023 р.

3. Вихідні дані до роботи: аналіз принципів роботи корпоративної мережі.

4. Зміст пояснювальної записки: Принцип побудування корпоративної мережі на базі обладнання Cisco.

5. Перелік обов'язкового графічного (ілюстративного) матеріалу: слайди презентації у програмному пакеті Microsoft Power Point.

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	22.05.2023-24.05.2023	Виконано
2	Вступ	25.05.2023	Виконано
3	Функції та принципи побудови корпоративних мереж	26.05.2023-29.05.2023	Виконано
4	Комплексні системи захисту в КМ	30.05.2023-07.06.2023	Виконано
5	Проєктування корпоративної мережі малого підприємства на базі обладнання Cisco	08.06.2023-14.06.2023	Виконано
6	Усунення недоліків та захист кваліфікаційної роботи	15.06.2023-25.06.2023	

7. Дата видачі завдання: “19" травня 2023 р.

Керівник кваліфікаційної роботи _____ Віталій КУРУШКІН
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Іван КОТЕЛЕНЕЦЬ
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Тема кваліфікаційної роботи згідно з наказом» містить 70 сторінок, 6 рисунків, 16 використаних джерел.

КЛЮЧОВІ, СЛОВА, ВИКОРИСТОВУВАНІ, В ВАШІЙ, КВАЛІФІКАЦІЙНІЙ РОБОТІ.

Об’єкт дослідження – корпоративна мережа підприємства на базі обладнання Cisco.

Предмет дослідження – Корпоративна мережа авіапідприємства підприємства на базі обладнання Cisco.

Мета кваліфікаційної роботи – Проектування архітектури корпоративної мережі на основі обладнання Cisco.

Метод дослідження – Був проведений аудит мережевої інфраструктури, можлива подальша віртуалізація мережі, її моніторинг, в подальшому, за необхідності аналіз трафіку, варіації тестування безпеки мережі.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

DDoS (Distributed denial of service) – розподілена відмова в обслуговуванні.

DoS (denial of service) – відмова в обслуговуванні.

IDS (intrusion detection system) – система виявлення вторгнень.

КІС - корпоративна інформаційна система.

VPN (virtual private network) - віртуальна приватна мережа.

КМ - корпоративна мережа.

RJ-45 фізичний інтерфейс, що є одним з засобів з'єднання комп'ютерних мереж за допомогою витої пари.

OSPF - протокол маршутизації.

EIGRP - протокол маршрутизації.

NAT - це механізм у мережах TCP/IP, що дає змогу перетворювати IP-адреси транзитних пакетів.

DMZ - це сегмент мережі, який розташовується між внутрішньою мережею організації та зовнішньою мережею.

TCP/IP - мережева модель передачі даних.

QoS - технологія, яка може гарантувати пропуск у повному обсязі певного виду трафіку в заданих технологічних рамках.

LAN - бездротова мережа.

WAN - глобальна мережа.

STP - Spanning Tree Protocol усунення петель у топології довільної мережі Ethernet, у якій є один або більше мережевих мостів, пов'язаних надлишковими з'єднаннями.

ВСТУП

Актуальність теми. На сьогоднішній день нас повсюди оточують пристрої які мають вихід у глобальну мережу інтернет. Побудова корпоративної мережі на базі обладнання Cisco залишається актуальною темою для дипломної роботи. Cisco є одним з провідних виробників мережевого обладнання і має велику популярність у бізнес-середовищі.

Компанії різних розмірів та галузей використовують обладнання Cisco для побудови своїх корпоративних мереж. Отже, є потреба в експертах, які знають, як ефективно розгорнути та управляти мережами на базі Cisco.

Забезпечення безпеки мережі є надзвичайно важливим аспектом для будь-якої організації. Cisco пропонує різні інструменти та технології для захисту мережі, такі як мережеві фаєрволи, VPN, ідентифікація та контроль доступу, що робить цю тему актуальною для дослідження та розробки в рамках дипломної роботи.

Побудова мережі, яка забезпечує високу продуктивність та масштабованість, є важливим завданням для організацій. Обладнання Cisco пропонує різні технології, які допомагають досягти цих цілей, такі як мережеве вирівнювання навантаження, маршрутизація на основі політик, віртуалізація мережі та інші.

Мета і завдання дослідження. Метою дипломної роботи є розробка та побудова ефективної, безпечної та масштабованої корпоративної мережі на основі обладнання Cisco з урахуванням конкретних потреб підприємства.

Завдання, що в рамках дипломної роботи, включають:

1) Визначення вимог та потреб компанії щодо мережі, включаючи масштабність, продуктивність, безпеку, надійність та інші параметри.
2) Ознайомлення з різними моделями мережевого обладнання Cisco, їх можливостями, функціями та характеристиками.
3) Проектування архітектури корпоративної мережі на основі обладнання Cisco, включаючи розташування пристроїв, сегментацію мережі, протоколи комутації та маршрутизації, забезпечення безпеки та інші аспекти.

4) Вибір потрібного обладнання Cisco для реалізації запропонованої архітектури та його налаштування з урахуванням потреб підприємства.
5) Оформлення дипломної роботи, включаючи опис методології дослідження, аналіз результатів, рекомендації та висновки.

Об'єктом дослідження – корпоративна мережа підприємства на базі обладнання Cisco.

Предметом дослідження – Корпоративна мережа авіапідприємства підприємства на базі обладнання Cisco.

Методи досліджень. Був проведений аудит мережевої інфраструктури, можлива подальша віртуалізація мережі, її моніторинг, в подальшому, за необхідності аналіз трафіку, варіації тестування безпеки мережі.

Практичне значення отриманих результатів.

У процесі виконання буде складено та розроблено структурну схему, фізичну й логічну топологію, схему з'єднань й IP - адресації цієї мережі. Також було здійснено конфігурування пристроїв та моделювання роботи мережі у середовищі Cisco Packet Tracer.

Апробація отриманих результатів. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

- Науково-практична конференція «Проблеми експлуатації та захисту інформаційно-комунікаційних систем», м. Київ, 2023 р.

РОЗДІЛ 1
ФУНКЦІЇ ТА ПРИНЦИПИ ПОБУДОВИ КОРПОРАТИВНИХ МЕРЕЖ

1.1. Основні можливості КМ

Корпоративна мережа (КМ) - це інформаційна система, яка дозволяє компаніям об'єднувати свої ресурси і спільно використовувати їх. Основні можливості КМ включають [1]:

Підтримку спільної роботи: дозволяє співробітникам працювати над спільними проєктами, обмінюватися документами та координувати свої дії.

Покращення ефективності роботи: забезпечити доступ до потрібної інформації та інструментів швидше та з більшою точністю, що може покращити продуктивність роботи.

Забезпечення безпеки: КМ може забезпечити захист конфіденційної інформації та контроль доступу до різних ресурсів.

Зменшення витрат: КМ може допомогти скоротити витрати на IT-інфраструктуру та інформаційні послуги за рахунок спільного використання ресурсів.

Інфраструктура та обладнання: за допомогою корпоративних мереж можна спільно використовувати фізичне обладнання, таке як сервери, комутатори, маршрутизатори та сховища даних. Замість купівлі окремих пристроїв для кожного відділу або проєкту, організація може сконцентрувати ресурси та забезпечити їх ефективне використання, що дозволяє знизити витрати на закупівлю та підтримку обладнання.

Програмне забезпечення та ліцензії: корпоративні мережі дозволяють спільно використовувати програмне забезпечення та ліцензії, забезпечуючи доступ до них для багатьох користувачів у межах організації. Це може включати операційні системи, офісні пакети, бази даних та інші програми. В результаті, організація може скоротити витрати на придбання та оновлення ліцензійного програмного забезпечення.

Адміністрування та підтримка: у корпоративних мережах може бути централізоване адміністрування та підтримка, що дозволяє знизити витрати на обслуговування мережі. Замість наявності окремого адміністратора для кожного відділу або мережевого пристрою, можна мати команду фахівців, які відповідають за централізоване управління та підтримку, що ефективно використовує ресурси та зменшує витрати.

Управління мережевим обладнанням: адміністратори мережі відповідають за конфігурацію, моніторинг та підтримку мережевого обладнання, такого як комутатори, маршрутизатори, мережеві фаєрволи тощо. Вони забезпечують належне функціонування обладнання, відповідають за оновлення програмного забезпечення, встановлюють правила безпеки та моніторять роботу мережі для виявлення проблем.

Налаштування мережевої безпеки: адміністратори мережі встановлюють та налаштовують механізми безпеки, такі як фаєрволи, системи виявлення вторгнень, системи захисту від вірусів тощо. Вони розробляють політики безпеки, контролюють доступ користувачів до мережі та ресурсів, а також вчасно виявляють та врегульовують можливі загрози.

Моніторинг та аналіз мережевої активності: адміністратори мережі використовують спеціальні інструменти для моніторингу мережевої активності та аналізу її ефективності. Вони виявляють аномальну активність, проблеми з пропускною здатністю, перевантаженням мережі тощо, та вживають заходів для їх врегулювання.

Підтримка користувачів та вирішення проблем: адміністратори мережі надають підтримку користувачам, відповідають на їх запити щодо налаштування мережевих підключень, відновлення паролів, розв'язання проблем з доступом до ресурсів мережі та інші питання.

IT-послуги та додаткові ресурси: корпоративна мережа може забезпечити спільний доступ до IT-послуг, таких як електронна пошта, спільні сховища даних, інструменти спільної роботи та інші ресурси. Це дозволяє уникнути дублювання послуг для кожного відділу окремо, що призводить до зниження витрат на підтримку та обслуговування інформаційних послуг.

1.2. Переваги корпоративних мереж

Переваги корпоративних мереж включають [2] можливість централізованого дистанційного навчання; скорочення витрат на експлуатацію мереж та підвищення цінності інвестицій в мережеву інфраструктуру; прозорість роботи компанії, контроль над корпоративними мережевими ресурсами; повний контроль за діяльністю всіх служб та структурних підрозділів; автономність мережі та високий рівень безпеки; безперервне оновлення інформації між співробітниками підприємства дозволить приймати їм своєчасні та правильні рішення; гнучкість корпоративної мережі на внутрішні та зовнішні зміни в середині компанії; доступ до всіх інформаційних ресурсів підприємства в реальному часі, незалежно від місця знаходження співробітників: в офісі, в іншому місті, дома або в дорозі.

Забезпечення спільного доступу до ресурсів: корпоративні мережі дозволяють спільний доступ до файлів, даних та ресурсів всередині організації. Це сприяє поліпшенню комунікації та співпраці між співробітниками, що покращує продуктивність.

Централізоване управління: корпоративні мережі дозволяють централізовано керувати інфраструктурою, безпекою та налаштуваннями мережі. Це спрощує адміністрування та забезпечує однорідність налаштувань в усій організації

Централізована конфігурація та керування: За допомогою централізованого управління, адміністратори мережі можуть налаштовувати та керувати всіма компонентами мережі, такими як комутатори, маршрутизатори, бездротові точки доступу тощо, з одного центрального пункту. Це спрощує процес конфігурації та забезпечує єдиноформованість налаштувань усієї мережі.

Моніторинг та аналітика: централізоване управління дозволяє здійснювати моніторинг мережі та збирати дані про її роботу з різних джерел. Адміністратори можуть аналізувати ці дані для виявлення проблем, моніторингу пропускної здатності, виявлення аномальних активностей тощо. Це дозволяє вжити вчасних заходів для вирішення проблем та оптимізації роботи мережі.

Централізована безпека: централізоване управління також дозволяє забезпечувати централізований контроль доступу до мережі та ресурсів. Адміністратори можуть встановлювати політики безпеки та авторизації, керувати правами доступу користувачів та виявляти потенційні загрози або аномальну активність.

Централізоване управління резервними копіями та відновленням: За допомогою централізованого управління, адміністратори можуть розпочати та керувати процесом резервного копіювання даних, а також відновлення мережевих компонентів в разі неполадок або відновлення після аварійних ситуацій. Це допомагає забезпечити безпеку та надійність даних у разі втрати або пошкодження.

Підвищена безпека даних: корпоративні мережі дозволяють встановлювати централізовані політики безпеки, включно з автентифікацію, шифрування та контроль доступу. Це забезпечує захист важливих даних організації від несанкціонованого доступу.

Автентифікація та авторизація: корпоративні мережі забезпечують механізми аутентифікації, щоб перевірити, чи має користувач право доступу до системи, а також авторизацію, щоб визначити, які ресурси він може використовувати. Це дозволяє контролювати доступ до конфіденційної інформації та запобігати несанкціонованому доступу.

Шифрування даних: використовувати шифрування для захисту конфіденційної інформації, що передається по мережі. Шифрування забезпечує захист даних від перехоплення та незаконного доступу.

Фаєрволи та інтрузивні системи виявлення: корпоративні мережі можуть мати фаєрволи та системи виявлення вторгнень, що дозволяють виявляти та блокувати небажані мережеві активності. Це допомагає запобігати атакам зовнішніх загроз і захищати мережу від несанкціонованого доступу.

Захист від шкідливих програм: корпоративні мережі можуть використовувати антивірусне програмне забезпечення та інші механізми для виявлення та блокування шкідливих програм. Це допомагає запобігати інфікуванню систем і поширенню вірусів у мережі.

Резервне копіювання та відновлення даних: корпоративні мережі можуть мати механізми резервного копіювання та відновлення даних, що дозволяють відновити важливу інформацію в разі її втрати або пошкодження. Це допомагає забезпечити безпеку та цілісність даних в мережі.

Для підтвердження цих переваг та підвищення авторитету вашої роботи, ви можете посилатися на наукові статті, дослідження та стандарти безпеки мереж, такі як стандарти ISO/IEC 27001, NIST SP 800-53, або публікації від провідних виробників безпеки мереж, таких як Cisco, Palo Alto Networks, або F5 BigIP, FortiNet, Symantec.

Масштабованість: корпоративні мережі можуть бути розширені та масштабовані для врахування зростання організації. Це дозволяє легко додавати нові вузли, розширювати пропускну здатність та підтримувати зростаючі потреби мережі.

Додавання нових вузлів: корпоративні мережі можуть бути легко розширені шляхом додавання нових вузлів та пристроїв. Адміністратори мережі можуть встановлювати нове мережеве обладнання та налаштовувати його для включення до існуючої інфраструктури. Це дозволяє організації швидко реагувати на змінні потреби та забезпечити доступ до мережі для нових пристроїв та користувачів.

Розширення пропускної здатності: з ростом організації можуть збільшуватися вимоги до пропускної здатності мережі. Корпоративні мережі можуть бути масштабовані шляхом додавання нових мережевих пристроїв з вищою пропускною здатністю, встановлення більш швидкодіючих комутаторів або розширення каналів зв'язку. Це дозволяє підтримувати високу швидкість передачі даних та задовольняти зростаючі потреби користувачів.

Горизонтальна та вертикальна масштабованість: корпоративні мережі можуть бути масштабовані горизонтально та вертикально. Горизонтальна масштабованість передбачає розширення мережі шляхом додавання нових фізичних ресурсів, таких як комутатори або маршрутизатори, для розподілу навантаження та забезпечення більшої пропускної здатності. Вертикальна масштабованість передбачає підвищення продуктивності та масштабованості шляхом удосконалення наявних ресурсів, таких як оптимізація мережевих протоколів або використання високопродуктивних пристроїв.

Використання віртуалізації: віртуалізація є ще одним аспектом масштабованості в корпоративних мережах. Вона дозволяє логічно розділяти фізичну мережу на віртуальні сегменти, що дозволяє ефективніше використовувати ресурси, забезпечувати безпеку та контроль над доступом, а також здійснювати швидку настройку та розгортання нових мережевих сервісів.

Віртуальні приватні мережі (Virtual Private Networks, VPN): використання VPN дозволяє створювати зашифровані тунелі між різними мережами або віддаленими користувачами через публічну мережу, таку як Інтернет. Це забезпечує безпеку передачі даних та дозволяє забезпечити конфіденційність інформації, незалежно від фізичного розташування користувачів.

Віртуальні локальні мережі (Virtual Local Area Networks, VLAN): використання VLAN дозволяє фізично розділити мережу на логічні сегменти, незалежно від фізичної структури мережі. Це дозволяє групувати користувачів або пристрої в одну віртуальну мережу, незалежно від їх фізичного розташування. Віртуалізація VLAN спрощує управління трафіком, забезпечує більшу безпеку та контроль над доступом до ресурсів.

Віртуалізація мережевих функцій (Network Function Virtualization, NFV): використання NFV дозволяє відокремити мережеві функції від фізичних пристроїв та розмістити їх у віртуальному середовищі. Це дозволяє гнучко керувати та масштабувати функції мережі, знижує витрати на обладнання та спрощує управління мережевими сервісами.

Зменшення витрат: за допомогою корпоративних мереж можна досягти економії за рахунок спільного використання ресурсів, централізованого управління та оптимізації мережевої інфраструктури.

Забезпечення централізованого резервного копіювання даних: Корпоративні мережі дозволяють здійснювати резервне копіювання цінних даних на центральних серверах або мережевих сховищах. Це допомагає запобігти втраті даних в разі непередбачених ситуацій, таких як віруси, помилкові видалення або технічні збої.

Централізоване зберігання: у корпоративній мережі дані можуть бути централізовано збережені на серверах або зберігальних пристроях. Це дозволяє

зберігати всі важливі дані в одному місці, що спрощує їх управління та резервне копіювання.

Автоматизоване резервне копіювання: централізована система резервного копіювання даних може бути налаштована для автоматичного копіювання важливих даних з різних джерел. Це включає файли, бази даних, електронну пошту та інші цифрові ресурси. Автоматизація спрощує процес резервного копіювання та забезпечує його регулярність та надійність.

Ієрархічне зберігання: централізована система резервного копіювання може використовувати ієрархічну структуру зберігання, де копії даних зберігаються на різних рівнях. Це включає локальні копії для швидкого відновлення та зовнішні пристрої для довготривалого зберігання. Ієрархічне зберігання дозволяє ефективно використовувати ресурси та забезпечує надійність резервного копіювання.

Централізований доступ до резервних копій: забезпечення централізованого доступу до резервних копій даних є важливим аспектом управління резервними копіями. Відповідні права доступу можуть надаватися відповідним користувачам або адміністраторам для відновлення втрачених або пошкоджених даних.

Забезпечення мобільності співробітників: корпоративні мережі можуть підтримувати мобільні пристрої, що дозволяє співробітникам отримувати доступ до корпоративних ресурсів незалежно від їх місця знаходження. Це підвищує продуктивність та ефективність роботи команд, які працюють на віддаленій основі.

Підвищення надійності та доступності: корпоративні мережі можуть бути сконфігуровані з резервуванням, розділенням навантаження та іншими механізмами, що забезпечують надійність і неперервність роботи. Це зменшує ризик виникнення відмов та забезпечує стабільну доступність до ресурсів.

Покращення комунікації: корпоративні мережі дозволяють використовувати електронну пошту, відеоконференції, чати та інші засоби комунікації для ефективного обміну інформацією всередині організації. Це сприяє швидкому та зручному обміну ідей та спільному прийняттю рішень.

Підтримка централізованої системи управління користувачами: Корпоративні мережі дозволяють централізовано керувати правами користувачів, автентифікацією та авторизацією. Це спрощує процеси управління користувачами та забезпечує безпеку даних всередині мережі.

1.3 Концепція корпоративної мережі

Основи концепції корпоративної мережі [3]:

Централізоване управління: корпоративна мережа зазвичай має централізовану систему управління, яка контролює всю мережеву інфраструктуру. Це дозволяє адміністраторам керувати мережевими ресурсами, налаштовувати політики безпеки та контролювати доступ користувачів до різних ресурсів.

Централізоване керування мережевими пристроями: включає централізоване налаштування, моніторинг та керування роутерами, комутаторами, файрволами та іншими мережевими пристроями. Адміністратори можуть віддалено керувати цими пристроями, встановлювати правила маршрутизації, налаштовувати безпеку та контролювати трафік.

Централізована автентифікація та авторизація: у корпоративних мережах використовуються централізовані системи аутентифікації, такі як сервери директорії(ActiveDirectory) або RADIUS-сервери та LDAP, для перевірки ідентифікації користувачів та надання прав доступу до ресурсів. Це дозволяє забезпечити єдиний точки входу для користувачів та централізоване керування їх доступом.

Централізоване керування політиками безпеки: має централізовану систему керування політиками безпеки, де визначаються правила та політики безпеки для всіх мережевих пристроїв. Це дозволяє одночасно встановлювати та оновлювати політики безпеки в усіх точках мережі, забезпечуючи єдиноформний рівень безпеки.

Моніторинг та аналіз мережевої діяльності: централізована система управління може включати моніторинг та аналіз мережевої діяльності для виявлення проблем,

відстеження трафіку, виявлення загроз безпеці та вирішення проблем мережі. Адміністратори можуть отримувати повідомлення про події, моніторити пропускну здатність та ефективність мережі та приймати відповідні заходи.

Централізоване управління оновленнями та конфігураціями: може спрощувати процеси оновлення програмного забезпечення та конфігурацій мережевих пристроїв. Адміністратори можуть виконувати оновлення централізовано, уникати несумісності версій та забезпечувати єдиноформність налаштувань.

Розподілені мережеві сегменти: корпоративна мережа може бути розбита на логічні сегменти або підмережі, які відповідають різним відділам, підрозділам або фізичним розташуванням користувачів. Це дозволяє забезпечити ефективну організацію мережі, керування трафіком та забезпечення безпеки.

Забезпечення безпеки: корпоративна мережа має високі вимоги до безпеки, оскільки вона містить конфіденційну інформацію та доступ до різних ресурсів організації. Захист мережі зазвичай здійснюється за допомогою мережевих протоколів, файрволів, систем ідентифікації та автентифікації, систем виявлення вторгнень та інших засобів.

Висока доступність: корпоративна мережа повинна бути з високодоступною, щоб забезпечити безперервну роботу організації. Це може бути досягнуто за допомогою резервування мережевих компонентів, дублювання серверів та налаштування мережевої інфраструктури з урахуванням масштабованості та відмовостійкості.

Інтеграція з іншими системами: корпоративна мережа повинна бути здатна інтегруватися з іншими системами організації, такими як системи управління базами даних, електронною поштою, коллаборації та іншими. Інтеграція дозволяє ефективно обмінюватися даними та забезпечує спільну роботу користувачів.

Масштабованість: корпоративна мережа повинна бути здатна масштабуватися для врахування зростання організації. Це може включати додавання нових вузлів, розширення пропускної здатності та підтримку зростаючих потреб мережі.

Фізична масштабованість: корпоративна мережа повинна бути гнучкою і здатною розширюватися фізично. Це означає, що мережа повинна підтримувати

додавання нових вузлів, мережевих пристроїв і сегментів без значних змін в існуючій інфраструктурі. Фізична масштабованість може бути досягнута за допомогою використання гнучких топологій мережі, масштабованих комутаторів та маршрутизаторів, а також забезпечення достатньої пропускної здатності і підтримки резервування мережевих з'єднань.

Логічна масштабованість: корпоративна мережа повинна бути здатною розширюватися логічно, що означає, що вона може підтримувати зростання обсягу даних, кількості користувачів та додатків, які працюють у мережі. Логічна масштабованість може бути досягнута шляхом використання масштабованих мережевих протоколів, таких як OSPF, RIP, EIGRP, IS-IS або BGP, розподілення навантаження між серверами та використання віртуалізації для ефективного використання ресурсів.

Управління масштабованістю: корпоративна мережа повинна мати засоби управління масштабованістю, які дозволяють адміністраторам легко керувати і моніторити розширення мережі. Це включає автоматизацію процесів розгортання нових вузлів, моніторинг пропускної здатності та виявлення аномалій, а також можливості прогнозування потреб у мережевих ресурсах і планування розширення.

Обробка зростаючого трафіку: зростаюча кількість користувачів, додатків і обсягів даних вимагає мережевої інфраструктури, яка може ефективно обробляти цей зростаючий трафік.

Масштабованість корпоративної мережі повинна включати забезпечення достатньої пропускної здатності, використання швидких комутаторів і маршрутизаторів, а також оптимізацію трафіку для покращення продуктивності мережі.

1.4. Призначення корпоративної мережі

Корпоративна мережа - система, що забезпечує передачу інформації між різними додатками, які у системі корпорації. Корпоративна мережа є мережа окремої

організації. Корпоративною мережею вважається будь-яка мережа, що працює за протоколом TCP/IP і використовує комунікаційні стандарти Інтернету, і навіть сервісні програми, які забезпечують доставку даних користувачам мережі. Наприклад, підприємство може створити сервер Web для публікації оголошень, виробничих графіків та інших службових документів. Службовці здійснюють доступ до документів за допомогою засобів перегляду Web.

Сервери Web корпоративної мережі можуть забезпечити користувачам послуги, аналогічні послугам Інтернету, наприклад роботу з гіпертекстовими сторінками (що містять текст, гіперпосилання, графічні зображення та звукозаписи), надання необхідних ресурсів на запит клієнтів Web, а також здійснення доступу до баз даних. У цьому посібнику всі служби публікації називаються службами Інтернету незалежно від того, де вони використовуються (в Інтернеті або корпоративній мережі).

Корпоративна мережу, зазвичай, є територіально розподіленої [4], тобто, об'єднує офіси, підрозділи та інші структури, що знаходяться на значній відстані один від одного. Принципи, якими будується корпоративна мережу, досить сильно від тих, що використовуються під час створення локальної мережі. Це обмеження є принциповим, і при проектуванні корпоративної мережі слід вживати всіх заходів для мінімізації обсягів даних, що передаються. В іншому ж корпоративна мережа не повинна вносити обмежень на те, які саме додатки і яким чином обробляють інформацію, що переноситься по ній.

Можна виділити основні етапи процесу створення корпоративної інформаційної системи:

Провести інформаційне обстеження організації;

За результатами обстеження вибрати архітектуру системи та апаратно-програмні засоби її реалізації. за результатами обстеження вибрати та/або розробити ключові компоненти інформаційної системи;

Система управління корпоративною базою даних;

Система автоматизації ділових операцій та документообігу;

Система управління електронними документами;

Спеціальні програмні засоби;

Системи підтримки прийняття рішень.

1.5. Процес створення корпоративної інформаційної системи

Ось загальна схема процесу створення КІС [5]:

Аналіз вимог - на цьому етапі визначаються потреби організації і вимоги до КІС. Проводиться дослідження бізнес-процесів, ідентифікація потенційних проблем та визначення функціональності, яка необхідна для оптимального функціонування системи.

Проектування системи - на основі аналізу вимог розробляється архітектура КІС. Визначаються компоненти системи, їх взаємозв'язки та логічна структура. Розробляються плани мережі, серверів, баз даних та інших необхідних компонентів.

Розробка програмного забезпечення - на цьому етапі розробляються програми та додатки, необхідні для роботи КІС. Програми можуть бути розроблені внутрішніми розробниками або залучені зовнішні партнери. Під час розробки необхідно дотримуватись вимог безпеки та ефективності.

Впровадження та тестування, розроблену КІС впроваджують в організацію. Виконується установка та налаштування обладнання, програмного забезпечення та мережі. Проводяться тестування системи на відповідність вимогам та виявлення можливих проблем.

Навчання та підтримка користувачів: після впровадження КІС проводиться навчання користувачів щодо роботи з системою. Забезпечується підтримка та технічна допомога користувачам у разі виникнення проблем або питань.

Моніторинг та підтримка: КІС підлягає постійному моніторингу та підтримці. Здійснюється контроль над роботою системи, виявлення та усунення можливих проблем, оновлення та поновлення компонентів системи.

1.6. Віртуальні мережі передачі даних

VPN дозволяє працівникам отримувати безпечний віддалений доступ до корпоративних ресурсів з будь-якого місця. Це особливо корисно для працівників, які працюють з віддалених офісів, відділень або з дому. Вони можуть підключатися до корпоративної мережі через захищений тунель і отримувати доступ до файлів, додатків, баз даних та інших ресурсів.

Особливості VPN [6]:

1) VPN забезпечує захищену передачу даних шляхом шифрування інформації, що передається по мережі. Це унеможливлює перехоплення і читання даних третіми особами. Крім того, VPN може забезпечити автентифікацію, тобто перевірку ідентифікації користувачів, що підключаються до мережі.

2) З'єднання філій та відділень за допомогою VPN може бути використаний для з'єднання різних філій та відділень організації в єдину корпоративну мережу .

Це дозволяє спільно використовувати ресурси, обмінюватись даними та забезпечувати безпеку комунікацій між різними розподіленими локаціями.

3) Забезпечення контролю використання VPN дозволяє організаціям забезпечувати контроль над комунікаціями в мережі. Вони можуть встановлювати правила доступу, фільтрувати трафік і контролювати використання ресурсів для забезпечення безпеки та оптимального функціонування мережі.

У корпоративних мережах VPN можуть бути реалізовані за допомогою різних протоколів, таких як IPsec, SSL/TLS, L2TP та інші. Організації можуть встановлювати власні VPN-сервери або використовувати послуги VPN-провайдерів для створення і керування віртуальними мережами передачі даних у своїй корпоративній інфраструктурі.

1.7. Технології, що використовуються в корпоративних мережах

Ethernet є найпоширенішою технологією передачі даних в локальних мережах (LAN). Вона використовує кабельну інфраструктуру для передачі пакетів даних між пристроями.

Wi-Fi технологія дозволяє бездротове підключення до мережі. Вона використовує радіохвильові сигнали для передачі даних між пристроями і точками доступу.

VLAN (Virtual Local Area Network) - VLAN дозволяє створювати віртуальні локальні мережі в межах фізичної мережі. Вона дозволяє групувати пристрої відповідно до функціональних або відділових потреб, забезпечуючи безпеку та ефективність.

VPN (Virtual Private Network) - VPN технологія дозволяє створювати безпечні тунелі для передачі даних через незахищені мережі, такі як Інтернет. Вона шифрує дані та забезпечує приватність комунікацій.

Файрвол є системою безпеки, що контролює трафік, що проходить через мережу. Вона фільтрує небажаний трафік і захищає мережу від несанкціонованого доступу та зовнішніх загроз.

Routing використовується для визначення оптимального шляху передачі даних між різними мережевими сегментами. Роутери виконують функцію маршрутизації і вибирають найкоротший шлях для передачі пакетів даних.

DHCP (Dynamic Host Configuration Protocol): DHCP дозволяє автоматичну настройку IP-адрес та параметрів мережевого підключення для пристроїв в мережі. Вона спрощує процес налаштування та управління IP-адресами.

Active Directory - централізоване управління ідентифікацією: Active Directory дозволяє створювати та керувати обліковими записами користувачів, групами та іншими об'єктами. Це спрощує процес управління доступом користувачів до різних ресурсів в мережі.

Аутентифікація та авторизація - Active Directory забезпечує механізми аутентифікації та авторизації користувачів. Вона перевіряє правильність облікових

записів користувачів та надає доступ до відповідних ресурсів згідно з встановленими політиками безпеки.

Управління політиками безпеки Active Directory дозволяє встановлювати політики безпеки на рівні мережі. Це включає встановлення складних паролів, обмеження доступу до ресурсів, застосування шифрування та інші механізми для забезпечення безпеки мережі.

Розподілене зберігання даних: Active Directory використовує розподілену базу даних для зберігання інформації про користувачів, групи, комп'ютери та інші об'єкти. Це дозволяє швидкий доступ до даних та резервне копіювання для забезпечення надійності.

Інтеграція з іншими службами Microsoft: Active Directory інтегрується з іншими продуктами та сервісами Microsoft, такими як Microsoft Exchange Server, Microsoft SharePoint, Microsoft Azure і багатьма іншими. Це забезпечує єдино цінну точку управління та спрощує інтеграцію цих рішень у корпоративній мережі.

Active Directory є ключовим компонентом багатьох корпоративних мереж, особливо в середовищах, які використовують рішення Microsoft. Вона забезпечує централізоване управління та забезпечує безпеку та доступність ресурсів в мережі.

1.8. Способи побудови локальної мережі підприємства

Комп'ютерна мережа – це складний комплекс взаємозв'язаних і функціонально узгоджених програмних і апаратних компонентів.

Комп'ютерну мережу можна представити багатошаровою моделлю, що складається яка складається з наступних компонентів: комп'ютери, комунікаційне устаткування, операційні системи, мережеві додатки.

Основою будь-якої локальної мережі є ПК, які підключаються до мережі за допомогою мережевої карти. Всі комп'ютери локальних мереж можна розділити на два класи: сервери і робочі станції.

Комунікаційне устаткування. Мережевий адаптер – це спеціальний пристрій, який призначений для сполучення комп'ютера з локальною мережею і для організації двонаправленого обміну даними в мережі. Мережева карта вставляється у вільний слот розширення на материнській платі і обладнана власним процесором і пам'яттю, а для підключення до мережі має роз'єм типа RJ-45. Найбільш поширені карти типу PCI, які вставляються в слот розширення PCI на материнській платі. Залежно від вживаної технології Ethernet, Fast Ethernet або Gigabit Ethernet і мережевої карти швидкість передачі даних в мережі може бути: 10, 100 або 1000 Мбіт/с.

Як кабелі для з’єднання окремих ПК і комунікаційного устаткування в локальних мережах застосовуються [8]:

1. Вита пара – передавальна лінія зв'язку у вигляді двох проводів, перекручених один з одним з певним кроком з метою зниження впливу електромагнітних полів.

2. Коаксіальний кабель – кабель, який складається з одного центрального провідника в ізоляторі і другого провідника розташованого поверх ізолятора.

3. Оптичний кабель – це кабель, в якому носієм інформації є світловий промінь, що поширюється по оптичному волокну.

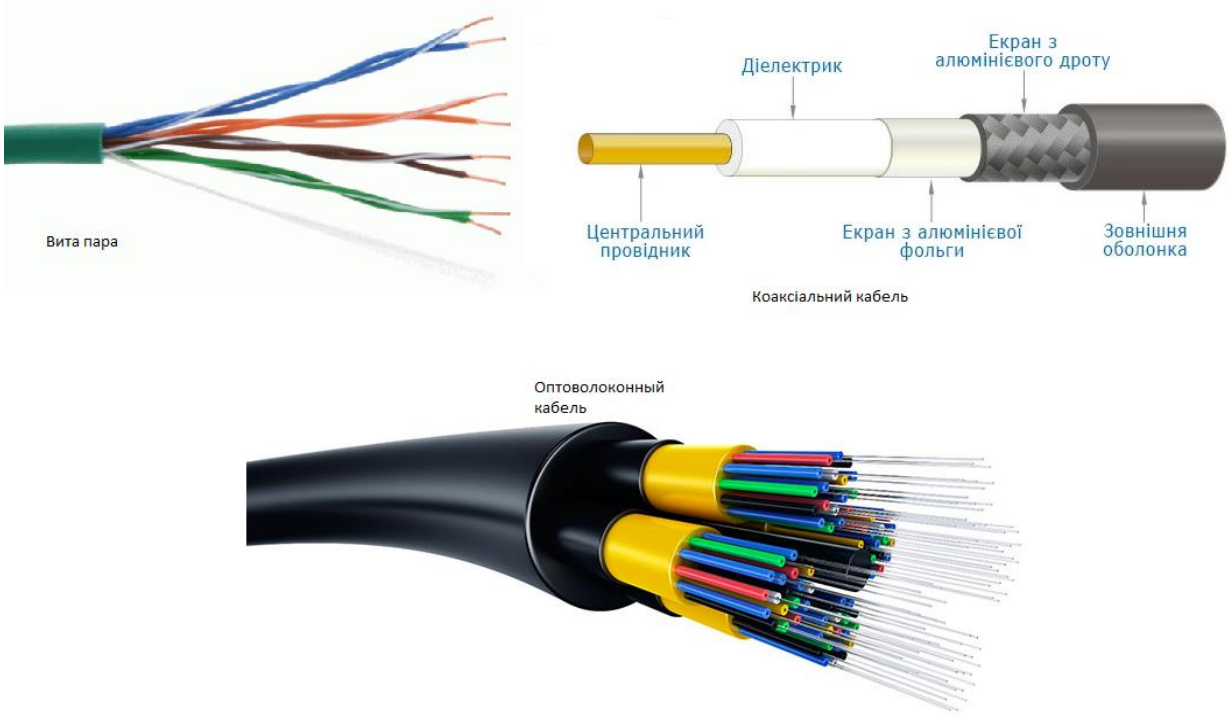

Рис.1.1 Види кабелів під’єднання до мережі

Крім того, як передавальне середовище в безпровідних локальних мережах використовуються радіохвилі в мікрохвильовому діапазоні.

До комунікаційного устаткування локальних мереж відносяться: трансивери, повторювачі, концентратори, мости, комутатори, маршрутизатори і шлюзи.

Частина устаткування (приймачі або трансивери, повторювачі або репітери і концентратори або hubs) служить для об'єднання декількох комп'ютерів в необхідну конфігурацію мережі. Сполучені з концентратором ПК утворюють один сегмент локальної мережі, тобто концентратори є засобом фізичної структуризації мережі, оскільки, розбиваючи мережу на сегменти, спрощують підключення до мережі великої кількості ПК.

Інша частина устаткування (мости, комутатори) призначені для логічної структуризації мережі. Оскільки локальні мережі є широкомовними (Ethernet і Token Ring), то із збільшенням кількості комп'ютерів в мережі, побудованій на основі концентраторів, збільшується час затримки доступу комп'ютерів до мережі і виникнення колізій. Тому в мережах побудованих на хабах встановлюють мости або комутатори між кожними трьома або чотирма концентраторами, тобто здійснюють логічну структуризацію мережі з метою недопущення колізій.

Третя частина устаткування призначена для об'єднання декількох локальних мереж в єдину мережу: маршрутизатори (routers), шлюзи (gateways). До цієї частини устаткування можна віднести і мости (bridges), а також комутатори (switches).

Повторювачі (repeater) – пристрої для відновлення і посилення сигналів в мережі з метою збільшення її довжини.

Приймачі (трансивери) – це пристрої, призначені для прийому пакетів від контроллера робочих станцій мережі і передачі їх в мережу. Трансивери (конвертори) можуть перетворювати електричні сигнали в інші види сигналів (оптичні або радіосигнали) з метою використання інших середовищ передачі інформації.

Концентратори або хабы (Hub) – пристрої множинного доступу, які об'єднують в одній точці окремі фізичні відрізки кабелю, утворюють загальне середовище

передачі даних або сегменти мережі, тобто хаби використовуються для створення сегментів і є засобом фізичної структуризації мережі.

Мости (bridges) – це програмно апаратні пристрої, які забезпечують з'єднання декількох локальних мереж між собою. Мости призначені для логічної структуризації мережі або для з'єднання в основному ідентичних мереж, що мають деякі фізичні відмінності.

Комутатори (switches) - програмно – апаратні пристрої є швидкодіючим аналогом мостів, які ділять загальне середовище передачі даних на логічні сегменти. Логічний сегмент утворюється шляхом об'єднання декількох фізичних сегментів за допомогою одного або декількох концентраторів. Кожен логічний сегмент підключається до окремого порту комутатора. Під час передачі даних з комп'ютера - відправника на який-небудь з портів комутатор передасть ці дані, але не на всі порти, як в концентраторі, а лише на той порт, до якого підключений сегмент, що містить комп'ютер, - одержувач даних.

Маршрутизатори (routers). Ці пристрої забезпечують вибір маршруту передачі даних між декількома мережами, що мають різну архітектуру або протоколи. Вони забезпечують складний рівень сервісу, оскільки можуть виконувати “інтелектуальні” функції: вибір найкращого маршруту для передачі повідомлення, адресованого іншій мережі; захист даних; буферизацію даних; різні протокольні перетворення. Маршрутизатори застосовують лише для зв'язку однорідних мереж.

Шлюзи (gateway) – пристрої (комп'ютер), що служать для об'єднання різнорідних мереж з різними протоколами обміну. Шлюзи виконують протокольне перетворення для мережі, зокрема перетворення повідомлення з одного формату в інший.

Ефективність функціонування ЛОМ визначається параметрами, вибраними при конфігурації мережі. Конфігурація мережі базується на існуючих технологіях і світовому досвіді, а також на прийнятих у всьому світі стандартах побудови ЛОМ і визначається вимогами, що пред'являються до неї, а також фінансовими можливостями організацій.

Виходячи з існуючих умов і вимог, у кожному окремому випадку вибирається топологія мережі, кабельна структура, комунікаційне устаткування, протоколи і методи передачі даних, способи організації взаємодії пристроїв, мережева операційна система.

Програмне забезпечення локальних мереж. До програмних компонентів мереж відносяться: операційні системи і мережеві додатки або мережеві служби. Мережева операційна система – це основа будь-якої обчислювальної мережі.

Мережева операційна система необхідна для управління потоками повідомлень між робочими станціями і серверами. Вона може дозволити будь-якій робочій станції працювати з мережевим розділеним диском або принтером, які фізично не підключені до цієї станції.

У мережевій операційній системі окремого комп'ютера можна виділити декілька частин.

Засоби управління локальними ресурсами комп'ютера, до яких відносяться: функції розподілу оперативної пам'яті між процесами, планування і диспетчеризації процесів, управління процесорами в мультипроцесорних машинах, управління периферійними пристроями і інші функції управління ресурсами локальних ОС.

Засоби надання власних ресурсів і послуг в загальне користування – серверна частина ОС (сервер). Ці засоби забезпечують, наприклад, блокування файлів і записів, необхідних для їх спільного використання; ведення довідників імен мережевих ресурсів; обробку запитів віддаленого доступу до власної файлової системи і бази даних; управління чергами запитів віддалених користувачів до своїх периферійних пристроїв.

Засоби запиту доступу до віддалених ресурсів і послуг і їх використання – клієнтська частина ОС. Ця частина виконує розпізнавання і перенаправлення в мережу запитів до віддалених ресурсів від додатків і користувачів, при цьому запит поступає від додатку в локальній формі, а передається в мережу в іншій формі, відповідно вимогам сервера. Клієнтська частина також здійснює прийом відповідей від серверів і перетворення їх в локальний формат, так що для додатку виконання локальних і віддалених запитів не розрізняється.

Комунікаційні засоби ОС, за допомогою яких відбувається обмін повідомленнями в мережі. Ця частина забезпечує адресацію і буферизацію повідомлень, вибір маршруту передачі повідомлення по мережі, надійність передачі і тому подібне, тобто є засобом транспортування повідомлень.

Залежно від функцій, що покладаються на конкретний комп'ютер, в його операційній системі може бути відсутнім або клієнтська, або серверна частині.

Мережеві операційні системи UNIX. UNIX є дуже потужною, гнучкою і динамічною операційною системою, яка в змозі обробляти практично будь-яке запропоноване користувачем завдання. Має широкий набір засобів, за допомогою яких можна вирішити більшість проблем, що виникають при роботі з інформаційними технологіями. До переваг UNIX відносяться потужність роботи, стабільність і надійність, повна автоматизація, а також підтримка безлічі мов програмування.

Ця операційна система має оптимальні рішення для роботи з Internet, включаючи доступ до ресурсів Web, Telnet, FTP, базам даних і тому подібне Оскільки система UNIX створювалася спеціально для обробки великих масивів даних і повної інтеграції з мережевим середовищем, вона майже завжди перевершує по швидкодії будь-яку іншу комбінацію апаратного і програмного забезпечення. Linux є версією UNIX, адаптованою для процесорів Intel.

ОС NetWare фірми Novell. Novell була однією з перших компаній, які почали створювати ЛОМ. Як файловий сервер в NetWare може використовуватися звичайний ПК, мережева ОС якого здійснює управління роботою ЛОМ. Функції управління включають координацію робочих станцій і регулювання процесу розділення файлів і принтера в ЛОМ. Мережеві файли всіх робочих станцій зберігаються на жорсткому диску файлового сервера, а не на дисках робочих станцій.

Мережеві ОС фірми Microsoft. Спочатку Windows NT існувала в двох версіях: Windows NT Advanced Server встановлювалася на серверах мережі NT, а Windows NT Workstation була потужною настільною операційною системою з функціональними можливостями.

Наступна версія Windows NT, призначена для використання на серверах, була перейменована в Windows NT Server. Висока продуктивність і покращена підтримка додатків зробили її однієї з найпопулярніших операційних систем.

Windows NT 4.0 об'єднувала в собі покращену інтеграцію з Internet і корпоративними мережами, підвищену продуктивність, відмінну сумісність з іншими операційними системами компанії Microsoft.

Сімейство програмних продуктів Windows 2022 Server – є наступним поколінням серії операційних систем Windows NT Server, в якому надійні, зручні для роботи в інтернеті служби каталога, мережеві служби і служби додатків, об'єднані з потужним комплексним управлінням.

Windows Server 2022 — це операційна система нового покоління. Вона призначена для забезпечення користувачів найбільш продуктивною платформою, що дозволяє розширити функціональність додатків, мереж і веб-служб, від робочих груп до центрів даних.

При спільному використанні клієнтських комп'ютерів Windows і серверів під Windows Server 2022 значно підвищується продуктивність, надійність мережі.

Глобальні мережі з комутацією каналів і пакетів. Глобальні мережі Wide Area Networks (WAN), які відносяться до територіальних комп'ютерних мереж, призначені, як і локальні мережі для надання послуг, але значно більшій кількості користувачів, що знаходяться на великій території.

У глобальних мережах існує три принципово різні схеми комутації:

- комутація каналів;
- комутація повідомлень
- комутація пакетів;

Комутація каналів в глобальних мережах – процес, який за запитом здійснює з'єднання двох або більше станцій даних і забезпечує монопольне використання каналу передачі даних до тих пір, поки не станеться роз'єднання. Комутація каналів має на увазі утворення безперервного фізичного каналу із послідовно сполучених окремих канальних ділянок для прямої передачі даних між вузлами. Окремі канали

з'єднуються між собою спеціальною апаратурою – комутаторами, які можуть встановлювати зв'язки між будь-якими кінцевими вузлами мережі.

Комутація повідомлень в глобальних мережах – процес пересилки даних, що включає прийом, зберігання, вибір вихідного напряму і подальшу передачу повідомлень без порушення їх цілісності. Використовуються в тих випадках, коли не очікується негайної реакції на повідомлення. Повідомлення передаються між транзитними комп'ютерами мережі з тимчасовою буферизацією їх на дисках кожного комп'ютера. Повідомленнями називаються дані, що об'єднані смисловим змістом, мають певну структуру і придатні для обробки, пересилки або використання.

Джерелами повідомлень можуть бути голос, зображення, текст, дані. Для передачі звуку традиційно використовується телефон, зображень – телебачення, тексту – телеграф (телетайп), даних – обчислювальні мережі. Встановлення з'єднання між відправником і одержувачем з можливістю обміну повідомленнями без помітних тимчасових затримок характеризує режим роботи online. При істотних затримках із запам'ятовуванням інформації в проміжних вузлах маємо режим offline.

Комутація пакетів в глобальних мережах – це комутація повідомлень, представлених у вигляді адресованих пакетів, коли канал передачі даних зайнятий лише під час передачі пакету і по її завершенню звільняється для передачі інших пакетів. Комутатори мережі, в ролі яких виступають шлюзи і маршрутизатори, приймають пакети від кінцевих вузлів і на підставі адресної інформації передають їх один одному, і в кінці станції призначення.

У глобальних мережах для передачі інформації застосовуються наступні види комутації:

комутація каналів (використовується при передачі аудіоінформації по звичайних телефонних лініях зв'язку;

комутація повідомлень (застосовується в основному для передачі електронної пошти, в телеконференціях, електронних новинах);

комутація пакетів (для передачі даних, в даний час використовується також для передачі аудіо - і відеоінформації)

Перевагою мереж комутації каналів є простота реалізації (утворення безперервного фізичного каналу), а недоліком - низький коефіцієнт використання каналів, висока вартість передачі даних, підвищений час чекання інших користувачів.

При комутації повідомлень передача даних (повідомлення) здійснюється після звільнення каналу, поки воно не дійде до адресата. Кожен сервер проводить прийом, перевірку, збірку, маршрутизацію і передачу повідомлення. До переваг можна віднести - зменшення вартості передачі даних. Недоліком даного способу є низька швидкість передачі інформації, неможливість ведення діалогу між користувачами.

Пакетна комутація має на увазі обмін невеликими пакетами (частина повідомлення) фіксованої структури, які не спричиняють утворення черг у вузлах комутації. Достоїнства: швидке з'єднання, надійність, ефективність використання мережі.

РОЗДІЛ 2.
КОМПЛЕКСНІ СИСТЕМИ ЗАХИСТУ В КМ

2.1. Основні принципи захисту інформації при підключенні до мережі Інтернет

Під час передачі конфіденційної інформації через Інтернет важливо використовувати безпечний протокол, наприклад HTTPS. Це забезпечує шифрування даних і запобігає несанкціонованому доступу.

Налаштування надійних паролів і двофакторної автентифікації допомагає запобігти несанкціонованому доступу до мережевих ресурсів. Важливо використовувати унікальні паролі для кожного облікового запису та регулярно їх оновлювати.

Встановлення та налаштування брандмауера дозволяє відстежувати трафік, що входить у вашу мережу та виходить із неї. Це допомагає запобігти несанкціонованому доступу та забезпечує безпеку мережі.

Комп’ютери можуть залишатися вільними від вірусів і троянів, якщо антивірусне програмне забезпечення встановлено та оновлено належним чином. Це програмне забезпечення виявляє та запобігає шкідливому програмному забезпеченню, зберігаючи вашу систему чистою та захищеною.

Щоб утриматися від хакерів, важливо регулярно виправляти будь-які виявлені прогалини в операційних системах і програмному забезпеченні. Виконання оновлень має ключове значення, щоб запобігти використанню цих недоліків.

Обмеження доступу до ресурсів мережі лише для авторизованих користувачів досягається за допомогою контролю доступу. Це робиться шляхом встановлення прав доступу, розробки політик доступу та використання рівнів авторизації, які разом забезпечують контроль над інформацією.

Рис. 2.1 Ієрархічний підхід до забезпечення безпеки інформації

2.2. NAT-Перетворення

В локальній мережі використовуються приватні IP-адреси з діапазонів, які визначені спеціально для цього. Найпоширеніші діапазони приватних IP-адрес [9] включають 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. NAT дозволяє замаскувати приватні IP-адреси з публічними IP-адресами, що дозволяє пристроям в локальній мережі виходити в Інтернет через одну або декілька публічних IP-адрес.

У локальних мережах NAT змінює IP-адресу вихідних пакетів, посилаючись на свою таблицю перетворення IP-адрес. Ця таблиця містить зіставлення між приватною та загальнодоступною IP-адресами, тому, коли пристрій у локальній мережі надсилає пакет до Інтернету, приватна IP-адреса буде перетворена на відповідну публічну IP-адресу на основі таблиці.

Трансляція NAT передбачає трансляцію як IP-адреси, так і порту. Кожен пакет, що проходить, містить унікальний номер порту, який відповідає програмі або службі. NAT з'єднує публічні та приватні мережеві порти відповідно, забезпечуючи передачу даних до та з Інтернету.

Для онлайн-захисту NAT є корисним інструментом, оскільки він забезпечує безпеку локальної мережі шляхом фільтрації трафіку. Ви можете використовувати загальнодоступну IP-адресу для зовнішнього зв'язку, але приватні IP-адреси не доступні для прямого підключення до Інтернету, додаючи додатковий рівень захисту від зовнішніх загроз.

Використання трансляції NAT у мережах компаній має вирішальне значення, оскільки це дозволяє раціоналізовано використовувати обмежену кількість публічних IP-адрес. Крім того, при підключенні до Інтернету це гарантує захист і відокремленість в локальній мережі.

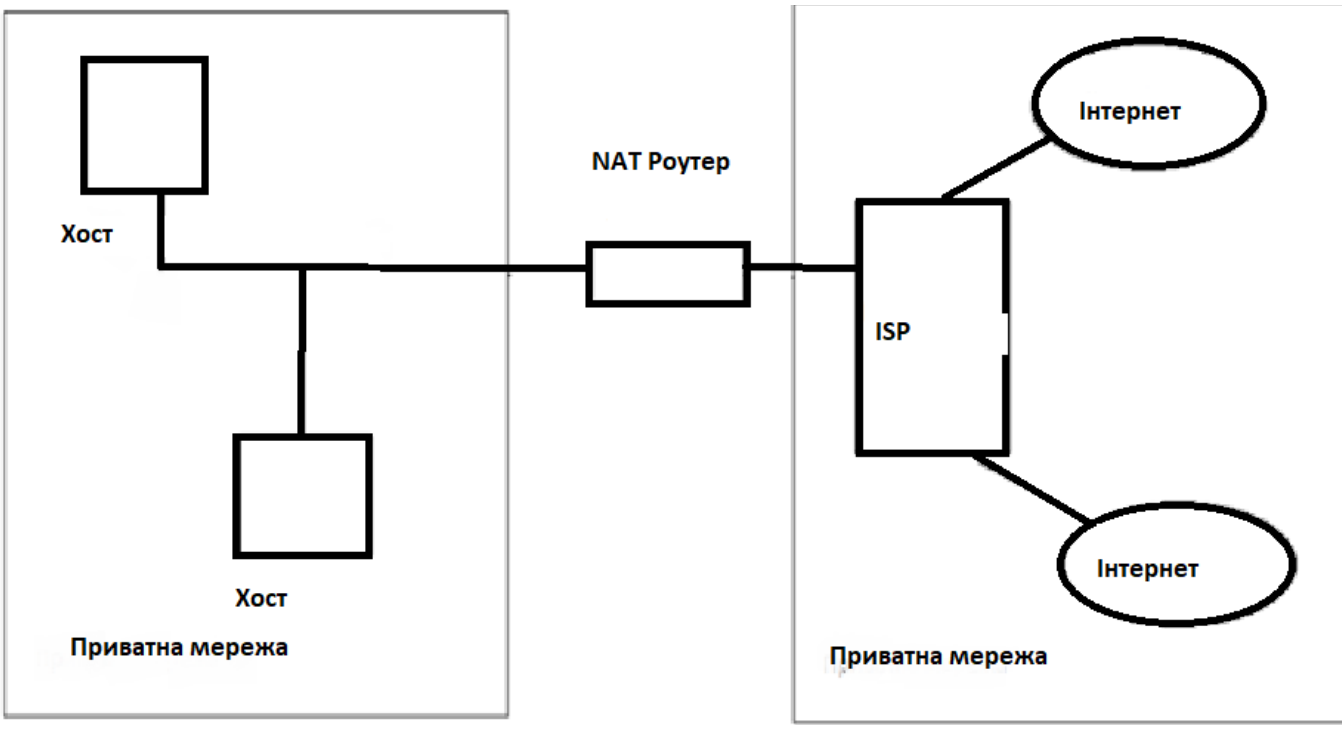

Рис.2.2 Принцип роботи NAT

2.3. Демілітаризована зона

Демілітаризована зона (DMZ) - це сегмент мережі, який розташовується між внутрішньою мережею організації та зовнішньою мережею, зазвичай Інтернетом. DMZ використовується для розміщення публічно доступних ресурсів, таких як веб-сервери, електронна пошта, VPN-сервери та інші, які потребують зовнішнього доступу.

Основна мета DMZ полягає в тому, щоб відокремити публічні ресурси від внутрішньої мережі, що містить цінну корпоративну інформацію. Це робиться для забезпечення додаткового рівня безпеки, де зовнішні користувачі мають обмежений доступ до внутрішніх ресурсів.

Основні принципи та компоненти DMZ в корпоративних мережаху наведені нижче.

Розміщення серверів - в DMZ розташовуються сервери, які необхідні для зовнішнього доступу. Це можуть бути веб-сервери, поштові сервери, FTP-сервери тощо. Вони налаштовані таким чином, щоб надавати публічним користувачам обмежений доступ до відповідних ресурсів.

Файрвол - встановлюється між DMZ та внутрішньою мережею, а також між DMZ та зовнішньою мережею. Він контролює трафік між цими зонами та застосовує правила безпеки. Файрвол фільтрує трафік та забезпечує захист внутрішніх ресурсів від несанкціонованого доступу.

DMZ-хост - це сервер або пристрій, який розміщується в DMZ та відповідає за безпеку мережі. Він може включати механізми моніторингу, інтранет-сервіси, системи ідентифікації та аутентифікації, а також інші засоби захисту.

Разделение трафіку - у DMZ зазвичай використовуються різні підмережі для публічних серверів та інших ресурсів. Це дозволяє контролювати та обмежувати доступ до окремих серверів та послуг.

DMZ дозволяє організаціям надати зовнішнім користувачам доступ до публічних ресурсів, забезпечуючи при цьому відокремлення внутрішньої мережі та захист корпоративної інформації. Вона використовується для створення безпечних окремих зон у корпоративній мережі та забезпечення безпеки комунікації між зовнішніми та внутрішніми ресурсами.

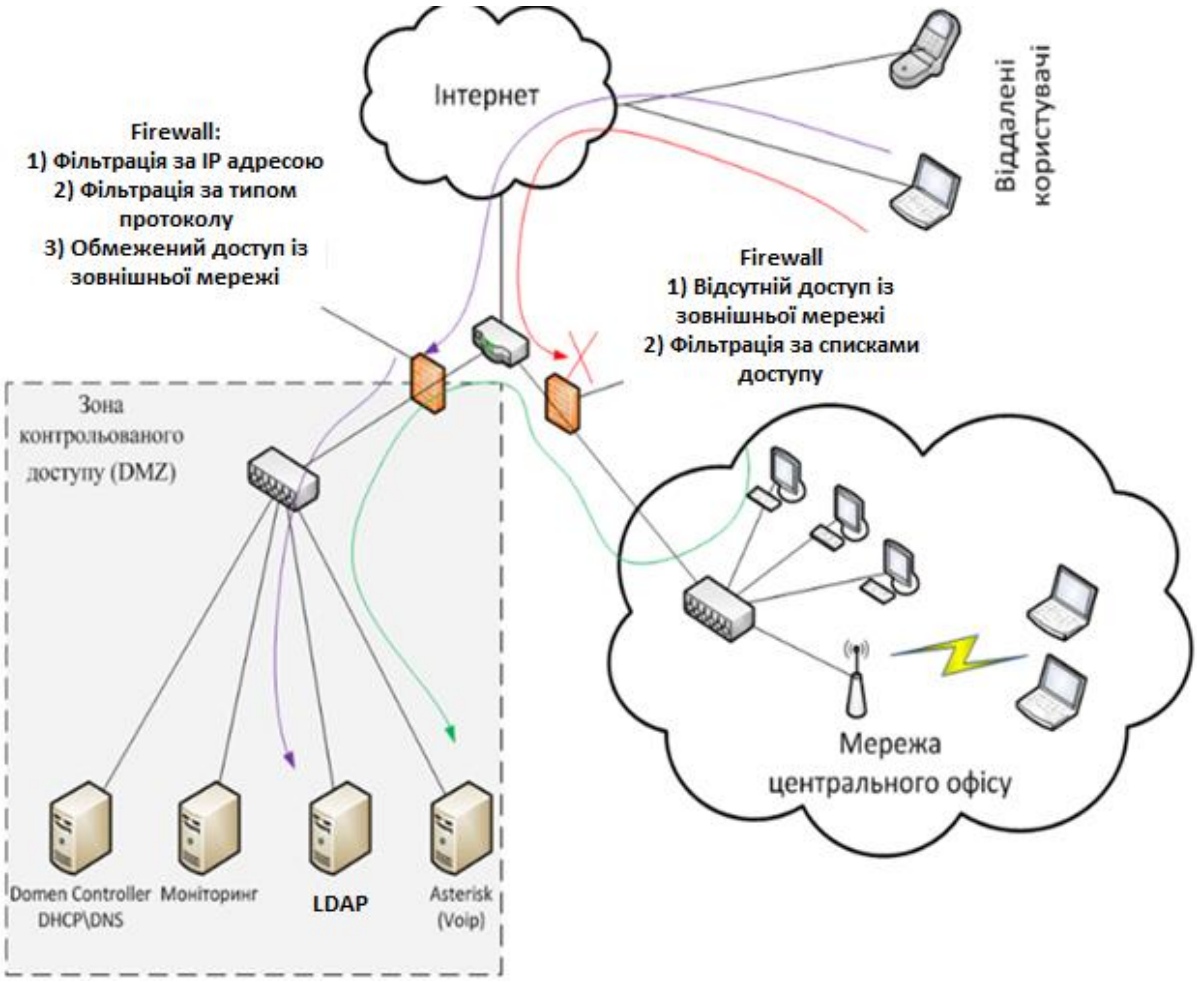

Рис. 2.3 - Зони контрольованого доступу

2.4. Антивірусний захист КМ

Антивірусний захист є важливою складовою безпеки корпоративних мереж. Він призначений для виявлення, блокування та видалення шкідливих програм, таких як віруси, троянські програми, черв'яки та інші види шкідливого програмного забезпечення, що можуть завдати шкоди мережі та комп'ютерам внутрішньої мережі.

Основні принципи та компоненти антивірусного захисту в корпоративних мережах - антивірусне програмне забезпечення. Це основний компонент антивірусного захисту. Антивірусне програмне забезпечення встановлюється на комп'ютерах та серверах в мережі і постійно сканує систему на наявність шкідливих програм. Воно виявляє та блокує віруси, сповіщає про загрози та видаляє або поміщає їх в карантин для подальшого аналізу.

Оновлення вірусних баз конче необхідне для безпеки пристроїв. Антивірусне програмне забезпечення [10] використовує вірусні бази даних, які містять інформацію про відомі віруси та їх варіанти. Ці бази оновлюються регулярно, щоб виявляти нові загрози та забезпечувати ефективний захист від них. Оновлення вірусних баз зазвичай проводяться через Інтернет.

Антивірусне програмне забезпечення проводить періодичні сканування комп'ютерів та серверів в мережі для виявлення шкідливих програм. Сканування може бути заплановане на певний час або виконуватися у режимі реального часу, коли нові файли або програми додаються на комп'ютер.

Антивірусне програмне забезпечення може бути інтегроване з брандмауером, що дозволяє контролювати трафік, що виходить і входить до мережі. Це допомагає блокувати вхідні та вихідні підозрілі з'єднання та захищає мережу від потенційних загроз.

Корпоративні мережі повинні мати встановлені політики безпеки, що включають правила використання антивірусного програмного забезпечення. Ці політики встановлюють вимоги до встановлення та оновлення антивірусного програмного забезпечення на всіх пристроях, що підключені до мережі.

Корпоративні мережі можуть використовувати системи моніторингу, які виявляють підозрілу активність, сповіщають про потенційні загрози та дозволяють швидко реагувати на вразливості та атаки.

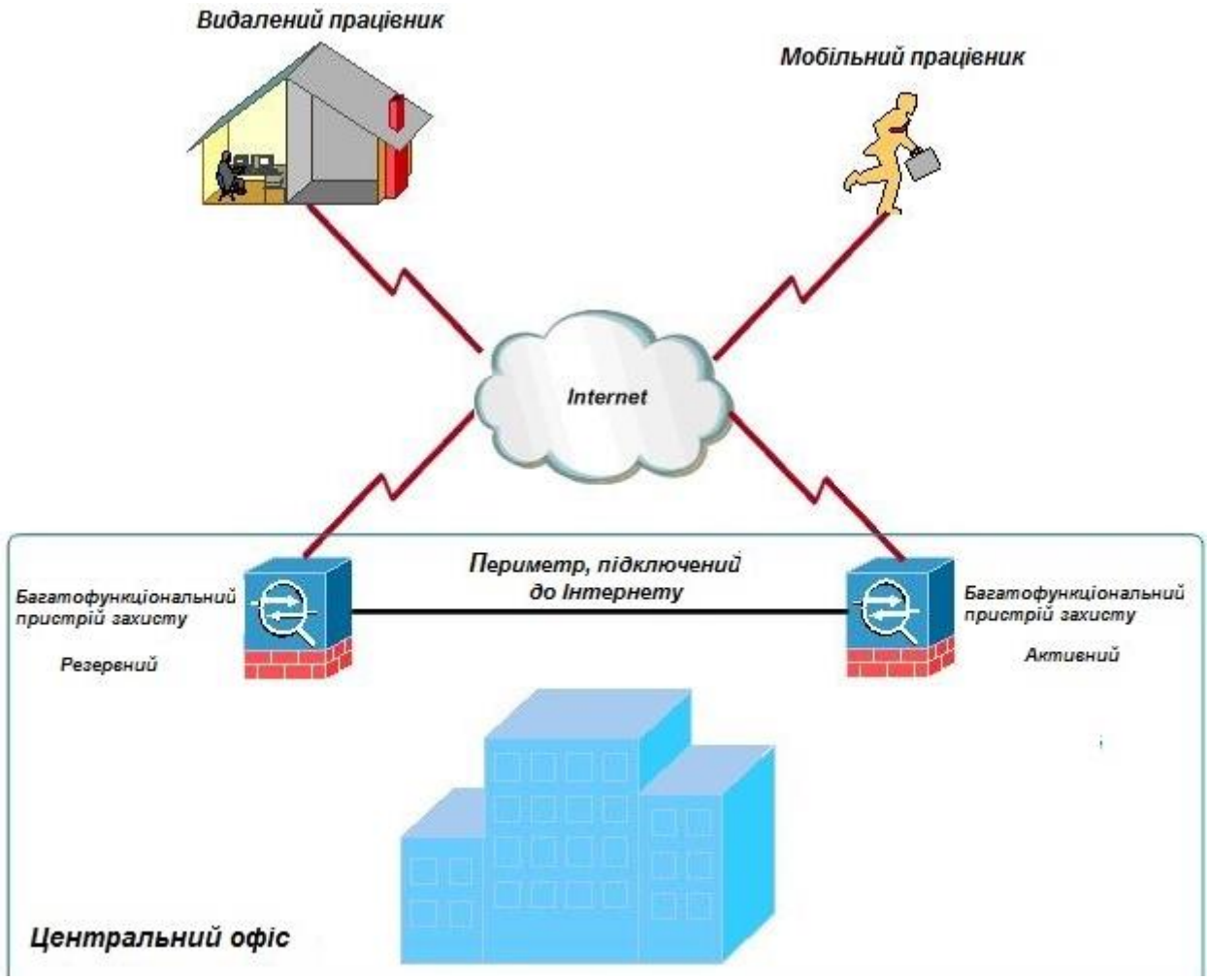

Рис. 2.4 Периметр безпеки корпоративної мережі

Важливо пам'ятати, що антивірусний захист варто поєднувати з іншими заходами безпеки, такими як брандмауери, системи виявлення вторгнень та регулярні оновлення програмного та апаратного забезпечення.

2.5. Використання Log-Серверу

Використання Log-серверу [11] в корпоративних мережах є важливою складовою безпеки та управління мережею. Log-сервер (лог-сервер) - це сервер, який призначений для зберігання та аналізу лог-файлів, які містять інформацію про події, що відбуваються в мережі, такі як з'єднання, авторизації, активності користувачів, зміни конфігурацій тощо.

Основні принципи та функції використання Log-серверу в корпоративних мережах наведені нижче.

Log-сервер отримує лог-файли від різних пристроїв та систем в мережі, таких як мережеві комутатори,маршрутизатори, сервери, брандмауери та інші мережеві пристрої. Він зберігає ці лог-файли для подальшого аналізу та архівування.

Log-сервер дозволяє аналізувати лог-файли для виявлення незвичайних або підозрілих активностей в мережі. Це допомагає виявляти можливі загрози безпеці та інциденти, такі як спроби несанкціонованого доступу, атаки злому паролів, вторгнення тощо.

За допомогою Log-сервера можна виявити проблеми у мережі, такі як відмови обладнання, перевантаження мережі, некоректну конфігурацію тощо. Аналіз лог-файлів може допомогти вчасно виявити та вирішити ці проблеми, що сприяє підтримці безперебійної роботи мережі.

Log-сервер дозволяє виконувати аудит та збирати дані, необхідні для відповідності з обов'язковими вимогами та регуляторними стандартами, такими як PCI DSS, HIPAA, GDPR. Він забезпечує збір та збереження лог-файлів, необхідних для аудиту та перевірки відповідності.

У разі виявлення потенційних інцидентів безпеки, Log-сервер дозволяє проводити подальше розслідування шляхом аналізу лог-файлів та відстеження послідовності подій. Це допомагає ідентифікувати джерело інциденту, оцінити його наслідки та прийняти відповідні заходи для відновлення безпеки мережі.

Log-сервер може забезпечувати захист лог-файлів від несанкціонованого доступу або випадкової втрати даних. Лог-файли можуть бути резервовані, шифровані та забезпечені механізмами контролю доступу, щоб забезпечити їх цілісність та конфіденційність.

Використання Log-серверу в корпоративних мережах дозволяє забезпечити контроль, аналіз та захист важливої інформації, а також сприяє виявленню потенційних загроз безпеці та управлінню мережевою інфраструктурою.

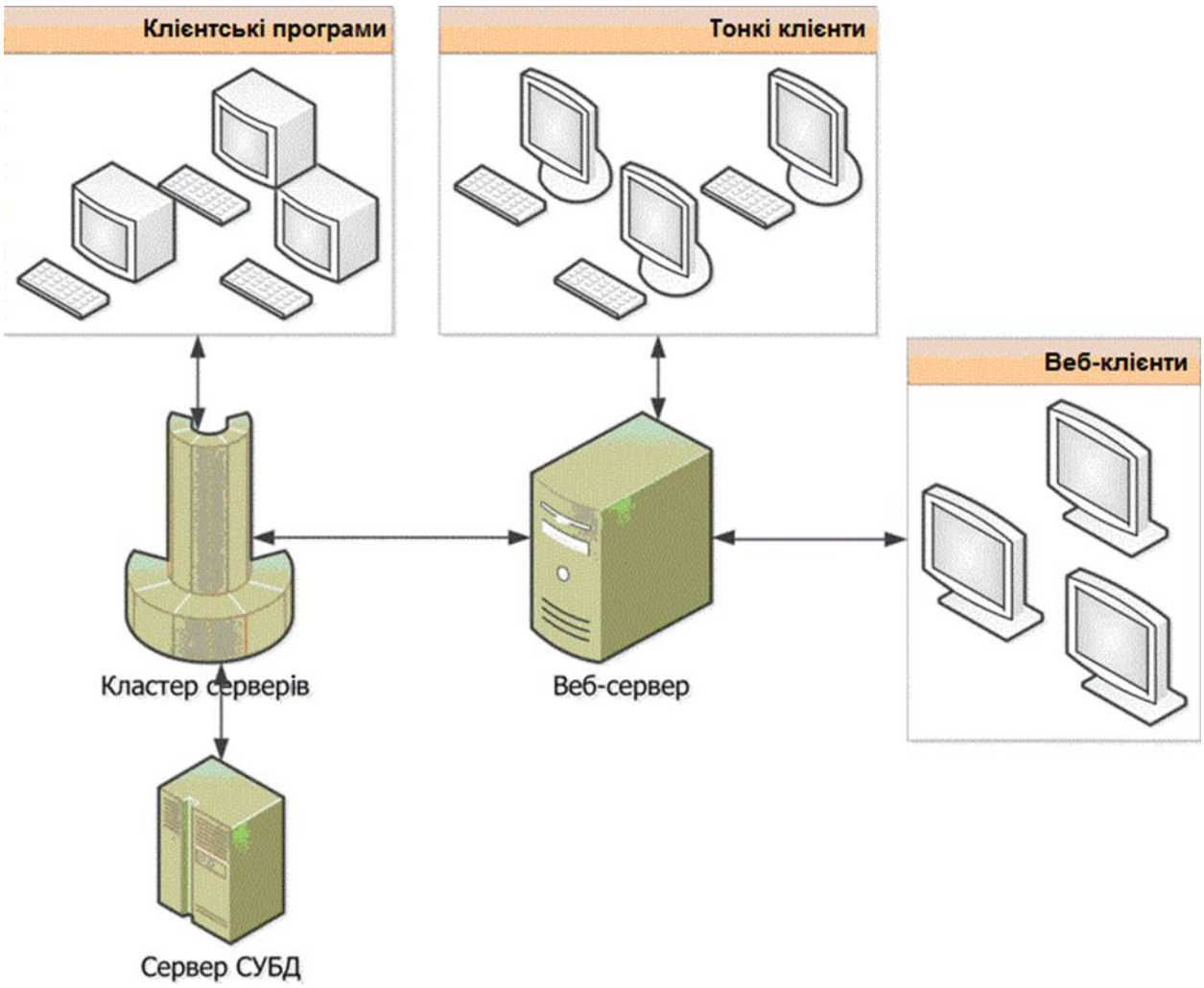

Рис. 2.5 Принцип влаштування використання Log-Серверу

2.6. Захист інформації за допомогою міжмережевих екранів

Захист інформації за допомогою міжмережевих екранів (firewalls) є важливою складовою безпеки корпоративних мереж. Міжмережеві екрани є спеціальними пристроями або програмними рішеннями, які контролюють трафік, що проходить між мережами, і застосовують набір правил для фільтрації, блокування та дозволу доступу до ресурсів мережі.

Міжмережевий екран фільтрує трафік, що проходить через нього, на основі заданих правил. Це дозволяє заблокувати небажаний трафік, такий як шкідливі атаки, несанкціонований доступ, віруси, спам та інші загрози безпеці мережі.

Міжмережні екрани дозволяють налаштовувати правила доступу до ресурсів мережі [12]. Це включає блокування небажаного доступу зовнішніх користувачів до внутрішніх ресурсів, установку обмежень на основі IP-адрес, портів, протоколів тощо.

Міжмережевий екран може використовувати технологію NAT (Network Address Translation) для перетворення IP-адрес і портів між зовнішньою і внутрішньою мережами. Це дозволяє забезпечити захист внутрішніх ресурсів, ховаючи їх реальні IP-адреси від зовнішнього світу.

Міжмережеві екрани можуть підтримувати віртуальні приватні мережі (VPN), що забезпечують зашифровану комунікацію між розрізненими мережами або віддаленими користувачами. Це дозволяє забезпечити безпечний обмін даними і захищений доступ до мережевих ресурсів з будь-якої точки підключення.

Міжмережевий екран може вести журнал подій, які стосуються трафіку, переходів, блокування та інших подій безпеки. Журнали можуть бути використані для аналізу і розслідування інцидентів, моніторингу безпеки мережі та виявлення нетипової активності.

Для виявлення та блокування шкідливого трафіку, який може призвести до компрометації безпеки мережі міжмережеві екрани можуть застосовувати методи перевірки цілісності трафіку, такі як інспекція пакетів (packet inspection) або використання сигнатур атак.

Міжмережеві екрани є необхідним елементом безпеки в корпоративних мережах, оскільки вони дозволяють забезпечити контроль, фільтрацію та захист трафіку, що проходить між мережами. Це допомагає попередити атаки, захищати внутрішні ресурси та забезпечувати безпеку мережі в цілому.

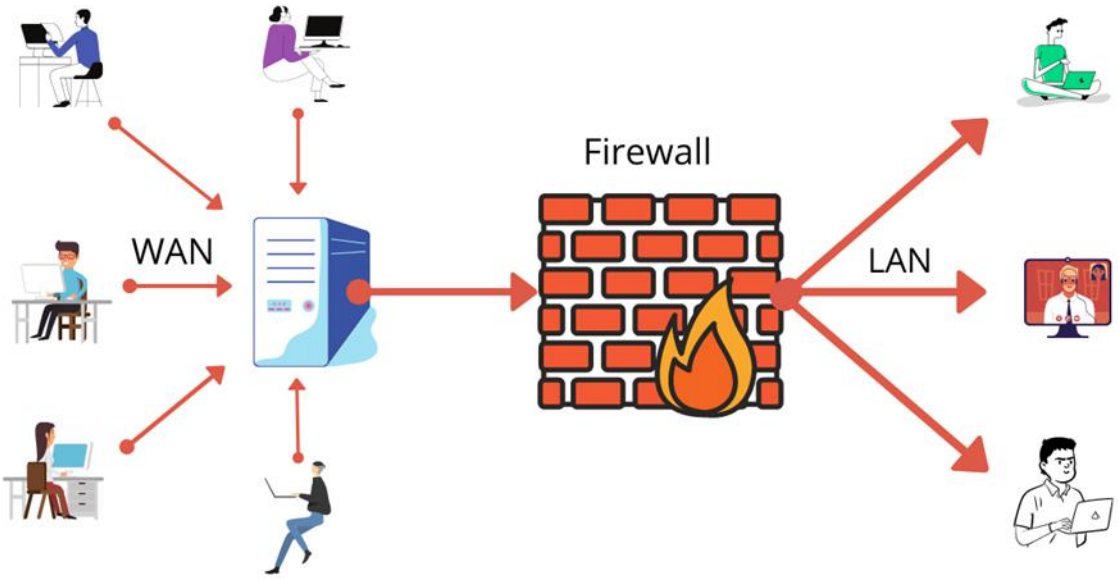

Рис. 2.6 Принцип роботи міжмережевого екрану

РОЗДІЛ 3
Проєктування корпоративної мережі малого підприємства на базі обладнання Cisco

3.1. Характеристика авіапідприємства

Авіакомпанія - це організація, яка надає послуги цивільної авіації. Характеристики авіакомпанії можуть включати наступні елементи:

- Тип авіакомпанії: існують різні типи авіакомпаній: авіакомпанії, виробники літаків та постачальники авіаційних послуг.
- Розмір: авіакомпанії варіюються за розміром від невеликих місцевих авіакомпаній до великих міжнародних авіакомпаній.
- Транспорт: авіакомпанії зазвичай забезпечують пасажирські та вантажні перевезення. Деякі компанії можуть пропонувати інші послуги, такі як чартерні рейси, пасажирські літаки загального призначення та повітряні таксі.
- Маршрути та пункти призначення: авіакомпанії можуть мати внутрішні та міжнародні напрямки. Деякі з них виконують регулярні рейси, а інші спеціалізуються на напрямках для відпочинку.
- Літаки: авіакомпанії можуть мати парк літаків різних типів і розмірів, включаючи пасажирські, вантажні, легкомоторні літаки та гелікоптери.
- Безпека: авіакомпанії повинні дотримуватися високих стандартів безпеки, включаючи відповідність міжнародним правилам і нормам, таким як правила Міжнародної організації цивільної авіації (ІКАО).
- Класи обслуговування: багато авіакомпаній пропонують пасажирам різні класи обслуговування, такі як економ-клас, бізнес-клас і перший клас. Кожен клас може мати свої особливості з точки зору комфорту пасажирів, послуг та зручностей.

- Міжнародна присутність: деякі авіакомпанії мають розгалужену міжнародну мережу маршрутів і працюють у багатьох країнах. Це може включати міжнародні рейси, партнерські відносини з іншими авіакомпаніями та участь у глобальних альянсах авіакомпаній.
- Інновації та технології: деякі авіакомпанії активно впроваджують нові технології та інновації, такі як використання безпілотних літаків, інтелектуальних систем управління мережею, сучасних засобів зв'язку та електронних послуг для пасажирів.
- Екологічна стійкість: враховуючи вплив авіаційної діяльності на навколишнє середовище, багато авіакомпаній зменшують свій вплив на довкілля, зосереджуючись на скороченні викидів парникових газів, використанні екологічно чистих видів палива та впровадженні енергоефективних технологій.
- Репутація та безпека: репутація та історія авіакомпанії є значущими факторами при виборі авіакомпанії. Клієнти будуть звертати увагу на безпеку польотів, рівень обслуговування бортів, стабільність і надійність компанії.

3.2. Розрахунок необхідної кількості комп’ютерного устаткування корпоративної мережі

Щоб розрахувати кількість комп'ютерного обладнання, для мережі компанії, необхідно враховано наступні фактори:

1) Визначено загальну кількість людей, підключених до мережі. Враховано як ключових співробітників, так і додаткових користувачів, таких як стажери та тимчасові працівники.

2) Кількість пристроїв на одного працівника. Враховано кількість пристроїв (наприклад, комп'ютерів, ноутбуків, смартфонів), якими

користується кожен працівник. Це допоможе визначити загальну кількість необхідних мережевих портів.

3) Вимоги до пропускної здатності. Визначено пропускну здатність, необхідну для корпоративної мережі. Це залежить від типу бізнесу та вимог до швидкості передачі даних. Наприклад, нашій компанії не знадобиться більша пропускна здатність за відсутності великої кількісті мультимедійного контенту.

4) Апаратне забезпечення: визначено, яке апаратне забезпечення буде використовуватися для побудови мережі, наприклад, комутатори, маршрутизатори, маршрутизатори безпеки та мережеві кабелі. Визначено необхідну кількість пристроїв, виходячи з розміру мережі та потреб користувачів.

5) Резервування та масштабованість – продумане резервування та масштабованість мережі. Розглянуто можливість додавання нових працівників або розширення можливостей мережі в майбутньому.

6) Безпека - враховуючи вимоги до безпеки мережі обрано необхідне обладнання, яке забезпечує високий рівень захисту даних та безпеки мережі.

7) Розраховано кількість комп'ютерного обладнання, необхідного для мережі компанії.

3.3. Вибір і обґрунтування програмного забезпечення КМ

Вибір та обґрунтування програмного забезпечення для корпоративної мережі (КМ) залежить від конкретних потреб та вимог вашої компанії, типу бізнесу, розміру організації та бюджету. Однак нижче наведено деякі загальні категорії програмного забезпечення для КМ та їх обґрунтування.

Системи електронного документообігу (EDMS) дозволяють ефективно обробляти та управляти документами в електронному форматі. СЕД також допомагає забезпечити управління документами відповідно до внутрішніх та законодавчих вимог.

Системи управління взаємовідносинами з клієнтами (CRM) дозволяють відстежувати, управляти та аналізувати дані про клієнтів та їхню взаємодію. Вони допомагають покращити процеси продажу, маркетингу та обслуговування клієнтів, підвищити їхню лояльність та задоволеність, а також покращити комунікацію з клієнтами.

Системи управління проектами допомагають планувати, організовувати та контролювати реалізацію проектів. Вони можуть управляти завданнями, ресурсами, термінами і витратами проекту, а також сприяти комунікації та співпраці між учасниками проекту.

Системи управління людськими ресурсами (HRM) допомагають автоматизувати та оптимізувати процеси управління персоналом, такі як найм, відбір, навчання, оцінка працівників та управління персональними даними. Вони забезпечують централізоване зберігання та доступ до даних працівників, спрощують адміністративні процедури та підвищують ефективність управління персоналом.

Системи планування ресурсів підприємства (ERP) інтегрують різні функціональні області компанії, такі як фінанси, управління запасами, логістика та виробництво. ERP-системи підтримують ефективне планування та управління ресурсами, оптимізують бізнес-процеси та забезпечують інтегроване управління ресурсами.

Обґрунтування вибору конкретного програмного забезпечення для КМ має ґрунтуватися на аналізі потреб компанії, бюджету, можливостей впровадження та підтримки, оцінках і оглядах програмного забезпечення.

3.4. Вибір серверного обладнання

Вибір серверного обладнання для нашої компанії залежить від різних факторів, включаючи масштаби бізнесу, тип додатків або послуг, що будуть розгортані на серверах, обсяги обробки даних, бюджет та вимоги до надійності та масштабованості. Ось критерії, які я враховував при виборі серверного обладнання:

1) Продуктивність: враховувати обсяг обчислювальних ресурсів (процесори, оперативна пам'ять) та потужність сервера. Якщо ви плануєте виконувати великі завдання або розгортати важкі додатки, потрібні сервери з високою продуктивністю.

2) Масштабованість: розглянути можливості масштабування серверів. Якщо ви очікуєте зростання обсягу даних або потреб, важливо мати можливість додавати нове обладнання або розширювати наявне.

3) Надійність: визначити вимоги до надійності серверів. Ви можете розглянути сервери з підтримкою резервування живлення, можливістю гарячої заміни компонентів та іншими функціями для забезпечення безперебійної роботи.

4) Сховище даних: розглянути обсяг і тип сховища даних, які будуть потрібні для вашої компанії. Це може включати внутрішній накопичувач, мережеві сховища (NAS або SAN) або хмарні рішення.

5) Система охолодження: взяти до уваги потужність охолодження серверних приміщень. Деякі сервери можуть вимагати спеціальних вимог щодо охолодження, щоб запобігти перегріву.

6) Підтримка та гарантія: Перевірте наявність технічної підтримки та гарантійних умов від виробників серверного обладнання.

Як основний сервер я обрав Блейд-сервер Cisco UCS B200 M5 Cisco UCS B200 M5 [13] встановлюється в шасі Cisco UCS 5108 і має вдвічі меншу ширину. Кількість лез у шасі може досягати восьми, що забезпечує легке масштабування інфраструктури. Ключовими особливостями Cisco UCS B200 M5 є висока щільність забезпечення і підтримка віртуальних і фізичних середовищ. Найбільш поширеними сферами застосування цього блейд-сервера є центри обробки даних і розподілені структури.

Блейд-сервер Cisco UCS B200 M5, розроблений для використання в середовищах розподіленої інфраструктури, характерних для різних корпоративних середовищ, є ідеальним рішенням для центрів обробки даних завдяки своїй збалансованій щільності та високій продуктивності. Cisco UCS B200 M5 справляється з великими робочими навантаженнями і дозволяє розгорнути практично будь-яке хмарне рішення. Широкий спектр комерційного програмного забезпечення може

бути легко доставлений з цим типом сервера. Блейд-сервери Cisco UCS B200 M5 не потребують додаткового живлення та охолодження, окрім стандартних блоків живлення та охолодження в корпусі, і мають достатню обчислювальну потужність для вимогливих корпоративних додатків, таких як SAP HANA та Oracle. . Форм-фактор. Блейд-сервери - це леза половинної ширини; в шасі 5108 Blade Server Chassis можна розмістити до восьми блейд-серверів. Процесор. UCS B200 M5 - це двопроцесорний блейд на базі масштабованих процесорів Intel Xeon з підтримкою наступних сімейств процесорів: Bronze; Platinum; і Silver; і Gold; і підтримує наступні сімейства процесорів: Bronze; Platinum; Silver; Gold. Він також може бути оснащений до двох графічних процесорів Nvidia, по одному в кожному з проміжних слотів на передній і задній панелі корпусу. Пам'ять. Кожен процесор блейд-сервера оснащений двома триканальними контролерами пам'яті, кожен з яких підтримує два слоти DRAM. Таким чином, UCS B200 M5 може вмістити 12 модулів пам'яті на кожному процесорі і 24 модулі пам'яті в системі в цілому. ВВЕДЕННЯ/ВИВЕДЕННЯ На задній панелі блейд-сервера UCS B200 M5 розташований модульний слот LAN-on-motherboard (mLOM) для комбінованих адаптерів, з можливістю встановлення додаткових адаптерів у верхній слот мезоніну. Варіанти встановлення адаптерів слот mLOM Cisco UCS VIC 1440 (4x10 Гбіт/с уніфікований ввід/вивід) Cisco VIC 1340 (2x40 Gigabit Ethernet, Fibre Channel over Ethernet (FCoE)) Мезонінний слот: Мезонінна карта Cisco UCS VIC 1480 (VIC 1440 з +4 додатковими портами уніфікованого вводу/виводу 10 Гбіт/с). Мезонінна плата Cisco VIC 1380 (+2 порти до VIC 1340 з уніфікованим вводом/виводом 40 Гбіт/с). Мезонінна плата розширення портів Cisco (+4 порти 10 Гбіт/с уніфікованого вводу/виводу до VIC 1440). Задня мезонінна карта з графічним процесором Cisco nVIDIA P6 Blade NVMe карта пам'яті Cisco Передній слот мезоніну також доступний і може бути встановлений тут: слот мезоніну: SAS RAID-контролер Cisco FlexStorage 12 Гбіт/с RAID-контролер Cisco FlexStorage 12 Гбіт/с SAS з кешем 2 ГБ Cisco FlexStorage NVMe або модуль міграції Передня мезонінна карта з графічним процесором Cisco nVIDIA P6 Зберігання даних Для зберігання локальних даних на блейд-серверах доступні наступні варіанти 2 карти SD (Secure Digital) (32, 64 або 128 ГБ з дзеркальним відображенням); 2 флеш-

накопичувачі M.2 SATA об'ємом 240 ГБ або 960 ГБ; PCIe флеш-пам'ять: 560 ГБ High Endurance або 3,2 ТБ Medium Endurance, встановлюється в задній відсік мезоніну; Два 2,5-дюймових SSD/HDD або NVMe SSD з можливістю гарячого підключення на передній панелі. Особливості блейд-сервера Cisco UCS B200 M5 До ключових особливостей цього обладнання можна віднести наступні: "В основі блейд-сервера лежать два процесори Intel Xeon, включаючи високопродуктивну модель з 28 ядрами на чіп: цього достатньо, щоб впоратися з робочими навантаженнями сучасних віртуальних і фізичних середовищ. Апаратне забезпечення має 24 слоти DIMM для розміщення модулів пам'яті DDR4. Продуктивність зростає з кожною новою плашкою: максимальний обсяг оперативної пам'яті може становити до 3 ТБ. У половину слотів можна встановити постійну пам'ять Intel Optane DC Persistent Memory. Підключення мережевих пристроїв здійснюється через конвергентний адаптер Cisco VIC 1340/1440 40/10, додатковий адаптер Gb+ Cisco VIC 1380/1480 в слоті MLOM і порт Port Extender (мезонін). Система може бути підключена наступним чином. Локальну підсистему зберігання даних можна розширити двома 2,5-дюймовими дисками. Можна встановити як твердотільні, так і механічні накопичувачі. Технічні характеристики блейд-сервера Cisco UCS B200 M5 Поєднання потужного апаратного забезпечення та програмного забезпечення для управління Cisco UCS Manager робить UCS B200 M5 дуже високопродуктивним і безпечним рішенням. UCS B200 M5 є одним з найбільш компактних і доступних за ціною завдяки продуманному шасі і високій щільності розміщення декількох серверів. Серед інших переваг цього блейд-сервера Один адаптер для карт розширення на передній і один на задній панелі корпусу; Широкий вибір карт розширення Два GPU; Підсистема локальних дисків Cisco Flex Storage; Два слоти малого форм-фактора (SFF, 2,5") для SSD/HDD накопичувачів. До двох роз'ємів M.2 SATA або SD для підключення карт пам'яті; Інтерфейс LAN/SAN забезпечує пропускну здатність до 80 ГБ/с. Блейд-сервер Cisco UCS B200 M5 може впоратися з найрізноманітнішими завданнями вивантаження даних в локальне сховище. Для обробки ресурсоємних додатків реалізована можливість підключення до двох графічних процесорів, а

інтелектуальні механізми управління дозволяють перевести багато завдань в автономний режим.

3.5. Вибір технології передачі даних

При виборі технології передачі даних для корпоративної мережі слід враховувати наступні фактори які описані ниОцініть потреби вашої організації у швидкості передачі даних і пропускній здатності мережі. Якщо вам потрібно передавати великі обсяги даних або обробляти медіа файли з високою роздільною здатністю, можливо, варто використовувати високошвидкісні технології, такі як Ethernet, Gigabit Ethernet або 10 Gigabit Ethernet. Відстань передачі: Враховуйте відстань, необхідну для передачі даних всередині компанії. Якщо вам потрібно з'єднати різні віддалені місця або обробляти дані на великих відстанях, корисними можуть бути бездротові технології, такі як Wi-Fi або супутниковий зв'язок. Надійність та стабільність: Важливо вибрати технологію передачі даних, яка забезпечує надійне і стабільне з'єднання. Цього можна досягти за допомогою технологій з надлишковими з'єднаннями, таких як Ethernet, або шляхом використання вдосконалених протоколів маршрутизації для запобігання втраті пакетів. Безпека Забезпечення безпеки даних є важливим фактором. Розгляньте технології, які забезпечують шифрування даних, автентифікацію та контроль доступу, такі як віртуальні приватні мережі (VPN), протоколи шифрування TLS/SSL та брандмауери. Масштабованість: Якщо ми плануємо рости і розширювати свою мережу, обираємо технології, які можна легко масштабувати. Наприклад, Ethernet широко підтримується і може бути розширена шляхом додавання комутаторів і маршрутизаторів. Вартість: враховувати витрати на встановлення та обслуговування обраної нами технології передачі даних. Порівняйте витрати на обладнання, встановлення, обслуговування та підтримку. Залежно від конкретних потреб компанії можна використовувати різні комбінації технологій передачі даних, включаючи комутовані мережі Ethernet, бездротові мережі Wi-Fi, віртуальні приватні мережі

(VPN) . В нашому випадку вибір пав на “Gigabit Ethernet” оскільки це оптимальний варіант під наші потреби.

Основні характеристики Gigabit Ethernet наведені нижче.

Швидкість передачі даних - Gigabit Ethernet пропонує пропускну здатність до 1 Гбіт/с, забезпечуючи значно швидшу передачу даних, ніж попереднє покоління Ethernet (10/100 Мбіт/с). Стандарти Gigabit Ethernet базується на стандартах IEEE 802.3ab і 802.3z, що забезпечує сумісність з широким спектром пристроїв і мережевого обладнання. Фізичне підключення Gigabit Ethernet може використовувати кабельну інфраструктуру, вже доступну для Ethernet попереднього покоління, наприклад, категорії 5e і 6. Дуплексний режим: Gigabit Ethernet підтримує повнодуплексний режим, забезпечуючи одночасну передачу і прийом даних на максимальній швидкості. Буферизація пам'яті: комутатори та інше мережеве обладнання Gigabit Ethernet часто мають вбудовані буфери для управління потоком даних і запобігання втрати пакетів. Розширення мережі: Gigabit Ethernet дозволяє легко розширювати мережі шляхом додавання комутаторів і використання розширених протоколів маршрутизації. Gigabit Ethernet широко використовується в корпоративних мережах, центрах обробки даних і локальних мережах, де потрібна висока швидкість передачі даних. Завдання, що вимагають високої пропускної здатності мережі, такі як швидка передача великих файлів, потокове відео та ресурсоємні програми, є можливими.

3.6. Вибір комутаційного обладнання корпоративної мережі

У якості головного та резервного маршрутизатора мій вибір пав на Cisco ISR4331-SEC/K9 тому що маршрутизатор Cisco ISR4331-SEC/K9 надає високоякісні послуги локальної мережі для всього підприємства та його філій завдяки багатоядерним процесорам, програмному забезпеченню Cisco IOS® XE, масштабованості та можливості інтеграції нових сервісів. Пристрої мають прискорені механізми шифрування, сервіси для обробки трафіку, в тому числі медіа-даних, і

пропонують різноманітні варіанти підключення: порти T1/E1, T3/E3 і Gigabit Ethernet. Послуги для філій Призначений для філіалів, Cisco ISR4331-SEC/K9 надає повний набір сервісів для обробки голосових і відеоданих, забезпечення високого рівня мережевої безпеки і надання доступу до мережі мобільним клієнтам. Модульний форм-фактор дозволяє модернізувати цей пристрій і оптимізувати його для прямого підключення до мережі шляхом встановлення нових модулів у слоти. Пристрої, що підключаються Маршрутизатор оснащений двома портами Gigabit Ethernet, до яких можна підключати SFP-пристрої. Крім того, Cisco ISR4331-SEC/K9 має два порти з роз'ємами RJ-45 для підключення більшості обслуговування мережевих пристроїв. Також є інтерфейс Gigabit Ethernet для управління самим маршрутизатором. Високоінтелектуальне програмне забезпечення Програмне забезпечення Cisco IOS XE призначене для надання послуг безпеки, голосового зв'язку, IP-маршрутизації та IP-мультиадресації. Також до складу пакету входять функції QoS, IP-мобільність, багатопротокольна комутація міток, підтримка декількох VPN і вбудовані інтерфейси управління. Додаткові функції також можна придбати, активувавши ліцензії на програмне забезпечення: На Cisco ISR4331-SEC/K9 можна встановити три розширені ліцензії в порівнянні з базовою ліцензією (IP-ліцензія встановлюється за замовчуванням): Досвід роботи з додатками: включає функції підвищення продуктивності та додатки. Об'єднані комунікації: охоплює голос, відео та додаткові мультимедійні сервіси. Безпека без шифрування даних або корисного навантаження: надає функції для захисту мережевої інфраструктури. Надійність передачі даних. Cisco ISR4331-SEC/K9 забезпечує новий рівень безпеки завдяки інноваційній технології Cisco Secure Development Lifecycle і Cisco Trust Anchor Technology Cisco SDL - це певна комбінація процесів і правил, які разом знижують ризик вразливості і підвищують відмовостійкість мережевої інфраструктури; TAT надає ряд послуг безпеки, заснованих на включенні модуля Trust Anchor, який перевіряє справжність програмного забезпечення Cisco під час завантаження.

Безпечна передача даних. Пристрій має вбудований брандмауер Cisco ISR-CX, який забезпечує додатковий захист критично важливої інформації та запобігає доступу несанкціонованих користувачів до ресурсів приватної мережі. Крім того,

програмне забезпечення Cisco IOS XE надає широкий спектр послуг для захисту мережевого трафіку і клієнтських пристроїв. Group Encrypted Transport VPN, Dynamic Multipoint VPN (DMVPN), Flex VPN і Easy VPN для захисту даних під час передачі Усунення мережевих загроз і запобігання мережевим атакам за допомогою програмного забезпечення Cisco IOS XE Zone-Based Firewall Захист мережі від несанкціонованого доступу шляхом аутентифікації, авторизації та обліку користувачів, а також створення інфраструктури відкритих ключів Продуктивність додатків. Функції додатків Cisco IOS XE, такі як виявлення мережевих додатків, IP SLA і NetFlow, забезпечують контроль трафіку і підвищують ефективність роботи співробітників Спеціальні функції і сервіси, такі як QoS, ACL і маршрутизація продуктивності, мінімізують час простою клієнтського обладнання. Крім того, мережевий досвід можна ще більше покращити, додавши Cisco Wide Area Application Services для реалізації передових методів оптимізації WAN, таких як оптимізація TCP, кешування, стиснення і прискорення роботи додатків. Крім того, Cisco ISR4331-SEC/K9 з інтегрованим WAAS надає повний набір функцій для забезпечення оптимальної продуктивності додатків, що доставляються з центрального офісу в філії. [15]

При виборі комутаторів, я вирішив зробити свій вибір на користь CISCO WS-C2960-24TT-L. Серія Cisco Catalyst 2960 - це сімейство комутаторів з фіксованою конфігурацією з портами Fastethernet, і Gigabit Ethernet, які надають розширені послуги локальної мережі для бізнесу початкового рівня і мереж віддалених офісів. Catalyst 2960 підтримує передачу голосу, даних, відео та захищений доступ. Він також забезпечує масштабоване управління в міру зміни потреб бізнесу. Cisco Catalyst 2960 пропонує інтелектуальні функції (створення складних списків контролю доступу, підвищена безпека), уніфіковані гігабітні аплінки (мідні 10/100/1000BASE-T Ethernet або SFP модулі для міграції на інше середовище - Cisco 1000BASE-SX, 1000BASE-LX, 1000BASE-ZX, 100BASE-FX, 100BASE-LX, CWDM SFP). Catalyst 2960 також пропонує QoS, багаторівневе обмеження швидкості, ACL (на основі MAC або IP-адреси і порту UDP/TCP), послуги багатоадресної розсилки, можливість регулювання швидкості передачі кожного порту з кроком 64 кбіт, більш швидкі з'єднання між

комутатором і сервером Підтримка агрегації каналів для прискорення з'єднань між комутаторами і серверами, підтримка тегів 802. 1q, до 255 VLAN на комутатор, до 4000 ідентифікаторів VLAN, управління за допомогою Cisco Network Assistant (підтримка широкого спектру моделей комутаторів від Cisco Catalyst 2960 до Cisco Catalyst 4506). Прошивка для коммутатора Cisco Catalyst 2960 доступна у версіях LAN Base і Lan Lite Image; LAN Base надає додаткові функції контролю доступу, такі як розширена безпека (ACL), DHCP Snooping, веб-аутентифікація і розширення 802.1x, опції конфігурації QoS, підтримка резервних джерел живлення RPS, а також більш широкий спектр інших функцій з більшою кількістю портів SFP. До них відносяться flexlink і моніторинг стану з'єднання, збільшення кількості підтримуваних VLAN (до 256), хостів IPv6, MLD snooping, LLDP-MED, RSPAN, MVR, DHCP Option 82 і IP SLA (відповідач).

Настільний роутер Cisco SB RV215W-E-K9-G5-RF

Частота роботи Wi-Fi - 2.4 ГГц

Швидкість LAN портів - 100 Мбіт/с

WAN-порт - Ethernet

Швидкість Wi-Fi - 150 Мбіт/с

Інтерфейси - 4 x LAN 10/100 Fast Ethernet, 1 x WAN 10/100 Fast Ethernet

Бездротові можливості - 802.11b, 802.11g, 802.11n

Функції безпеки:

1) Stateful Packet Inspection (SPI) брандмауер
2) Port Forwarding і запуску
3) Firewall списків контролю доступу та фільтрації вмісту
4) Відмова в обслуговуванні (DoS) попередження
5) MAC на основі бездротового контролю доступу
6) Статичне блокування URL або ключового слова блокування
7) Планування на основі політики доступу в Інтернет

3.7. Розрахунок адресного простору IP-адрес

Розрахунок адресного простору IP-адрес включає в себе визначення діапазону IP-адрес, які будуть використовуватись у мережі. Основні кроки для розрахунку адресного простору IP-адрес наступні:

Визначаємо версію протоколу IP (IPv4 або IPv6), залежно від потреб мережі. Більшість мереж зараз використовують IPv4 тому й в цій роботі буде використано цю версію.

Визначимо клас IPv4-адреси (A, B, C, D і E). Для менеджменту буде використано клас B. Це потрібно лише для семантичного виділення мережі. Весь адресний простір використовуватись не буде. Але для мережі підприємства буде використовуватись весь клас C.

Розрахуємо скільки мереж потрібно. Це може бути важливо для масштабування мережі та організації сегментів мережі для покращення безпеки та продуктивності.

Потрібна наступна кількість мереж:

1) 3 мережі для офісних працівників;
2) 1 для взаємодії між роутерами настільними та підключеними до них девайсами;
3) 1 мережа для лептопів і принтеру;
4) 2 мережі LAN для настільних роутерів;
5) Менеджмент.

Розрахунок, скільки IP-адрес потрібно в кожній підмережі.

1) Для офісних працівників в кожній має бути не більше 253 девайсів (мережа в подальшому планує рости);
2) Не більше 2 IP для кожного настільного роутера;
3) Мережа має містити 1 принтер і не більше 5 девайсів;
4) Так як LAN для настільних роутерів, то може дублюватись і не більше 253 девайсів;
5) Цю мережу винесли в окремий клас тому розмір може бути довільний.

Розподіляємо доступні IP-адреси між підмережами відповідно до потреб мережі. Тут враховані на потреби кожної підмережі та можливість розширення де це потрібно.

192.168.0.0/24, 192.168.1.0/24, 192.168.2.0/24 мережа для офісних працівників.

192.168.3.248/29 для принтера та ймовірної кількості декількох лептопів які друкуватимуть на ньому документацію.

192.168.3.254/30 для настільного роутера, тому що не більше 2 роутерів в межах компанії має бути, і на самоому роутері локальний dhcp 192.168.0.0/24 для обладнення на складі.

Менеджмент мережі 172.16.0.0/24 и 172.16.1.1/24

Кожна IP-адреса буде унікальна в мережі.

3.8. Побудова корпоративної мережі на основі обраного обладнання

Враховуючи всю інформацію яку я зібрав в процес виконання дипломного проєкту, я приступив до побудову Корпоративної мережі. Яка буде побудована за топологією - Зірка. Всі комп'ютери мережі під'єднані до центрального вузла, утворюючи фізичний сегмент мережі.

За основу було взято два роутери - Cisco ISR4331. Це зроблено задля високої відмовостійкості системи, оскільки один з них може вийти з ладу в процесі роботи за різних причин, то в нас буде резерв, на який переключимося у разі відмови першого. Це реалізується за допомогою протоколу STP. Далі в нашій мережі присутні 4 комутатори Cisco 2960-24TT. Три з яких є основними, а четвертий виконує роль резерву, у випадку недоступності одного з них. Це виконано також за допомогою STP протоколу. До першого та другого роутеру я підключив комутатор SW1,SW4. Оскільки SW1 один є головним і від нього далі підключені інші комутатори в мережі, а SW4 є резервом. До головного я під'єднав SW2,SW3.

Вони виконують однакову функцію, але знаходяться в різних Vlan, таким чином ми зменшили навантаження на широкомовний домен та надали необхідні доступи

працівникам до ресурсів яких вони потребують. Оскільки безпека мережі напряму залежить від кількості можливостей дій в мережі, які надані тому, чи іншому працівнику. До обох комутаторів також підключені роутери Cisco SB RV215W-E-K9-G5-RF для внутрішнього використання пристроїв, які не матимуть доступ в мережу підприємства. Наприклад, для працівників складських приміщень, або підсобників, які будуть вести облік на підприємстві.

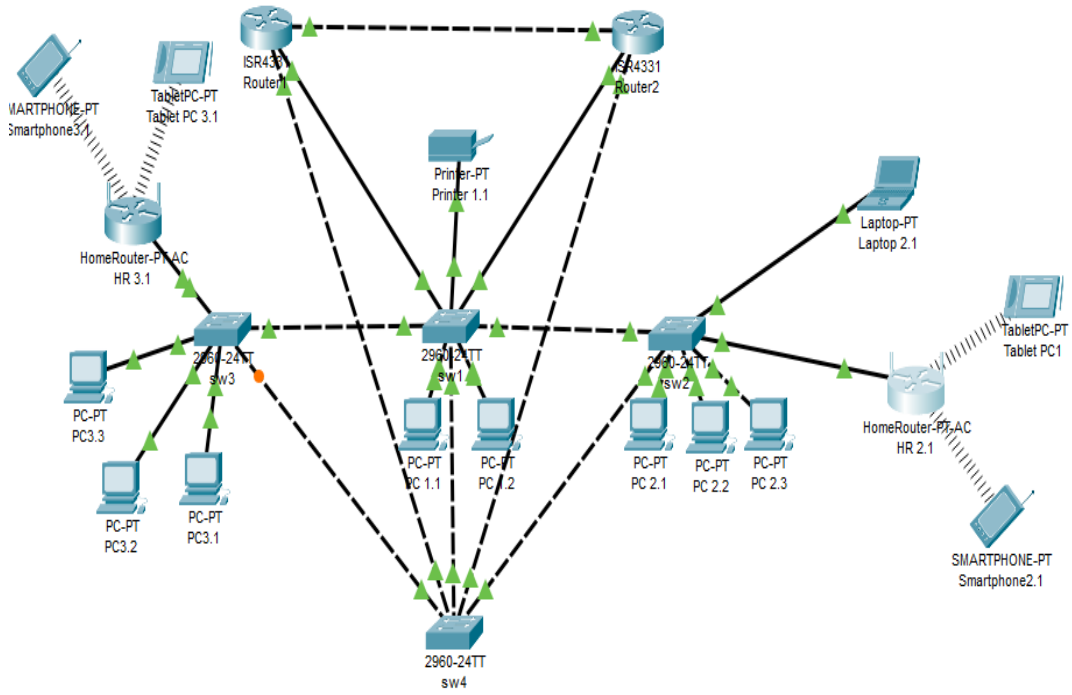

Рис. 3.1. Топологія підприємства

ВИСНОВКИ

В ході виконання дипломного проекту були вирішені завдання побудови корпоративної мережі малого підприємства із застосуванням технологій VLAN, STP, EIGRP, LAN

1. Виконано аналіз існуючих мереж, в ході якого було вирішено вибрати топологію побудування мережі “Зірка”

2. Проведено теоретичне ознайомлення з технологіями, які застосовуються при побудові корпоративної мережі, можливості реалізації, тенденції розвитку, її переваги та недоліки.

3. Була побудована функціональна модель корпоративної мережі програмі Cisco Packet Tracer, де були використані моделі справжнього обладнання, якими користуються компанії по всьому світу.

4. Проведено конфігурацію маршрутизаторів, а саме було налаштовано протокол маршрутизації з клієнтом.

5. Налаштовано EIGRP всередині мережі провайдера, в якості протоколу маршрутизації для VLAN; налаштовано VLAN Spanning Tree (PVST), що призначений для роботи з декількома VLAN.

Мережі, побудовані для авіакомпаній на базі обладнання Cisco, є добре організованими та надійними. Використання обладнання Cisco забезпечує високу продуктивність, безпеку та масштабованість мережі.

Обладнання Cisco відоме своєю високою якістю, передовими технологіями та широким спектром можливостей. Воно дозволяє ефективно управляти мережами, забезпечуючи надійне з'єднання та оптимальну пропускну здатність.

Мережеві конфігурації на базі обладнання Cisco дозволяють ефективно розподіляти трафік, управляти багаторівневими протоколами, використовувати віртуалізацію та захищати мережу від потенційних загроз.

Крім того, обладнання Cisco надає доступ до широкого спектру підтримки та послуг, включаючи технічну підтримку, оновлення програмного забезпечення та консультації фахівців.

Загалом, мережа на базі обладнання Cisco є надійною, ефективною та масштабованою і здатна задовольнити потреби авіакомпаній у надійному та безперебійному зв'язку та обміні даними.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Побудова корпоративних мереж передачі даних - 2019 - Режим доступу: https://www.telesphera.net/blog/corporate-networking.html
2. Особливості побудови і використання сучасних корпоративних комп'ютерних мереж - 2017 - Режим доступу: https://conferences.vntu.edu.ua/public/files/1/fitki_2017_netpub.pdf
3. Корпоративна мережа - 2019 - Режим доступу: http://surl.li/iaybm
4. Принципи побудови і призначення комп'ютерних мереж - 2019 - Режим доступу: http://surl.li/iadst
5. Загальні принципи побудови корпоративної мережі - 2020 Режим доступу: - https://studfile.net/preview/5470625/
6. How a VPN (Virtual Private Network) Works - 2021 - Режим доступу: https://computer.howstuffworks.com/vpn.htm
7. Як не заплутатися у дротах. Типи мережевих кабелів – 2023 - Режим доступу: https://maxnet.ua/blog/kak-ne-zaputatsya-v-provodakh-tipy-setevykh-kabeley/
8. Як не заплутатися у дротах. Типи мережевих кабелів - 2022 - Режим доступу: https://maxnet.ua/blog/kak-ne-zaputatsya-v-provodakh-tipy-setevykh-kabeley/
9. У чому відмінність "білої" та "сірої" IP-адреси? - 2019 - Режим доступу: http://surl.li/iadsh
10. Cybersecurity, everywhere you need it - 2023 - Режим доступу: https://www.fortinet.com/
11. Signed Syslog Messages - 2010 - Режим доступу: https://datatracker.ietf.org/doc/html/rfc5848
12. Polo Alto - 2019 - Режим доступу: https://techexpert.ua/it-products/palo-alto/

13. Cisco UCS B200 M5 Blade Server Data Sheet - 2023 - Режим доступу: https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-b-series-blade-servers/datasheet-c78-739296.html
14. Gigabit Ethernet - 2016 - Режим доступу: https://wiki.cuspu.edu.ua/index.php/Gigabit_Ethernet
15. Cisco ISR4331-SEC/K9 - 2023 - Режим доступу: https://itel.ua/ru/isr4331-seck9
16. Cisco Cisco Catalyst 2960 - 2023 - Режим доступу: https://itel.ua/ua/isr4331-seck9