**Міністерство освіти і науки України**

**Луцький національний технічний університет**
(повне найменування закладу вищої освіти)

**Факультет комп'ютерних та інформаційних технологій**
(повне найменування факультету)

**Кафедра комп'ютерної інженерії та кібербезпеки**
(повне найменування кафедри)

# КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

## КОРПОРАТИВНА МЕРЕЖА КОВЕЛЬСЬКОЇ ФІЛІЇ ВОДОКАНАЛУ
## CORPORATE NETWORK OF THE KOVELSK BRANCH OF THE WATER VODOKANAL

спеціальність 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи КІс-21
Гаврилюк Владислав Володимирович

(підпис)

Керівник:
д.пед.н., професор
Чернящук Наталія Леонідівна

(підпис)

Кваліфікаційну роботу
допущено до захисту
« 07 » червня 2024 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2024 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерних та інформаційних технологій*
Кафедра *комп'ютерної інженерії та кібербезпеки*
Ступінь вищої освіти: *бакалавр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *123 Комп'ютерна інженерія*
Освітня програма: *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ проф. Н.Чернящук
« 10 » 01 2024 р.

# ЗАВДАННЯ
# НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

*Гаврилюку Владиславу Володимировичу*
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Корпоративна мережа Ковельської філії Водоканалу*

Керівник роботи *д.пед.н., професор Чернящук Наталія Леонідівна*

затверджені наказом закладу вищої освіти від «30» грудня 2023 року № 459/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 11.06.2024р.

*3.* Вихідні дані до роботи *Джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області та різні інтернет-ресурси технічного спрямування*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
*Вступ*
*Постановка задачі та огляд систем*
*Огляд технологій*
*Програмна реалізація та отримані результати*
*Висновки*

5. Перелік графічного (ілюстративного) матеріалу:
*Концепція захисту даних інформації*
*Демілітаризована зона*
*Зображення захисту комп'ютерної мережі*
*Зображення роботи сервера*
*Firewalls та захист мережі*
*Зображення корпоративної мережі водоканалу*

6. Консультанти розділів роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| *Аналіз проблеми за темою роботи та постановка завдань дослідження* | *Чернящук Н.Л., професор* | | |
| *Теоретичне дослідження та практична реалізація* | *Чернящук Н.Л., професор* | | |
| *Практична реалізація об'єкта проектування* | *Чернящук Н.Л., професор* | | |
| *Нормоконтроль* | *Багнюк Н.В., доцент* | | |
| *Гарант ОП* | *Лавренчук С.В., доцент* | | |
| *Показник запозичень тексту* | ***___%*** | | |
| *Академічна доброчесність* | *Міскевич О.І.,асистент* | | |

7. Дата видачі завдання 10.01.2024 р.

КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1. | *Розділ 1. Огляд літератури із досліджуваної проблеми. Проектування корпоративної мережі* | до 15.02.2024 р. | Виконано |
| 2. | *Розділ 2. Системи захисту комп'ютерної мережі* | до 15.03.2024 р. | Виконано |
| 3. | *Розділ 3. Проект корпоративної мережі Ковельської філії Водоканалу* | до 04.05.2024 р. | Виконано |
| 4. | *Висновки та пропозиції* | до 07.05.2025 р. | Виконано |
| 5. | *Формування списку використаних джерел* | до 10.05.2024 р. | Виконано |
| 6. | *Формування додатків* | до 15.05.2024 р. | Виконано |
| 7. | *Оформлення ілюстративного матеріалу* | до 20.05.2024 р. | Виконано |
| 8. | *Нормоконтроль* | до 01.06.2024 р. | Виконано |
| 9. | *Інструментальна перевірка на академічний плагіат* | до 04.06.2024 р | Виконано |
| 10. | *Представлення кваліфікаційної роботи бакалавра до захисту* | до 11.06.2024 р. | Виконано |

**Здобувач вищої освіти** _____ Гаврилюк В.В.
(підпис) (прізвище, ініціали)

**Керівник кваліфікаційної роботи** _____ Чернящук Н.Л.
(підпис) (прізвище, ініціали)

# АНОТАЦІЯ

Гаврилюк В.В. Корпоративна мережа Ковельської філії Водоканалу. Рукопис.

Кваліфікаційна робота бакалавра ОП «Комп'ютерна інженерія» спеціальності 123 Комп'ютерна інженерія. Луцький національний технічний університет. Луцьк, 2024.

Кваліфікаційна робота складається з вступу, трьох розділів, висновків, списку використаних джерел, трьох додатків.

Метою роботи є розробка ефективної, безпечної корпоративної мережі з урахуванням конкретних потреб Ковельської філії Водоканалу.

Завдання кваліфікаційної роботи бакалавра:

– визначити вимоги та потреби водоканалу щодо мережі;

– здійснити проектування корпоративної мережі, включаючи розташування пристроїв, сегментацію мережі, протоколи комутації та маршрутизації;

– здійснити вибір потрібного обладнання для реалізації архітектури та її налаштування з урахуванням потреб водоканалу.

Об'єктом дослідження – корпоративна мережа Ковельської філії Водоканалу.

Предметом дослідження – корпоративна мережа Ковельської філії Водоканалу 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. Розроблено структурну схему, фізичну й логічну топологію, схему з'єднань й IP – адресації цієї мережі, здійснено конфігурування пристроїв та моделювання роботи мережі у середовищі Cisco Packet Tracer.

Ключові слова: корпоративна мережа, Cisco Packet Tracer, Network Address Translation, LAN/WAN.

# ANNOTATION

Gavrilyuk V.V. Corporate network of the Kovel branch of Vodokanal. Manuscript.

Bachelor's qualification thesis of the OP "Computer Engineering" specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2024.

The qualification work consists of an introduction, three sections, conclusions, a list of used sources, and three appendices.

The purpose of the work is to develop an effective, secure corporate network taking into account the specific needs of the Kovel branch of Vodokanal.

Tasks of the bachelor's qualification work:

– determine the requirements and needs of the water utility regarding the network;

– carry out the design of the corporate network, including the location of devices, network segmentation, switching and routing protocols;

– choose the necessary equipment for the implementation of the architecture and its configuration, taking into account the needs of the water utility.

The object of the research is the corporate network of the Kovel branch of Vodokanal.

The subject of the study is the corporate network of the Kovel branch of Vodokanal based on Cisco equipment.

Research methods. An audit of the network infrastructure was carried out, further virtualization of the network is possible, its monitoring, later, if necessary, traffic analysis, variations of network security testing.

Practical significance of the obtained results. The structural diagram, physical and logical topology, connection diagram and IP addressing of this network were developed, devices were configured and the network was modeled in the Sisso Rasket Tracer environment.

Keywords: corporate network, Sisso Rasket Tracer, Network Address Translation, LAN/WAN.

**ЗМІСТ**

# ВСТУП

Актуальність теми корпоративної мережі Ковельської філії Водоканалу обумовлена низкою факторів, які впливають на ефективність та якість роботи. Сучасна корпоративна мережа дозволяє автоматизувати багато процесів, що зменшує людський фактор і помилки, а також підвищує швидкість обробки даних та прийняття рішень. Наявність надійної мережевої інфраструктури важлива для захисту даних від несанкціонованого доступу, кібератак та втрат інформації. Це критично для підприємства, яке працює з великою кількістю конфіденційної інформації. Інтеграція сучасних технологій у корпоративну мережу дозволяє зменшити операційні витрати, зокрема за рахунок зниження потреби в паперовому документообігу та ручних процесах. Мережа сприяє ефективнішій комунікації між співробітниками, відділами та з іншими філіями підприємства, що полегшує обмін інформацією та координацію діяльності. З розвитком інформаційних технологій постійно з'являються нові можливості для підвищення ефективності роботи. Корпоративна мережа є платформою для впровадження таких інновацій, як Інтернет речей (IoT), великі дані (Big Data), хмарні обчислення тощо. Наявність сучасної мережевої інфраструктури допомагає підприємству відповідати вимогам законодавства та галузевим стандартам, що регулюють зберігання та обробку даних.

Зручний доступ до інформації та автоматизація процесів дозволяє швидше і якісніше обслуговувати клієнтів, що підвищує їх задоволеність і лояльність до підприємства.

Враховуючи ці аспекти, модернізація та розвиток корпоративної мережі Ковельської філії Водоканалу є необхідними для забезпечення стабільної та ефективної роботи підприємства, а також для підтримки його конкурентоспроможності в умовах сучасного ринку.

Метою роботи є розробка та впровадження ефективної, надійної та безпечної корпоративної мережі Ковельської філії Водоканалу. Для досягнення мети потрібно виконати ряд завдань:

– оптимізувати внутрішні процеси та комунікації для забезпечення ефективного управління та координації роботи філії;

– розробити та впровадити заходи з кібербезпеки для захисту конфіденційної інформації та запобігання несанкціонованому доступу;

– впровадити автоматизовані системи управління для зменшення кількості ручної роботи та підвищення точності виконання завдань;

– використовувати новітні технології (хмарні сервіси, Інтернет речей (IoT), великі дані) для покращення роботи мережі та надання додаткових можливостей для аналізу і управління;

– забезпечити відповідність роботи корпоративної мережі всім необхідним законодавчим вимогам та стандартам галузі;

– створення стабільної та надійної мережевої інфраструктури, яка забезпечить безперебійне функціонування філії в будь-яких умовах.

Об’єктом дослідження – корпоративна мережа Ковельської філії Водоканалу.

Предметом дослідження – корпоративна мережа Ковельської філії Водоканалу на базі обладнання Cisco.

Практичне значення отриманих результатів дослідження корпоративної мережі Ковельської філії Водоканалу полягає в автоматизації та оптимізації робочих процесів, що зменшить час на виконання завдань, дозволить підвищити продуктивність праці співробітників, зменшення кількості помилок та повторної роботи завдяки більш точному і швидкому обміну інформацією.

# РОЗДІЛ 1
# ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ

## 1.1 Функції корпоративних мереж

Корпоративні мережі (КМ) є важливими для забезпечення ефективної роботи організацій. Вони поєднують різні компоненти інформаційної інфраструктури та надають доступ до спільних ресурсів. Давайте розглянемо функції, принципи побудови та основні можливості корпоративних мереж.

Функції корпоративних мереж. Комунікація та співпраця. Забезпечення внутрішньої та зовнішньої комунікації через електронну пошту, миттєві повідомлення, відеоконференції та інші засоби зв'язку. Підтримка колективної роботи через спільні документи, бази даних та програми.

Спільне використання ресурсів. Надання доступу до принтерів, сканерів та інших периферійних пристроїв. Спільне використання програмного забезпечення та додатків.

Забезпечення безпеки. Реалізація механізмів контролю доступу, автентифікації та шифрування даних. Моніторинг та захист від несанкціонованих доступів і кібератак. Централізоване управління та адміністрування. Керування користувачами та пристроями з єдиного центру. Здійснення централізованого оновлення та підтримки систем. Доступ до Інтернету та зовнішніх мереж. Забезпечення доступу до Інтернету для всіх користувачів мережі. Організація захищеного доступу до зовнішніх ресурсів через VPN. Принципи побудови корпоративних мереж. Модульність. Корпоративна мережа повинна складатися з модулів, які легко доповнюються та модернізуються. Масштабованість. Мережа повинна бути здатною до розширення без значних змін у її структурі. Надійність та відмовостійкість. Використання резервних каналів зв'язку та дублювання критичних компонентів для забезпечення безперервної роботи.

Безпека. Реалізація багаторівневої системи безпеки, що включає фізичну безпеку, мережеві заходи безпеки, антивірусний захист та системи виявлення вторгнень.

Продуктивність. Забезпечення необхідної пропускної здатності та швидкості передачі даних для підтримки вимог бізнесу. Простота адміністрування. Інтуїтивно зрозумілий інтерфейс для адміністраторів мережі та можливість автоматизації рутинних задач. Основні можливості корпоративних мереж. Інтеграція різноманітних систем. Об'єднання різних інформаційних систем та платформ в єдину мережу для спрощення обміну даними. Віртуалізація ресурсів. Використання віртуальних машин та контейнерів для підвищення ефективності використання серверних ресурсів. Хмарні сервіси. Інтеграція з хмарними платформами для зберігання даних та запуску додатків. Підтримка мобільності. Надання безпечного доступу до корпоративної мережі для віддалених та мобільних працівників. Багаторівнева безпека. Впровадження комплексних рішень для захисту від загроз на всіх рівнях мережі. Аналітика та моніторинг. Використання інструментів для моніторингу мережевого трафіку, аналізу продуктивності та виявлення аномалій.

Корпоративні мережі є основою для забезпечення ефективного обміну інформацією та ресурсами в організації. Їх функції та можливості дозволяють забезпечити надійну, масштабовану та безпечну інформаційну інфраструктуру, що відповідає потребам сучасного бізнесу. Принципи побудови таких мереж допомагають створити систему, яка легко адаптується до змін та розвитку організації.

Корпоративні мережі (КМ) є важливими інструментами для забезпечення ефективної взаємодії, комунікації та управління інформацією всередині організацій. Вони складаються з різних апаратних і програмних компонентів, які забезпечують підключення, передачу даних та управління мережею. Основні функції та принципи побудови корпоративних мереж, а також їх основні можливості можна охарактеризувати наступним чином.

Функції корпоративних мереж. Комунікація та співпраця. Email та месенджери. забезпечують обмін інформацією між працівниками. Відеоконференції та голосовий зв’язок. сприяють проведенню віддалених зустрічей та нарад. Спільний доступ до файлів. дозволяє співробітникам працювати над документами разом у реальному часі. Управління даними. Централізоване зберігання даних. полегшує доступ та управління інформацією. Системи управління базами даних. дозволяють ефективно зберігати та обробляти великі обсяги інформації. Безпека. Аутентифікація та авторизація. забезпечують доступ до ресурсів тільки авторизованим користувачам. Шифрування даних. захищає інформацію під час передачі через мережу. Мережеві екрани та антивірусні програми. забезпечують захист від кіберзагроз. Управління та моніторинг. Моніторинг мережевої активності. дозволяє відстежувати роботу мережі в режимі реального часу. Управління трафіком. оптимізує використання мережевих ресурсів. Підтримка додатків. Хостинг веб-додатків. забезпечує роботу внутрішніх та зовнішніх веб-сервісів. Підтримка корпоративних інформаційних систем. таких як ERP та CRM. Принципи побудови корпоративних мереж. Модульність та масштабованість. Корпоративна мережа повинна мати можливість розширення та зміни конфігурації без значних зусиль та витрат. Відмовостійкість та надійність. Використання резервних компонентів та дублювання критичних елементів для забезпечення безперебійної роботи. Безпека. Впровадження багаторівневої системи захисту, що включає фізичну безпеку, захист мережевих пристроїв та захист даних. Продуктивність. Забезпечення високої пропускної здатності та низької затримки для критичних додатків. Уніфікація та стандартизація. Використання стандартних протоколів та технологій для забезпечення сумісності між різними компонентами мережі. Основні можливості корпоративних мереж. Віртуалізація. Використання віртуальних серверів та мереж для оптимізації ресурсів та зниження витрат.

Хмарні сервіси. Інтеграція з хмарними платформами для підвищення гнучкості та масштабованості IT-інфраструктури. Інтернет речей (IoT).

Підключення та управління IoT пристроями для збору даних та автоматизації бізнес-процесів. Аналіз великих даних.

Використання аналітичних інструментів для обробки та аналізу великого обсягу інформації. Мобільність. Забезпечення доступу до корпоративних ресурсів з будь-якого місця та будь-якого пристрою. Корпоративні мережі відіграють критичну роль у функціонуванні сучасних організацій, забезпечуючи ефективну комунікацію, безпеку та управління даними. Впровадження новітніх технологій та принципів побудови мереж дозволяє підприємствам адаптуватися до змін та забезпечувати стабільний розвиток.

## 1.2 Корпоративні мережі та їх переваги

Корпоративні мережі (КМ) пропонують численні переваги для організацій, що використовують їх для підвищення ефективності, безпеки та комунікації. Основні переваги корпоративних мереж можна розподілити на кілька ключових аспектів. Переваги корпоративних мереж. Покращена комунікація та співпраця.

Швидкий доступ до інформації. Співробітники можуть обмінюватися інформацією та файлами в реальному часі. Інтеграція комунікаційних засобів. Використання електронної пошти, месенджерів, відеоконференцій та інших засобів комунікації в єдиній системі. Зручність спільної роботи. Можливість одночасної роботи над документами та проектами з будь-якої точки світу. Ефективне управління ресурсами. Централізоване управління. Можливість централізованого управління ресурсами, такими як сервери, сховища даних та мережеве обладнання. Оптимізація використання ресурсів. Віртуалізація та хмарні технології дозволяють зменшити витрати на фізичну інфраструктуру та підвищити ефективність використання ресурсів.

Підвищена безпека. Захист даних. Використання шифрування, брандмауерів та інших засобів захисту для забезпечення безпеки даних. Аутентифікація та авторизація. Забезпечення доступу до корпоративних ресурсів лише авторизованим користувачам.

Моніторинг та виявлення загроз. Постійний моніторинг мережевої активності для виявлення та реагування на потенційні загрози. Масштабованість та гнучкість. Легке розширення. Можливість додавання нових користувачів, пристроїв та додатків без значних змін у структурі мережі. Адаптація до змін. Швидке впровадження нових технологій та адаптація до змін у бізнес-процесах. Підвищена продуктивність. Висока пропускна здатність. Забезпечення швидкої передачі даних та стабільної роботи додатків. Зниження затримок. Оптимізація мережевих маршрутів та використання сучасних протоколів для зниження затримок. Зручність управління та адміністрування.

Автоматизація. Використання автоматизованих інструментів для управління та моніторингу мережі. Централізоване адміністрування. Спрощення управління мережею за допомогою централізованих систем контролю та управління.

Інновації та конкурентоспроможність. Впровадження нових технологій. Можливість швидкого впровадження інновацій, таких як Інтернет речей (IoT), великі дані та штучний інтелект. Покращення бізнес-процесів. Оптимізація та автоматизація бізнес-процесів завдяки інтеграції сучасних технологій. Корпоративні мережі надають компаніям широкі можливості для підвищення ефективності, безпеки та продуктивності. Вони сприяють покращенню комунікацій та співпраці між працівниками, забезпечують централізоване управління ресурсами, підвищують рівень безпеки та забезпечують гнучкість і масштабованість. Це робить їх незамінним інструментом для сучасних організацій, які прагнуть залишатися конкурентоспроможними та інноваційними.

Корпоративні мережі (КМ) надають організаціям численні переваги, які сприяють підвищенню ефективності, продуктивності та безпеки бізнес-процесів. Основні переваги корпоративних мереж можна виділити наступним чином.

1. Підвищення продуктивності. Спільний доступ до ресурсів. Співробітники можуть одночасно працювати з одними й тими самими файлами та додатками, що сприяє командній роботі та швидкому виконанню

завдань. Автоматизація процесів. Використання корпоративних мереж дозволяє автоматизувати рутинні завдання, що знижує витрати часу та підвищує ефективність.

2. Покращення комунікації. Швидкий обмін інформацією. Корпоративні мережі забезпечують миттєвий обмін даними між співробітниками через електронну пошту, месенджери та інші комунікаційні засоби. Відеоконференції та колективна робота. Інструменти для відеозв'язку та спільної роботи дозволяють проводити наради та обговорення незалежно від географічного розташування працівників.

3. Централізоване управління даними. Єдиний центр зберігання. Всі дані зберігаються в централізованому сховищі, що полегшує їх доступ та управління. Бекап та відновлення. Корпоративні мережі забезпечують регулярне резервне копіювання даних, що знижує ризик їх втрати.

4. Підвищення безпеки. Контроль доступу. Мережі дозволяють встановлювати правила доступу до інформації та ресурсів, забезпечуючи захист від несанкціонованого доступу. Моніторинг та аудит. Системи моніторингу та аудиту дозволяють відстежувати активність користувачів та виявляти підозрілі дії.

5. Гнучкість та масштабованість. Масштабованість. Корпоративні мережі легко масштабуються під потреби бізнесу, дозволяючи додавати нові користувачі та ресурси без значних витрат. Віртуалізація. Використання віртуальних мереж та серверів дозволяє ефективно використовувати ресурси та швидко адаптуватися до змін.

6. Економія витрат. Зниження витрат на IT. Завдяки централізованому управлінню та автоматизації процесів, знижуються витрати на обслуговування та підтримку IT-інфраструктури. Оптимізація ресурсів. Ефективне використання мережевих та обчислювальних ресурсів дозволяє зменшити витрати на обладнання та енергію.

7. Інтеграція з хмарними сервісами. Доступ до хмарних рішень. Інтеграція з хмарними платформами дозволяє використовувати додаткові сервіси та

ресурси, знижуючи навантаження на локальну інфраструктуру. Віддалений доступ. Співробітники можуть отримувати доступ до корпоративних ресурсів з будь-якого місця, що підвищує гнучкість роботи.

8. Покращення управління бізнес-процесами. ERP та CRM системи. Інтеграція корпоративних мереж з ERP та CRM системами дозволяє автоматизувати та оптимізувати бізнес-процеси, покращуючи управління ресурсами та відносинами з клієнтами. Аналітика та звітність. Сучасні корпоративні мережі надають інструменти для збору та аналізу даних, що допомагає у прийнятті обґрунтованих рішень.

9. Підтримка мобільності. Мобільний доступ. Співробітники можуть працювати з мобільних пристроїв, що забезпечує гнучкість і мобільність роботи. Підтримка BYOD. Підтримка концепції Bring Your Own Device (BYOD) дозволяє працівникам використовувати особисті пристрої для роботи, що підвищує їх задоволеність та продуктивність.

10. Підтримка інновацій. Впровадження нових технологій. Корпоративні мережі дозволяють швидко впроваджувати нові технології та інновації, такі як Інтернет речей (IoT), штучний інтелект (AI) та великі дані (Big Data). Корпоративні мережі відіграють ключову роль у сучасному бізнесі, забезпечуючи ефективну комунікацію, управління даними та безпеку. Вони сприяють підвищенню продуктивності, економії витрат та підтримці інновацій, що є критично важливим для успіху в конкурентному середовищі.

### 1.3 Побудова корпоративних мереж

Концепція корпоративної мережі охоплює планування, розробку, впровадження та підтримку інтегрованої мережевої інфраструктури, яка забезпечує безперебійну комунікацію, ефективне управління даними та надійний захист інформації всередині організації. Розглянемо основні аспекти цієї концепції. Основні компоненти корпоративної мережі. Мережеве обладнання.

Комутатори (Switches). Забезпечують з’єднання пристроїв в локальній мережі (LAN). Маршрутизатори (Routers). Підключають локальні мережі до зовнішніх мереж, таких як Інтернет. Точки доступу (Access Points). Забезпечують бездротове підключення пристроїв.

Програмне забезпечення. Операційні системи та мережеві служби. Керують роботою серверів та робочих станцій. Мережеві протоколи. Забезпечують стандартизоване обмін даними (TCP/IP, DNS, DHCP).

Інфраструктура зберігання даних. Сервери та сховища даних (NAS, SAN). Центральні елементи для зберігання та обробки даних. Системи резервного копіювання. Забезпечують збереження копій важливих даних.

Системи безпеки. Мережеві екрани (Firewalls). Захищають мережу від зовнішніх загроз. Системи виявлення та запобігання вторгнень (IDS/IPS). Виявляють та реагують на підозрілу активність. Антивірусне ПЗ та засоби шифрування. Захищають від шкідливого ПЗ та несанкціонованого доступу.

Архітектура корпоративної мережі. Core Layer (Ядро). Центральний рівень мережі, який забезпечує високу швидкість та надійність передачі даних між різними сегментами мережі. Distribution Layer (Розподільчий шар). Відповідає за обробку трафіку, політики безпеки та управління трафіком між різними підмережами. Access Layer (Рівень доступу). Підключає кінцеві пристрої (комп’ютери, принтери) до мережі. Принципи побудови корпоративної мережі

Модульність. Забезпечення можливості розширення та зміни мережі без значних витрат та перебоїв у роботі. Надійність та відмовостійкість. Використання резервних компонентів та шляхів для зменшення ризику збоїв. Безпека. Реалізація багаторівневого підходу до захисту даних та мережевої інфраструктури. Продуктивність. Оптимізація пропускної здатності та мінімізація затримок для забезпечення високої якості обслуговування. Масштабованість. Легке додавання нових користувачів, пристроїв та додатків з мінімальними зусиллями. Основні можливості корпоративних мереж. Інтеграція та уніфікація. Інтеграція різних IT-систем та додатків для забезпечення єдиного

інформаційного простору. Підтримка хмарних сервісів. Використання хмарних рішень для зберігання даних, обчислень та забезпечення віддаленого доступу. Підтримка мобільності. Забезпечення доступу до корпоративних ресурсів з будь-якого місця та з будь-якого пристрою.

Автоматизація управління. Використання систем моніторингу та управління для автоматизації процесів обслуговування та адміністрування мережі. Аналітика та звітність. Збір та аналіз даних про мережеву активність для підвищення ефективності та прийняття обґрунтованих рішень. Переваги корпоративних мереж. Підвищення продуктивності та ефективності роботи співробітників. Забезпечення надійного та безпечного зберігання та обробки даних. Економія витрат на IT-інфраструктуру та її обслуговування. Підтримка інновацій та гнучкість у впровадженні нових технологій. Покращення комунікації та співпраці між співробітниками. Корпоративна мережа є фундаментальною складовою сучасної організації, забезпечуючи ефективну взаємодію, безпеку та управління ресурсами. Її правильне проектування та впровадження дозволяє компаніям ефективно функціонувати, швидко адаптуватися до змін та зберігати конкурентоспроможність.

Корпоративна мережа (КМ) – це інтегрована система інформаційних і комунікаційних технологій, яка забезпечує обмін даними, ресурси та послуги всередині організації. Концепція корпоративної мережі включає різні аспекти, такі як архітектура, функціональність, безпека та управління. Основними елементами концепції корпоративної мережі є наступні.

1. Архітектура корпоративної мережі. Фізична інфраструктура. Мережеве обладнання. маршрутизатори, комутатори, сервери, точки доступу. Кабельні системи. оптичні волокна, мідні кабелі (Ethernet), бездротові з’єднання (Wi-Fi). Дата-центри. приміщення для розміщення серверного обладнання та зберігання даних. Логічна інфраструктура. Локальна мережа (LAN). мережа всередині однієї локації або офісу. Регіональна мережа (MAN). мережа, що охоплює кілька близько розташованих локацій. Глобальна мережа (WAN). мережа, що об’єднує різні регіональні мережі та офіси, розташовані в різних частинах світу.

Віртуальні приватні мережі (VPN). безпечні з’єднання через інтернет для доступу до корпоративних ресурсів.

2. Функціональність корпоративної мережі. Комунікаційні послуги. Електронна пошта та месенджери. для обміну повідомленнями між співробітниками. Відеоконференції та VoIP. для проведення віддалених зустрічей та дзвінків. Спільне використання ресурсів. Файлові сервери. для централізованого зберігання та доступу до документів. Принт-сервіси. для спільного використання принтерів та сканерів. Доступ до додатків та послуг. Корпоративні додатки. ERP, CRM, HRM системи для управління бізнес-процесами. Хмарні сервіси. інтеграція з хмарними платформами для додаткових можливостей.

3. Безпека корпоративної мережі. Аутентифікація та авторизація. Використання багатофакторної аутентифікації (MFA) для підвищення безпеки доступу. Розмежування прав доступу на основі ролей (RBAC). Захист даних. Шифрування даних при передачі та зберіганні. Використання VPN для захисту даних при віддаленому доступі. Моніторинг та виявлення загроз. Системи виявлення вторгнень (IDS/IPS). Антивірусні та антималварні програми для захисту від шкідливого ПЗ.

4. Управління корпоративною мережею. Моніторинг мережі. Постійний моніторинг стану мережі та її компонентів для забезпечення стабільної роботи. Використання спеціалізованих інструментів та програм для відстеження продуктивності та виявлення проблем. Адміністрування. Управління користувачами та їхніми правами доступу. Налаштування мережевих пристроїв та політик безпеки. Планування та масштабування. Прогнозування навантаження на мережу та планування її розширення. Впровадження нових технологій та оновлення обладнання для підтримки сучасних вимог.

5. Підтримка мобільності та віддаленого доступу. Підтримка BYOD (Bring Your Own Device). Надання безпечного доступу до корпоративних ресурсів з особистих пристроїв співробітників. Мобільні додатки. Розробка та використання мобільних додатків для доступу до корпоративних систем та

сервісів. Віртуальні робочі місця (VDI). Використання технологій віртуальних робочих місць для забезпечення віддаленої роботи. Корпоративна мережа є критично важливим елементом сучасної організації, що забезпечує ефективну комунікацію, управління інформацією та безпеку даних. Впровадження та підтримка корпоративної мережі вимагає ретельного планування, використання передових технологій та постійного моніторингу для забезпечення її стабільної та безпечної роботи.

## 1.4 Основні функції корпоративної мережі

Корпоративна мережа (КМ) має важливе призначення для сучасних організацій, оскільки вона забезпечує основу для інтеграції різних технологічних рішень та бізнес-процесів. Основні призначення корпоративної мережі включають.

1. Забезпечення комунікації та співпраці. Внутрішня комунікація. КМ забезпечує швидку та ефективну комунікацію між співробітниками через електронну пошту, миттєві повідомлення, відеоконференції та внутрішні соціальні мережі. Спільна робота. Забезпечення можливості для співробітників працювати разом над документами та проектами в режимі реального часу, незалежно від їх фізичного місцезнаходження.

2. Централізоване управління та зберігання даних. Єдиний центр зберігання. Корпоративна мережа надає централізоване сховище для даних, що полегшує доступ та управління інформацією. Бекап та відновлення. Автоматизовані системи резервного копіювання та відновлення даних для захисту від втрат інформації.

3. Безпека інформації. Контроль доступу. Впровадження механізмів аутентифікації та авторизації для захисту даних та ресурсів від несанкціонованого доступу. Шифрування даних. Захист даних під час їх передачі через мережу та під час зберігання.

4. Підтримка бізнес-процесів. Інтеграція корпоративних додатків. Підтримка роботи систем управління підприємством (ERP), управління відносинами з клієнтами (CRM) та інших критично важливих бізнес-додатків. Автоматизація процесів. Автоматизація рутинних операцій та оптимізація бізнес-процесів для підвищення ефективності.

5. Оптимізація ресурсів. Мережеве управління. Централізоване управління мережевими ресурсами для забезпечення їх ефективного використання та швидкого реагування на зміни. Масштабованість. Можливість легко розширювати мережу для підтримки зростання бізнесу та впровадження нових технологій.

6. Підтримка мобільності та віддаленої роботи. Віддалений доступ. Забезпечення безпечного доступу до корпоративних ресурсів з будь-якої точки світу через VPN та інші технології. Мобільні рішення. Інтеграція мобільних пристроїв та додатків для забезпечення продуктивності співробітників у дорозі.

7. Інтеграція з хмарними сервісами. Хмарні рішення. Використання хмарних платформ для зберігання даних, хостингу додатків та надання інших сервісів, що дозволяє знизити витрати на власну інфраструктуру. Гібридні рішення. Інтеграція локальних ресурсів з хмарними для забезпечення гнучкості та надійності.

8. Підтримка інновацій та розвитку. Впровадження нових технологій. Здатність швидко впроваджувати нові технології, такі як Інтернет речей (IoT), штучний інтелект (AI) та аналіз великих даних (Big Data). Адаптивність. Гнучкість мережевої інфраструктури для адаптації до змін у бізнес-середовищі та нових вимог. Корпоративна мережа є невід'ємною частиною сучасного бізнесу, яка підтримує комунікацію, безпеку, ефективність та інноваційність. Вона забезпечує основу для інтеграції різних технологічних рішень та бізнес-процесів, сприяючи досягненню стратегічних цілей організації. Корпоративна мережа (КМ) має різноманітне призначення, що охоплює кілька ключових аспектів функціонування сучасної організації. Вона забезпечує

комунікацію, управління даними, безпеку та підтримку різних бізнес-процесів. Основні призначення корпоративної мережі можна розділити на кілька категорій.

1. Комунікація та співпраця. Забезпечення внутрішньої комунікації. Електронна пошта та миттєві повідомлення. для швидкого обміну інформацією між співробітниками. Відеоконференції та телефонія через Інтернет (VoIP) для проведення віддалених зустрічей та конференцій. Спільна робота над проектами. Інструменти для спільного редагування документів. дозволяють кільком користувачам одночасно працювати над одним документом. Системи управління проектами. для координації завдань і відстеження прогресу.

2. Управління інформацією. Централізоване зберігання даних. Файлові сервери та бази даних. забезпечують централізоване зберігання інформації, полегшуючи доступ та управління даними. Обмін даними та інформацією. FTP та внутрішні веб-сервери. для безпечного обміну файлами та інформацією між співробітниками.

3. Забезпечення безпеки. Захист даних та конфіденційності. Шифрування даних. для захисту інформації при передачі та зберіганні. Системи аутентифікації та авторизації. для контролю доступу до ресурсів. Моніторинг та управління загрозами. Мережеві екрани та системи виявлення вторгнень (IDS/IPS). для захисту від кіберзагроз. Антивірусні програми. для захисту від шкідливого програмного забезпечення.

4. Підтримка бізнес-процесів. Інтеграція бізнес-додатків. ERP (Enterprise Resource Planning) системи. для управління ресурсами підприємства. CRM (Customer Relationship Management) системи. для управління відносинами з клієнтами. Автоматизація процесів. Системи управління документами. для автоматизації документообігу. Інструменти для бізнес-аналітики. для аналізу даних та підтримки прийняття рішень.

5. Гнучкість та масштабованість. Підтримка зростання компанії. Масштабованість мережі. забезпечує легке розширення інфраструктури при зростанні бізнесу. Інтеграція нових технологій. дозволяє швидко впроваджувати

нові рішення та інновації. Віддалений доступ та мобільність. Підтримка віддаленої роботи. забезпечує доступ до корпоративних ресурсів з будь-якого місця. Мобільні додатки та VPN. для безпечного підключення до корпоративної мережі з мобільних пристроїв.

6. Оптимізація ресурсів. Ефективне використання апаратних ресурсів. Віртуалізація серверів. дозволяє оптимально використовувати обчислювальні ресурси. Хмарні сервіси. зменшують навантаження на локальну інфраструктуру та забезпечують гнучкість. Зниження витрат. Централізоване управління. знижує витрати на обслуговування та підтримку мережі. Автоматизація управління. зменшує потребу в ручному управлінні та людських ресурсах. Призначення корпоративної мережі включає підтримку ефективної комунікації та співпраці, централізоване управління даними, забезпечення безпеки інформації, підтримку критичних бізнес-процесів, а також забезпечення гнучкості, масштабованості та оптимізації ресурсів. Це дозволяє організаціям ефективно функціонувати, швидко адаптуватися до змін та забезпечувати стабільний розвиток.

### 1.5 Основні етапи створення корпоративної мережі

Процес створення корпоративної інформаційної системи (КІС) є складним та багатоступеневим, який включає планування, розробку, впровадження та підтримку системи. Основні етапи створення КІС можна описати наступним чином.

1. Аналіз вимог. Визначення цілей та завдань. Визначення основних цілей, які повинна досягти інформаційна система (наприклад, підвищення ефективності, автоматизація процесів, поліпшення управління даними). Визначення конкретних завдань для досягнення цих цілей. Збір вимог. Інтерв'ю з ключовими зацікавленими сторонами (керівники відділів, IT-персонал, кінцеві користувачі). Аналіз існуючих бізнес-процесів та визначення їх потреб. Документування функціональних та нефункціональних вимог до системи.

Аналіз вимог. Аналіз зібраних вимог для визначення їх реалістичності та пріоритетності. Виявлення можливих обмежень та ризиків.

2. Планування. Розробка концепції системи. Створення високорівневого опису майбутньої системи. Визначення архітектури системи (модульність, інтеграція з існуючими системами, вибір технологій). Планування ресурсів. Визначення необхідних ресурсів (людських, фінансових, технологічних). Складання бюджету та графіку робіт. Вибір платформи та інструментів. Оцінка та вибір програмного забезпечення та апаратного забезпечення для розробки системи. Вибір методології розробки (наприклад, Agile, Waterfall).

3. Проектування. Розробка технічного завдання (ТЗ). Створення детального ТЗ на основі зібраних вимог. Визначення специфікацій для кожного компонента системи. Створення прототипів. Розробка прототипів інтерфейсу користувача та основних функціональних модулів. Отримання зворотного зв’язку від користувачів щодо прототипів. Проектування бази даних. Створення моделі даних (ER-діаграми). Визначення структури бази даних та зв’язків між таблицями.

4. Розробка. Програмування. Розробка коду для всіх модулів та компонентів системи. Використання інструментів контролю версій (Git, SVN). Інтеграція. Інтеграція всіх компонентів системи. Забезпечення сумісності з існуючими системами та сервісами. Тестування. Модульне тестування (unit testing) кожного окремого модуля. Інтеграційне тестування для перевірки взаємодії між модулями. Системне тестування для перевірки роботи всієї системи в цілому. Тестування продуктивності та безпеки.

5. Впровадження. Підготовка до запуску. Підготовка інфраструктури (сервери, мережеве обладнання). Встановлення та налаштування програмного забезпечення. Навчання користувачів. Проведення тренінгів та семінарів для користувачів системи. Розробка інструкцій та посібників користувача. Запуск системи. Міграція даних з існуючих систем. Виконання перевірки перед запуском (pre-launch testing). Запуск системи в експлуатацію.

6. Підтримка та супровід. Моніторинг та підтримка. Постійний моніторинг роботи системи для виявлення та усунення можливих проблем. Надання технічної підтримки користувачам. Оновлення та вдосконалення. Розробка та впровадження оновлень для покращення функціональності та безпеки. Збір зворотного зв'язку від користувачів для вдосконалення системи. Аудит та оцінка ефективності. Регулярний аудит системи для оцінки її ефективності та відповідності вимогам. Визначення нових потреб та планування подальших поліпшень.

Створення корпоративної інформаційної системи є багатоетапним процесом, що вимагає ретельного планування, аналізу вимог, розробки, впровадження та постійної підтримки. Ключем до успішного впровадження КІС є тісна співпраця з усіма зацікавленими сторонами, а також гнучкість і готовність до адаптації у процесі розвитку проекту.

Віртуальні мережі передачі даних (VPN) – це технологія, що дозволяє створювати безпечне з'єднання між двома або більше пристроями через публічну мережу, таку як Інтернет. Одна з головних переваг VPN полягає в забезпеченні конфіденційності та безпеки передачі даних, оскільки весь трафік між підключеними пристроями шифрується. VPN можна використовувати для різних цілей, таких як. Захист приватності. Всі дані, які ви відправляєте або отримуєте через VPN, шифруються, що ускладнює їх перехоплення та злам. Обхід обмежень. VPN дозволяє обходити географічні обмеження, які можуть бути застосовані до певного контенту або сервісів. Безпечне підключення до віддалених ресурсів. Компанії використовують VPN для безпечного доступу своїх співробітників до внутрішніх мереж з будь-якої точки з'єднання з Інтернетом.

Захист від перехоплення на публічних мережах. Використання VPN на відкритих мережах, таких як кав'ярні або аеропорти, допомагає уникнути ризику перехоплення чутливої інформації. Анонімне перегляд Інтернету. Деякі VPN-сервіси пропонують можливість приховати вашу IP-адресу, забезпечуючи анонімність під час перегляду веб-сторінок. Існують різні види VPN, такі як SSL

VPN, IPSec VPN, та мережі VPN на основі віртуальних тунелів. Кожен з них має свої переваги та обмеження, і вибір конкретної технології залежить від потреб користувача або організації. Віртуальні мережі передачі даних (VPN) – це технологія, яка дозволяє створювати безпечне з'єднання між комп'ютерами чи мережами через публічну мережу, таку як Інтернет. Основна мета VPN полягає у створенні зашифрованого тунелю між двома або більше точками, що забезпечує конфіденційність, цілісність та аутентичність даних, що пересилаються через цей тунель. VPN може бути використана для різних цілей. Забезпечення безпеки. Шифрування даних, що передаються через мережу, захищає їх від несанкціонованого доступу. Забезпечення конфіденційності даних, особливо важливо для бізнесів та осіб, які працюють з конфіденційною інформацією. Забезпечення анонімності. Із використанням VPN можна приховати реальну IP-адресу користувача від веб-сайтів, що дозволяє більш анонімне переглядання Інтернету.

Доступ до обмеженого контенту. VPN може дозволити користувачам отримати доступ до ресурсів, які обмежені за географічним принципом, наприклад, до стрімінгових платформ або веб-сайтів. З'єднання віддалених робочих місць. Корпоративні VPN дозволяють співробітникам підключатися до внутрішньої мережі компанії з будь-якої точки з доступом до ресурсів та даних компанії. Технологія VPN стала надзвичайно популярною в останні роки, особливо серед користувачів, які цінують приватність та безпеку у Інтернеті.

### 1.6 LAN/WAN локальна та глобальна мережі

У сучасних корпоративних мережах використовуються різноманітні технології для забезпечення ефективного обміну даними, забезпечення безпеки, підвищення продуктивності та забезпечення надійності. Ось кілька основних технологій, які широко використовуються в корпоративних мережах. LAN/WAN (локальна та глобальна мережі). Це основний фундамент для з'єднання комп'ютерів та інших пристроїв в межах підприємства та між його різними

розташованими місцями. Ethernet. Стандартна технологія для провідних мереж, яка дозволяє передавати дані між різними пристроями. Wi-Fi. Бездротовий доступ до мережі, який дозволяє пристроям підключатися до мережі без використання кабелів. VPN (віртуальні приватні мережі). Технологія, яка забезпечує безпечний доступ до мережі з віддалених місць через інтернет. Firewalls (брандмауери). Захисні системи, які контролюють трафік у мережі та фільтрують небажаний контент.

Intrusion Detection/Prevention Systems (системи виявлення/попередження вторгнень). Технології, які виявляють та запобігають спробам несанкціонованого доступу до мережі. SD-WAN (мережі з визначенням програмного забезпечення). Технологія, яка дозволяє ефективно керувати трафіком між різними шляхами зв'язку в корпоративних мережах.

Cloud Networking (мережі в хмарі). Використання хмарних послуг для забезпечення мережевої інфраструктури, включаючи зберігання даних та обробку. Unified Communications (єдина система зв'язку). Інтеграція різних комунікаційних засобів, таких як голосова телефонія, відеоконференції та миттєві повідомлення, в одну систему.

Software-Defined Networking (мережі з визначенням програмного забезпечення). Технологія, яка дозволяє програмно керувати та конфігурувати мережеві пристрої, спрощуючи управління мережею. Це лише деякі з основних технологій, що використовуються в корпоративних мережах. Зазвичай компанії використовують комбінацію цих технологій для створення надійної, безпечної та продуктивної мережевої інфраструктури. Корпоративні мережі використовують широкий спектр технологій для забезпечення надійного, безпечного та ефективного обміну даними та комунікації між різними вузлами в межах організації. Ось деякі з найпоширеніших технологій, що використовуються в корпоративних мережах.

Ethernet. Основний стандарт проводової мережі для підключення комп'ютерів, принтерів та інших пристроїв в офісному середовищі. Wi-Fi. Бездротова мережа, яка дозволяє підключати пристрої до мережі без потреби

проводів. VPN (Virtual Private Network). Технологія, що дозволяє створювати зашифровані з'єднання через публічні мережі, забезпечуючи безпеку підключення до внутрішньої мережі компанії з будь-якого місця. Firewalls (брандмауери). Захисні системи, що контролюють трафік мережі та застосовують правила безпеки для захисту від несанкціонованого доступу. Intrusion Detection Systems (IDS) та Intrusion Prevention Systems (IPS). Системи, що виявляють та запобігають несанкціонованому доступу або злому в мережі.

Unified Communications (UC). Технології, що інтегрують різні методи комунікації (наприклад, телефонію, відеоконференції, обмін повідомленнями) в єдину платформу для підвищення продуктивності співробітників. SD-WAN (Software-Defined Wide Area Network). Технологія, що дозволяє централізовано керувати та налаштовувати мережу через програмне забезпечення, забезпечуючи більшу гнучкість та ефективність управління. Cloud Services. Використання хмарних сервісів для зберігання даних, виконання обчислень та надання інших послуг, що дозволяє підвищити масштабованість та доступність мережі.

Load Balancers. Програмне або апаратне забезпечення, яке розподіляє навантаження між серверами або мережевими ресурсами, забезпечуючи оптимальне використання ресурсів та підвищуючи надійність системи. Identity and Access Management (IAM). Системи, що керують ідентифікацією та доступом користувачів до різних ресурсів мережі, забезпечуючи безпеку та конфіденційність даних.

## 1.7 Побудова локальної мережі LAN

Побудова локальної мережі (LAN) може включати в себе різні способи і технології, залежно від потреб організації, розміру та складності мережі. Ось кілька способів побудови локальної мережі для підприємства. Проводова мережа (Ethernet). Це один з найпоширеніших способів побудови LAN. Вона використовує Ethernet-кабелі для підключення комп'ютерів, принтерів, серверів та інших мережевих пристроїв до комутаторів або маршрутизаторів.

Бездротова мережа (Wi-Fi). Wi-Fi дозволяє підключати пристрої до мережі без проводів. Для побудови бездротової LAN потрібно налаштувати точки доступу (Access Points), які забезпечують бездротове підключення пристроїв. Вертикально-орієнтована мережа (VLAN). VLAN дозволяє розділити одну фізичну мережу на логічні сегменти. Це дозволяє контролювати трафік та забезпечувати безпеку та ефективність мережі.

Software-Defined Networking (SDN). SDN використовує програмне забезпечення для централізованого керування та налаштування мережі, що дозволяє швидше реагувати на зміни та оптимізувати мережеві процеси.

Fiber Optic Network. Використання волоконно-оптичних кабелів для побудови мережі може забезпечити високу швидкість передачі даних та більшу стійкість до електромагнітних перешкод.

Mesh Networking. В мережах типу Mesh кожен пристрій може бути підключеним до кожного іншого, утворюючи мережу без одного центрального вузла. Це може бути корисно для великих просторів або динамічних середовищ, де звичайні топології мереж неефективні.

Powerline Networking. Використання електричних проводів для передачі даних між пристроями в мережі. Coaxial Networking. Використання коаксіальних кабелів для побудови мережі, особливо корисно в середовищах, де вже є інфраструктура кабельного телебачення. Ці методи можуть бути використані окремо або в поєднанні,залежно від потреб, вимог та можливостей підприємства. Кабелі зображено на рисунку 1.1.

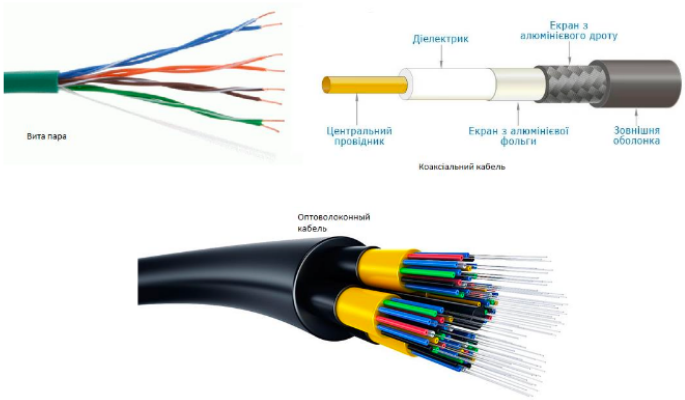


Рисунок 1.1 – Зображення кабелів [1]

Побудова локальної мережі (LAN) підприємства включає в себе кілька кроків та використання різних технологій. Ось кілька способів, які можна використовувати для створення LAN в підприємстві. Використання Ethernet кабелів. Встановлення мережевих кабелів, таких як категорія 5e (Cat5e) або категорія 6 (Cat6), для підключення комп'ютерів, принтерів та інших пристроїв до мережевого комутатора або концентратора. Бездротові технології (Wi-Fi). Встановлення більш гнучкої бездротової мережі для підключення пристроїв до LAN без потреби в кабелі. Мережеві комутатори (Switches). Використання мережевих комутаторів для забезпечення комутації даних між пристроями в мережі, що дозволяє ефективно використовувати пропускну здатність мережі.

Маршрутизатори (Routers). Використання маршрутизаторів для забезпечення з'єднання між локальною мережею та іншими мережами, такими як Інтернет або інші віддалені мережі.

Сегментація мережі (Subnetting). Розділення мережі на підмережі для підвищення її ефективності та безпеки, дозволяючи контролювати трафік та обмежувати доступ до різних частин мережі. Централізоване зберігання даних (Network-Attached Storage – NAS або Storage Area Network – SAN). Використання спеціалізованих пристроїв для централізованого зберігання даних, що дозволяє спільний доступ до них з різних пристроїв в мережі.

Захист мережі (Firewalls, Intrusion Detection Systems – IDS, Intrusion Prevention Systems – IPS). Використання захисних технологій для захисту мережі від несанкціонованого доступу та кібератак. Віртуалізація мережі. Використання віртуальних мережевих технологій, таких як віртуальні приватні мережі (VPN), для забезпечення безпеки та приватності комунікацій. Ідентифікація та керування доступом (Identity and Access Management – IAM). Використання систем управління ідентифікацією користувачів та контролю доступу до ресурсів мережі для забезпечення безпеки даних і ресурсів.

# РОЗДІЛ 2
# СИСТЕМИ ЗАХИСТУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

## 2.1 Захист мережі при підключенні

Комплексні системи захисту в інформаційних системах, зокрема в корпоративних мережах, включають в себе різноманітні заходи та технології для забезпечення безпеки даних та інфраструктури. Основні принципи захисту інформації при підключенні до Інтернету включають такі аспекти.

Firewalls (брандмауери). Встановлення захисних брандмауерів для контролю трафіку, який входить та виходить з мережі. Це дозволяє блокувати несанкціонований доступ та захищати внутрішні мережеві ресурси від зовнішніх загроз.

Віртуальні приватні мережі (VPN). Використання шифрування для забезпечення безпеки підключення до внутрішніх мереж через незахищені канали Інтернету. VPN дозволяють створювати безпечне з'єднання між віддаленими користувачами та ресурсами корпоративної мережі.

Ідентифікація та аутентифікація. Використання механізмів ідентифікації та аутентифікації користувачів для забезпечення доступу тільки авторизованим особам. Це може включати в себе використання паролів, біометричних даних, а також двофакторну аутентифікацію.

Інтегровані системи виявлення та запобігання вторгнень (IDS/IPS). Встановлення систем, які моніторять мережевий трафік для виявлення потенційних загроз та автоматичного реагування на них, що дозволяє попереджати кібератаки та недозволені дії в мережі.

Антивірусне програмне забезпечення та антишпигунські програми. Використання програм, які виявляють та нейтралізують віруси, шкідливі програми та шпигунське ПЗ, що може потенційно завдати шкоди інформаційній системі.

Регулярне оновлення програмного забезпечення та застосунків. Постійне оновлення оперативної системи, програмного забезпечення та додатків для виправлення виявлених уразливостей та забезпечення безпеки системи.

Захист периметра мережі. Встановлення технологій, що дозволяють захистити зовнішні точки доступу до мережі, такі як веб-проксі, мережеві фільтри та інші пристрої, які мінімізують ризик зовнішніх атак.

Ці принципи захисту інформації допомагають забезпечити безпеку корпоративної мережі під час підключення до Інтернету та зменшити ризик витоку даних та кібератак, що зображено на рисунку 2.1


Рисунок 2.1 – Концепція захисту даних інформації [2]

## 2.2 Network Address Translation

NAT (Network Address Translation) – це техніка, яка використовується в мережах для перетворення IP-адрес та портів пакетів даних, що проходять через маршрутизатор або файрвол. Це робиться для керування доступом до ресурсів мережі та забезпечення безпеки, а також для вирішення проблеми нестачі доступних IP-адрес.

Основні принципи NAT-перетворення. IP-адресування. Коли пакет даних надходить з внутрішньої мережі до маршрутизатора з NAT, його IP-адреса та порт внутрішнього джерела замінюються на зовнішню IP-адресу та порт

маршрутизатора. Це дозволяє зберегти приватні адреси внутрішньої мережі при взаємодії з зовнішньою мережею. Таблиця NAT. Маршрутизатор, який використовує NAT, зберігає таблицю, в якій зберігається відображення внутрішніх IP-адрес та портів на зовнішні IP-адреси та порти. Ця таблиця дозволяє маршрутизатору правильно маршрутизувати пакети даних. Типи NAT. Існують різні типи NAT, такі як Static NAT, Dynamic NAT та PAT (Port Address Translation). У кожного типу є власні особливості та сфера застосування.

Підтримка множини клієнтів. NAT дозволяє підтримувати більше клієнтів у внутрішній мережі, ніж доступних зовнішніх IP-адрес. Всі ці клієнти можуть спільно використовувати одну або кілька зовнішніх IP-адрес. Безпека. NAT допомагає приховати структуру внутрішньої мережі від зовнішнього світу, що ускладнює атакам зломувачів проникнення в мережу. Вирішення конфліктів адрес. NAT може допомогти вирішити проблеми з конфліктами адрес, що виникають у великих мережах через обмежену кількість доступних IP-адрес. NAT-перетворення є важливою технікою для керування та захисту мережі, особливо у великих організаціях з багатою інфраструктурою та великою кількістю клієнтів показано на рисунку 2.2.

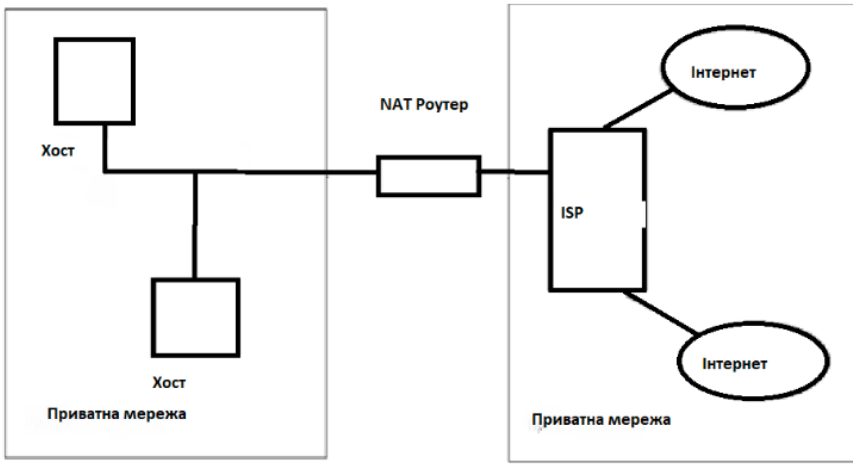


Рисунок 2.2 – Перетворення [2]

## 2.3 Основні характеристики та функції DMZ

Демілітаризована зона (DMZ) – це зона мережі, яка розділена між зовнішньою мережею та внутрішньою мережею (локальною мережею), яка захищається брандмауерами або іншими захисними пристроями. DMZ створюється для розміщення публічних ресурсів, таких як веб-сервери, поштові сервери або інші служби, які мають бути доступні зовнішнім користувачам, але при цьому вони потенційно можуть бути ціллю кібератак.

Основні характеристики та функції демілітаризованої зони (DMZ). Захист внутрішньої мережі. DMZ відокремлює публічні ресурси від внутрішньої мережі, що зменшує ризик вразливості цієї мережі в разі успішної атаки на публічні сервіси. Доступність публічних служб. Публічні сервери, такі як веб-сервери або поштові сервери, розміщені в DMZ, можуть бути доступні з Інтернету, що дозволяє зовнішнім користувачам отримувати доступ до цих ресурсів. Контроль доступу. DMZ дозволяє налаштувати брандмауери та інші захисні пристрої для контролю доступу до публічних серверів. Наприклад, можна обмежити доступ лише до певних портів або IP-адрес. Моніторинг та аналіз трафіку. DMZ дозволяє моніторити та аналізувати трафік, що надходить до публічних серверів, щоб виявити атаки або незвичайну активність.

Ізоляція вразливостей. Якщо публічний сервер в DMZ стає жертвою кібератаки, існує менша ймовірність того, що атака проникне в середину внутрішньої мережі, оскільки DMZ відокремлюється від цієї мережі. Зменшення впливу атак на внутрішню мережу.

Якщо публічний сервер в DMZ все ж таки стає жертвою атаки, ізольованість цієї зони допомагає зменшити можливість поширення атаки на інші ресурси в мережі. В цілому, демілітаризована зона є важливим елементом мережевої архітектури для забезпечення безпеки та доступності публічних служб в мережі, що зображено на рисунку 2.3.

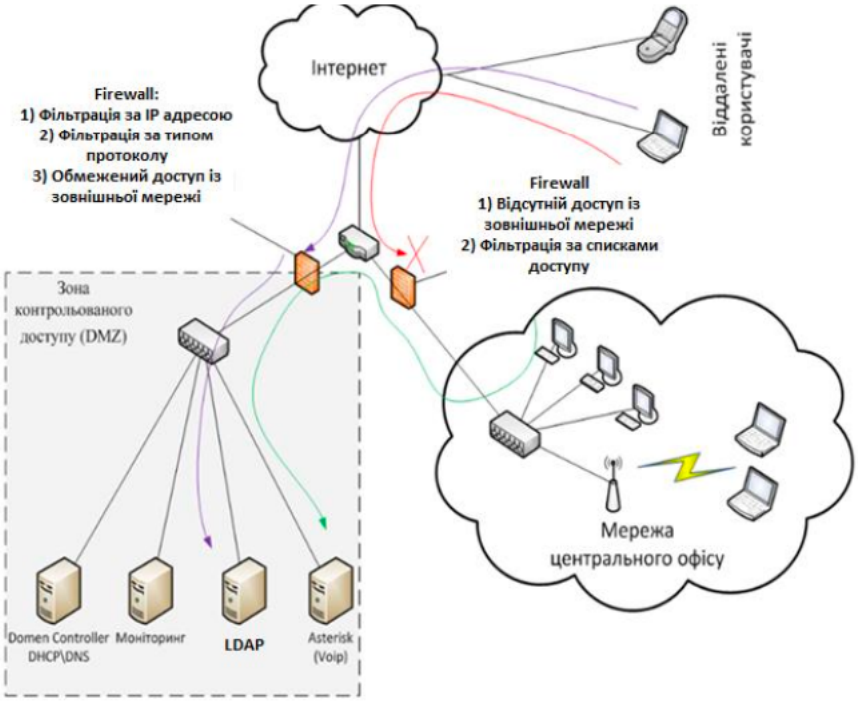


Рисунок 2.3 – Демілітаризована зона [3]

## 2.4 Основні аспекти антивірусного захисту комп'ютерної мережі

Антивірусний захист комп'ютерів (КМ) включає в себе використання спеціального програмного забезпечення для виявлення, блокування та видалення шкідливих програм, таких як віруси, черви, троянські програми, шпигунське ПЗ та інші загрози для безпеки системи.

Основні аспекти антивірусного захисту КМ включають наступне. Виявлення шкідливих програм. Антивірусне програмне забезпечення аналізує файли та дії на комп'ютері для виявлення потенційно небезпечних програм. Це може бути здійснено за допомогою сигнатур (списків відомих загроз) або евристичних алгоритмів (виявлення незвичайної або підозрілої активності).

Блокування шкідливих програм. Після виявлення потенційно небезпечної програми антивірус блокує її виконання або доступ до системних ресурсів, що запобігає поширенню інфекції та завданню шкоди системі.

Видалення загроз. Антивірусне програмне забезпечення може намагатися видалити виявлені шкідливі програми з комп'ютера або карантинувати їх, щоб

вони не могли запуститися. Оновлення бази даних. Антивірусні програми регулярно оновлюють свої бази даних сигнатур, щоб виявляти нові шкідливі програми та оновлені версії вже відомих загроз.

Захист в реальному часі. Деякі антивірусні програми працюють у режимі реального часу, аналізуючи дії та файли під час їх виконання для негайного виявлення та блокування загроз. Додаткові функції безпеки. Деякі антивірусні програми також можуть включати додаткові функції безпеки, такі як захист від фішингу, захист від шкідливих веб-сайтів, контроль додатків та інші. Враховуючи постійну еволюцію кіберзагроз та вірусів, важливо мати актуальне та ефективне антивірусне програмне забезпечення для захисту комп'ютерів та даних користувачів. Зображення безпеки корпоративної мережі показано на рисунку 2.4.

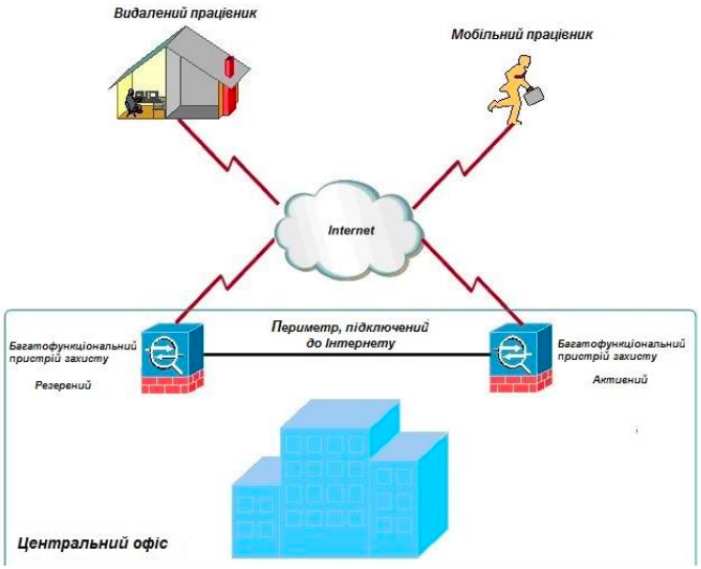


Рисунок 2.4 – Зображення захисту комп'ютерної мережі [4]

## 2.5 Налаштування та використання серверу

Використання log-сервера в мережі та системному адмініструванні є важливою складовою для моніторингу, аналізу та забезпечення безпеки та ефективності мережевих ресурсів. Основні аспекти використання log-сервера

включають наступне. Збір та агрегація логів. Log-сервер забезпечує централізований збір та агрегацію лог-файлів з різних джерел у мережі, таких як маршрутизатори, комутатори, сервери, пристрої безпеки та інші. Зберігання логів. Log-сервер може забезпечити довгострокове зберігання лог-файлів, що дозволяє зберігати історію подій у мережі для подальшого аналізу, відновлення та відповіді на інциденти. Аналіз логів. Централізований збір та зберігання лог-файлів дозволяє аналізувати великі обсяги даних для виявлення незвичайної або підозрілої активності, ідентифікації проблем та виявлення загроз безпеці. Моніторинг безпеки. Log-сервер може використовуватися для моніторингу безпеки мережі, виявлення потенційних загроз, а також спостереження за спробами несанкціонованого доступу або атаками. Відслідковування подій. Log-сервер дозволяє відслідковувати події в мережі, такі як входи в систему користувачів, зміни конфігурацій пристроїв, незвичайна активність та інші події, що відбуваються у мережі. Аудит та відповідність. Log-сервер може допомогти виконанню аудиту системи та відповідності до регуляторних вимог, які вимагають зберігання та моніторингу лог-даних. Управління інцидентами. Log-сервер є важливим інструментом для управління інцидентами, допомагаючи аналізувати та реагувати на події в мережі швидко та ефективно. Використання log-сервера допомагає підвищити безпеку, ефективність та доступність мережевих ресурсів, а також спрощує управління та моніторинг інфраструктури, роботу сервера показано на рисунку 2.5.

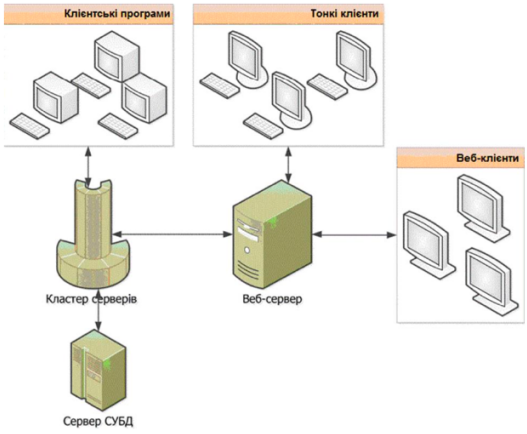


Рисунок 2.5 – Зображення роботи сервера [5]

## 2.6 Firewalls та захист мережі

Міжмережеві екрани (firewalls) є важливим засобом захисту мережі, який допомагає контролювати трафік, що входить та виходить з мережі, і забезпечує безпеку шляхом встановлення правил доступу та фільтрації пакетів даних. Ось деякі основні способи, які міжмережеві екрани використовуються для захисту інформації. Контроль доступу. Міжмережеві екрани дозволяють налаштовувати правила доступу, які визначають, хто із зовнішнього світу має доступ до ресурсів у вашій мережі та які ресурси можуть бути доступні для зовнішніх користувачів.

Фільтрація пакетів даних. Вони фільтрують трафік, що проникає у мережу, і блокують пакети даних, які містять підозрілі або небезпечні дані, такі як віруси, шкідливі коди чи інші загрози. Network Address Translation (NAT). Міжмережеві екрани можуть використовувати NAT для перетворення IP-адрес та портів, що дозволяє захистити внутрішню мережу, приховуючи її реальну структуру та IP-адреси.

Деякі міжмережеві екрани використовують Deep Packet Inspection (DPI) для аналізу пакетів даних на предмет шкідливих або небезпечних вмісту, що дозволяє виявляти складні загрози та кібератаки. Міжмережеві екрани відіграють важливу роль у захисті мережі та інформації, допомагаючи запобігти несанкціонованому доступу, атакам та витокам даних. Важливо правильно налаштувати та підтримувати їх, щоб забезпечити максимальний рівень безпеки для мережі, схематичне зображення подано на рисунку 2.6.

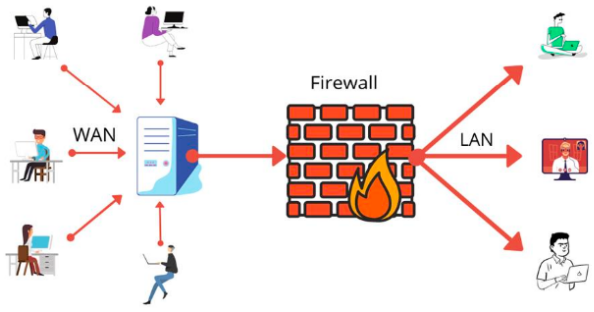


Рисунок 2.6 – Firewalls та захист мережі[8]

# РОЗДІЛ 3
# ПРОЕКТ КОМП'ЮТЕРНОЇ МЕРЕЖІ КОВЕЛЬСЬКОЇ ФІЛІЇ ВОДОКАНАЛУ

## 3.1 Характеристика мережі Ковельської філії Водоканалу

Проектування корпоративної мережі для Ковельської філії Водоканалу на базі обладнання Cisco може включати різні складові, такі як маршрутизатори, комутатори, мережеві пристрої безпеки, точки доступу Wi-Fi та інше обладнання, яке допомагає забезпечити надійну та безпечну мережеву інфраструктуру.

Аналіз потреб. Розуміння потреб бізнесу щодо мережі – скільки пристроїв потрібно підключити, які типи трафіку будуть передаватися, які додатки використовуються, які рівні безпеки необхідні тощо.

Розгортання маршрутизаторів і комутаторів. Вибір відповідних моделей маршрутизаторів та комутаторів Cisco, які забезпечать потрібні функціональність, пропускну здатність та безпеку для мережі.

Настройка мережевої безпеки. Встановлення брандмауерів, VPN-підключень, систем виявлення і запобігання вторгненням (IDS/IPS), а також інших заходів захисту для забезпечення безпеки мережі.

Управління мережею. Встановлення системи управління мережею (NMS) для моніторингу та керування мережею, включаючи моніторинг пристроїв, збір даних про продуктивність та безпеку, а також віддалене керування.

Бездротова мережа. Розгортання точок доступу Wi-Fi для бездротового підключення пристроїв та забезпечення потрібного рівня безпеки.

Резервне копіювання і відновлення. Налаштування резервного копіювання та відновлення для забезпечення надійності та доступності мережі.

Технічна підтримка. Планування технічної підтримки та обслуговування обладнання, включаючи оновлення програмного забезпечення та вирішення технічних проблем.

Це лише загальний огляд можливого підходу до проектування корпоративної мережі на базі обладнання Cisco для малого підприємства, і кожен проект може мати свої особливості, які потребують індивідуального підходу.

### 3.2 Планування комп'ютерної мережі Ковельської філії Водоканалу

Розрахунок необхідної кількості комп'ютерного устаткування для корпоративної мережі зазвичай ґрунтується на потребах і ресурсах підприємства. Ось кілька кроків, які можна виконати для розрахунку.

Визначення кількості співробітників. Потрібно визначити, скільки співробітників працює в підприємстві, включаючи тих, хто потребує доступу до комп'ютерних ресурсів.

Розподіл за відділами. Розподіліть співробітників за відділами або функціональними групами і визначте, скільки комп'ютерів потрібно для кожного відділу.

Планування росту. Врахуйте можливість зростання компанії та змін у кількості співробітників у майбутньому. Розрахуйте запасну місткість для майбутнього росту.

Призначення комп'ютерних ресурсів. Потрібно вирішити, які конкретні комп'ютерні ресурси (наприклад, стаціонарні ПК, ноутбуки, монітори, принтери тощо) потрібні кожному співробітникові або відділу.

Врахування додаткових пристроїв. Врахуйте інші пристрої, такі як принтери, сканери, копіювальні апарати, мережеві пристрої (маршрутизатори, комутатори), телефони та інше обладнання.

Планування мережевих ресурсів. Визначте, скільки портів мережевого обладнання потрібно для підключення комп'ютерів та інших пристроїв до мережі.

Бюджетні обмеження. Врахуйте бюджетні обмеження та відповідність вартості обладнання і розрахунків вашому підприємству.

За допомогою цих кроків можна розрахувати оптимальну кількість комп’ютерного устаткування для корпоративної мережі вашого підприємства. Також варто врахувати можливість консультації з фахівцями з інформаційних технологій або проведення додаткового дослідження щодо специфіки вашого бізнесу та його потреб у комп’ютерному обладнанні.

Розрахунок необхідної кількості комп’ютерного устаткування для корпоративної мережі включає в себе розгляд таких факторів, як кількість працівників, їх робочі потреби, рівень автоматизації, безпека мережі та інші. Ось кілька кроків, які можна виконати для цього розрахунку.

Кількість співробітників. Визначте загальну кількість працівників у вашій організації, які будуть підключені до мережі. Це включає не лише основний персонал, але й можливість підключення гостьових користувачів, консультантів або інших сторонніх осіб.

Функціональні потреби. Визначте, які конкретні завдання виконуватимуть користувачі на комп’ютерах мережі. Наприклад, чи потрібні їм потужні робочі станції для обробки великих обсягів даних, або ж їм достатньо більш простих комп’ютерів для стандартних офісних завдань?

Типи пристроїв. Розгляньте також інші типи пристроїв, що можуть бути підключені до мережі, такі як принтери, мультимедійні пристрої, мережеві сховища даних тощо.

Розташування робочих місць. Визначте розташування робочих місць у вашому офісі, щоб визначити необхідну довжину мережевих кабелів та кількість комутаторів і точок доступу Wi-Fi.

Зростання бізнесу. Передбачте потенційне зростання бізнесу та залучення нових співробітників, щоб забезпечити масштабованість мережі в майбутньому.

Безпека мережі. Розгляньте заходи безпеки мережі, такі як використання мережевих пристроїв безпеки, антивірусного програмного забезпечення, зашифрованого з’єднання тощо.

Після виконання цих кроків ви зможете приблизно визначити необхідну кількість комп’ютерного устаткування для вашої корпоративної мережі. Варто

також звернутися до спеціалістів у сфері IT або інженерів мереж, які допоможуть вам в розрахунках та виборі оптимального обладнання для вашої конкретної ситуації.

### 3.3 Програмне забезпечення для комп'ютерних мереж

Вибір програмного забезпечення для корпоративних мереж (КМ) залежить від різних факторів, включаючи потреби бізнесу, функціональні вимоги, рівень безпеки та інші фактори. Ось деякі критерії, які можна врахувати при обґрунтуванні вибору програмного забезпечення для КМ.

Функціональність. Перш за все, програмне забезпечення повинно відповідати функціональним потребам вашого бізнесу. Це можуть бути офісні пакети для роботи з документами, електронною поштою, спільної роботи тощо.

Сумісність. Важливо, щоб програмне забезпечення було сумісним з існуючим апаратним забезпеченням та операційною системою вашого КМ. Також слід врахувати сумісність з іншими програмними продуктами, які вже використовуються в організації.

Безпека. Оберіть програмне забезпечення, яке має високий рівень безпеки для захисту конфіденційності та цілісності даних вашого бізнесу. Переконайтеся, що програма має можливості аутентифікації, авторизації та захисту від загроз кібербезпеки.

Масштабованість. Якщо ваша організація збирається зростати, оберіть програмне забезпечення, яке може легко масштабуватися та пристосовуватися до змін потреб вашого бізнесу.

Підтримка та обслуговування. Важливо мати доступ до якісної технічної підтримки та обслуговування програмного забезпечення. Оберіть постачальника, який надає відмінну підтримку та часті оновлення програмного забезпечення.

Вартість. Оцініть вартість програмного забезпечення в контексті вашого бюджету. Пам'ятайте, що найнижча вартість не завжди означає найкращу якість,

а найвища вартість не завжди означає найкращу функціональність. Ліцензування. Оберіть модель ліцензування, яка найбільше підходить вашому бізнесу. одноразову покупку, підписку або хмарний сервіс. Враховуючи ці критерії, ви можете обґрунтувати вибір програмного забезпечення для вашої корпоративної мережі. Важливо також провести тестування та оцінку програмного забезпечення перед його впровадженням, щоб переконатися в його відповідності вашим потребам та очікуванням.

### 3.4 Серверне обладнання для комп'ютерної мережі Ковельської філії Водоканалу

Вибір серверного обладнання для корпоративної мережі потребує уважного аналізу та врахування різних факторів. Ось деякі критерії, які варто врахувати при виборі серверного обладнання. Потреби в продуктивності. Оцініть типи завдань, які сервер буде виконувати, і визначте необхідну продуктивність, обчислювальні потужності та ресурси (пам'ять, процесори, сховище тощо) для ефективного виконання цих завдань.

Масштабованість. Оберіть серверне обладнання, яке може масштабуватися разом з ростом вашого бізнесу. Важливо, щоб сервер був гнучким та легко розширювався за потреби. Надійність. Врахуйте рівень надійності та доступності серверного обладнання. Оберіть сервери відомих виробників з високим рівнем якості та підтримки, які забезпечать найвищу доступність для вашої мережі.

Безпека. Приділіть увагу функціям безпеки серверного обладнання, таким як захист від вторгнень, шифрування даних, аутентифікація користувачів та інші заходи безпеки.

Управління та моніторинг. Виберіть серверне обладнання, яке має потужні інструменти управління та моніторингу, що дозволить вам ефективно керувати серверами та відслідковувати їхню продуктивність. Вартість володіння. Розгляньте не лише вартість придбання серверного обладнання, але й витрати на

підтримку, обслуговування, енергоспоживання та інші операційні витрати на протязі життєвого циклу сервера.

Стандарти сумісності. Переконайтеся, що серверне обладнання відповідає сучасним стандартам та специфікаціям для забезпечення сумісності з існуючими і майбутніми компонентами мережі. Враховуючи ці критерії, ви зможете обрати серверне обладнання, яке найкращим чином відповідає потребам вашого підприємства і забезпечить надійну та ефективну мережеву інфраструктуру. Вибір серверного обладнання для корпоративної мережі є критичним завданням, оскільки сервери відіграють ключову роль у забезпеченні продуктивності, безпеки та доступності мережевих послуг. Ось деякі критерії, які можна врахувати при виборі серверного обладнання.

Відомості про завдання сервера. Ретельно проаналізуйте завдання, які повинен виконувати сервер (наприклад, файловий сервер, поштовий сервер, сервер баз даних тощо). Це допоможе визначити потрібні характеристики сервера, такі як обсяг пам’яті, кількість процесорних ядер, обсяг зберігання даних тощо. Характеристики процесора. Вибирайте сервери з потужними та надійними процесорами, які можуть ефективно обробляти завдання вашого бізнесу. Враховуйте кількість ядер, тактову частоту, кеш-пам’ять і можливості віртуалізації.

Пам’ять. Пам’ять є ще одним важливим фактором. Обирайте сервери з достатньою кількістю оперативної пам’яті для ефективної роботи з додатками та завданнями вашого бізнесу. Масштабованість. Плануйте майбутнє зростання вашого бізнесу і вибирайте сервери, які можуть масштабуватися відповідно до зростання потреб вашої мережі. Надійність і доступність. Обирайте сервери з високою надійністю та можливістю гарантованої доступності. Розгляньте наявність функцій резервного живлення, гарячої заміни компонентів, RAID-масивів для збереження даних тощо.

Мережеві можливості. Враховуйте мережеві можливості сервера, такі як швидкість мережевого підключення, підтримка стандартів передачі даних, а також наявність вбудованих інтерфейсів для підключення до мережі.Управління

сервером. Приділяйте увагу можливостям віддаленого управління сервером, таким як IPMI (Intelligent Platform Management Interface), що дозволяє адміністраторам віддалено керувати сервером та відстежувати його стан. Вартість та підтримка. Враховуйте вартість серверного обладнання та послуги підтримки, включаючи гарантійні та післягарантійні обслуговування. Обирайте серверне обладнання з урахуванням цих критеріїв, щоб забезпечити ефективну та надійну роботу вашої корпоративної мережі.

### 3.5 Передача даних в комп'ютерній мережі Ковельської філії Водоканалу

При виборі технології передачі даних для корпоративної мережі важливо враховувати потреби вашого бізнесу, вимоги щодо швидкості, безпеки, надійності та масштабованості. Ось декілька основних технологій передачі даних, які варто розглянути. Ethernet (проводова мережа). Ethernet є одним з найпоширеніших стандартів проводової мережі. Він забезпечує стабільну та високошвидкісну передачу даних за допомогою Ethernet-кабелів. Ethernet може бути розгалуженим (з використанням комутаторів) або лінійним (з використанням концентраторів), а також може підтримувати різні швидкості передачі даних, такі як 10/100/1000 Mbps або навіть 10 Gbps. Wi-Fi (бездротова мережа). Wi-Fi є бездротовою технологією, яка дозволяє підключати пристрої до мережі без необхідності використання кабелів. Вона зручна для мобільних пристроїв та для пристроїв, які розташовані на відстані від кабельної інфраструктури. Вибір підходящої Wi-Fi-технології (наприклад, 802.11ac або 802.11ax) залежить від потреб у швидкості та покритті мережі.

Fiber Optic (оптична мережа). Оптичні мережі використовують скляні або пластикові волоконні кабелі для передачі даних з високою швидкістю та на велику відстань. Вони забезпечують велику пропускну здатність та імунітет до електромагнітних перешкод, що робить їх ідеальним вибором для великих корпоративних мереж та мережі з великим обсягом даних. Virtual Private Network (VPN). VPN – це технологія, яка дозволяє безпечно передавати дані через

незахищені мережі, такі як Інтернет. Вона забезпечує шифрування даних та забезпечує конфіденційність та цілісність даних під час їх передачі. VPN особливо корисна для роботи з віддаленими робітниками або філіями компанії.

Software-Defined Networking (SDN). SDN – це архітектурний підхід до мережевого управління, який дозволяє централізовано керувати мережевим обладнанням і програмним забезпеченням з використанням програмних інтерфейсів (API). SDN може полегшити управління мережею, забезпечити гнучкість та масштабованість. Internet of Things (IoT). IoT – це мережа фізичних пристроїв, які підключені до Інтернету та обмінюються даними між собою. Вона використовується для збору даних та автоматизації процесів в різних галузях, включаючи промисловість, охорону здоров'я, транспорт тощо.

При виборі комутаційного обладнання для корпоративної мережі важливо враховувати різні фактори, такі як потужність, масштабованість, безпека та можливості управління. Ось кілька критеріїв, які можна врахувати при виборі комутаторів. Швидкість передачі даних. Оберіть комутатори з відповідною швидкістю передачі даних, яка відповідає потребам вашої мережі. Наприклад, Gigabit Ethernet (1 Gbps) для офісних мереж або 10 Gigabit Ethernet для більш великих мереж з високим обсягом даних. Кількість портів. Виберіть комутатори з достатньою кількістю портів для підключення всіх пристроїв в вашій мережі. Також розгляньте можливість розширення кількості портів у майбутньому.

Управління трафіком. Розгляньте комутатори з підтримкою розумного управління трафіком, які забезпечують QoS (Quality of Service) для пріоритезації важливих даних та контролюють розподіл пропускної здатності. Безпека. Важливо мати комутатори з вбудованими заходами безпеки, такими як контроль доступу на рівні портів, VLAN-ізоляція, детекція злому та інші функції захисту.

Масштабованість. Виберіть комутатори, які можуть масштабуватися з ростом вашої мережі. Розгляньте можливість додавання додаткових модулів або стекінгу комутаторів для розширення функціональності та пропускної здатності.

Управління мережею. Оберіть комутатори з підтримкою різних протоколів управління мережею, таких як SNMP, CLI та веб-інтерфейси, щоб забезпечити

легке керування та моніторинг мережі. Надійність. Приділяйте увагу надійності комутаторів, їх життєвому циклу та наявності гарантійного обслуговування. Вартість. Порівняйте вартість комутаторів з їхніми характеристиками та функціональністю, щоб знайти оптимальний баланс між витратами та якістю. Зважте на ці критерії при виборі комутаційного обладнання для вашої корпоративної мережі, щоб забезпечити її ефективну роботу та безпеку. При виборі комутаційного обладнання для корпоративної мережі важливо враховувати потреби вашого бізнесу, вимоги щодо пропускної здатності, безпеки, надійності та масштабованості. Ось деякі критерії, які можна врахувати при виборі комутаторів для корпоративної мережі.

Швидкість передачі даних. Обирайте комутатори з високою швидкістю передачі даних, що відповідає потребам вашого бізнесу. Враховуйте обсяг трафіку в вашій мережі та швидкість підключення пристроїв. Кількість портів. Плануйте кількість портів на комутаторі відповідно до кількості пристроїв, які потрібно підключити до мережі. Розгляньте не лише поточні потреби, але й майбутнє зростання бізнесу. Підтримка PoE. Якщо вам потрібно живлення пристроїв через Ethernet (наприклад, IP-телефони, відеокамери), варто розглянути комутатори з підтримкою технології PoE (Power over Ethernet).

Управління. Вибирайте комутатори з можливістю централізованого управління та моніторингу мережі. Опції управління можуть включати веб-інтерфейс, SNMP (Simple Network Management Protocol) або інші інтерфейси. Безпека. Обирайте комутатори з функціями безпеки, такими як VLAN (Virtual Local Area Network), ACL (Access Control Lists), 802.1X аутентифікація тощо, для забезпечення безпеки мережі та контролю доступу до ресурсів. Надійність. Розгляньте надійність та доступність комутатора, таку як можливість гарячої заміни компонентів, підтримка протоколів redundancy (наприклад, Spanning Tree Protocol), а також гарантійні умови.

Масштабованість. Обирайте комутатори, які можуть легко масштабуватися для відповіді на зростаючі потреби вашого бізнесу та мережі. Вартість. Оцініть вартість комутатора в контексті вашого бюджету, враховуючи

не лише витрати на придбання, але й витрати на підтримку та експлуатацію. Обирайте комутаційне обладнання з урахуванням цих критеріїв, щоб забезпечити ефективну та надійну роботу вашої корпоративної мережі.

### 3.6 Проектування мережі та IP-адреса Ковельської філії Водоканалу

Для розрахунку адресного простору IP-адрес в корпоративній мережі, ви повинні визначити кількість необхідних IP-адрес та обрану підмережу (subnet). Ось кроки, які можна виконати для розрахунку. Визначте кількість пристроїв у вашій мережі. Підрахуйте кількість комп'ютерів, принтерів, серверів, маршрутизаторів, комутаторів та інших мережевих пристроїв, які будуть підключені до вашої мережі. Включіть у цей розрахунок потенційне зростання мережі. Визначте клас IP-адресу. Розгляньте розподіл IP-адрес за класами (A, B, C, D, E) та виберіть той, який відповідає потребам вашої мережі. Наприклад, для невеликих до середніх корпоративних мереж зазвичай використовуються класи C або B. Оберіть підмережу (subnet). Розбийте вашу мережу на підмережі для ефективного управління IP-адресами та забезпечення безпеки мережі. Виберіть підмережу з урахуванням кількості пристроїв та потреб безпеки.

Визначте бітову довжину префіксу мережі (subnet mask). Це визначається кількістю бітів, які призначені для ідентифікації мережі. Наприклад, для підмережі з 254 IP-адресами, бітова довжина префіксу буде /24 для класу C або /23 для класу B. Розрахуйте діапазон IP-адрес. Використовуйте формули та правила для розрахунку можливих IP-адрес у визначеній підмережі. Наприклад, для підмережі з маскою підмережі /24 (255.255.255.0) та адресою мережі 192.168.1.0, діапазон IP-адрес буде від 192.168.1.1 до 192.168.1.254. Зарезервуйте IP-адреси. Зарезервуйте деякі IP-адреси для службових цілей, таких як адреси маршрутизаторів, серверів DHCP, DNS тощо.

Документуйте вашу конфігурацію. Створіть документацію, яка включає в себе вибраний клас IP-адресу, маску підмережі, адресу мережі, діапазон IP-адрес, зарезервовані адреси та інші важливі дані. Ці кроки допоможуть вам розрахувати

адресний простір IP-адрес для вашої корпоративної мережі та ефективно його управляти. Важливо дотримуватися нормативів та кращих практик щодо розподілу та використання IP-адрес у вашій мережі. Для розрахунку адресного простору IP-адрес в корпоративній мережі слід врахувати кількість пристроїв, які потрібно підключити до мережі, та вибрати підходящий діапазон IP-адрес. Ось кілька кроків для проведення цього розрахунку. Визначення кількості пристроїв.  Розрахунок підмереж та хостів. Виберіть клас IP-адрес, враховуючи кількість потрібних IP-адрес та потенційний зріст мережі у майбутньому. Потім розрахуйте кількість підмереж та кількість хостів у кожній підмережі. Вибір префіксу підмережі та маски підмережі. Оберіть префікс підмережі та маску підмережі для кожної підмережі з урахуванням кількості хостів, які будуть підключені до кожної з них. Надання IP-адрес. Надайте IP-адреси пристроям у вашій мережі, дотримуючись обраних діапазонів IP-адрес та масок підмереж.

Додаткові розгляди. Врахуйте потреби в резервних IP-адресах, а також можливість використання DHCP (Dynamic Host Configuration Protocol) для автоматичного призначення IP-адрес пристроям у вашій мережі. Наприклад, якщо у вас є 200 пристроїв, можливо, вибір класу C (який надає близько 254 хостів) буде достатнім. Ви можете використовувати маску підмережі /24, щоб створити одну підмережу з доступними IP-адресами від 192.168.0.1 до 192.168.0.254. Якщо вам потрібно більше хостів або підмереж, ви можете розглянути використання класу B або навіть класу A IP-адрес. Побудова корпоративної мережі на основі обраного обладнання включає кілька кроків. Проектування мережі. Розробіть план мережі, визначивши топологію мережі (наприклад, зірка, шина, кільце), розташування серверів, комутаторів, маршрутизаторів та інших мережевих пристроїв. Встановлення обладнання. Встановіть обране комутаційне, маршрутизаційне та інше мережеве обладнання відповідно до розробленого плану мережі. Підключіть пристрої до електромережі та забезпечте необхідне охолодження. Конфігурування пристроїв. Налаштуйте мережеве обладнання згідно з потребами вашої мережі. Встановіть IP-адреси, маски підмереж, VLAN, маршрутизаційні таблиці та інші

параметри. Налаштування безпеки. Забезпечте безпеку мережі шляхом встановлення правил файрвола, налаштування VPN-з'єднань, встановлення механізмів аутентифікації та авторизації, а також моніторингу мережевого трафіку. Резервне копіювання та відновлення. Налаштуйте процес резервного копіювання конфігурацій та даних мережевих пристроїв для забезпечення можливості швидкого відновлення у випадку виникнення непередбачених проблем. Тестування та налагодження. Проведіть тестування мережі для перевірки її працездатності, доступності та продуктивності. Усуньте будь-які проблеми, які виявлено під час тестування, та вдосконаліть налаштування мережі. Навчання персоналу. Навчіть персонал, який буде відповідальний за управління та підтримку мережі, використовувати та адмініструвати мережеве обладнання, а також реагувати на можливі проблеми. Підтримка та обслуговування. Забезпечте систематичне обслуговування мережі, включаючи відстеження стану обладнання, вчасне внесення оновлень та підтримку користувачів у разі виникнення проблем. Запровадження корпоративної мережі на основі обраного обладнання вимагає уважного планування, налагодження та тестування для забезпечення її ефективної та безперебійної роботи, топологія водоканалу зображена на рисунку 3.1.

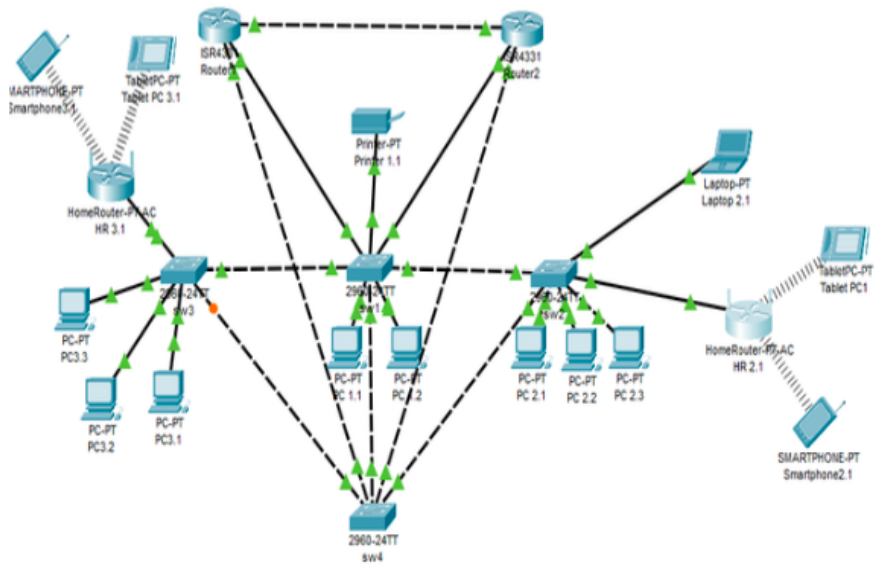


Рисунок 3.1 – Зображення корпоративної мережі водоканалу

# ВИСНОВКИ

Проведений аналіз існуючої корпоративної мережі показав, що вона потребує модернізації для підвищення ефективності роботи, забезпечення безпеки даних та відповідності сучасним технологічним вимогам. Виявлені проблеми включають застаріле обладнання, недостатній рівень кібербезпеки, обмежену автоматизацію процесів та неефективну комунікацію між підрозділами.

Розроблено рекомендації щодо модернізації мережевої інфраструктури, включаючи оновлення обладнання, впровадження сучасних засобів захисту даних та автоматизацію управлінських процесів.

Запропоновано інтеграцію новітніх технологій, таких як хмарні сервіси, Інтернет речей (IoT) та системи для великого обсягу даних (Big Data), що дозволить значно покращити ефективність роботи мережі. Впровадження комплексної системи кібербезпеки, включаючи файрволи, антивірусне програмне забезпечення, системи виявлення вторгнень та регулярне оновлення політик безпеки, забезпечить надійний захист інформації від несанкціонованого доступу та кібератак. Встановлення процедур резервного копіювання та відновлення даних гарантує збереження критично важливої інформації у разі технічних збоїв або аварійних ситуацій.

Впровадження автоматизованих систем управління дозволить значно знизити операційні витрати, пов’язані з паперовим документообігом та ручною обробкою даних. Використання хмарних сервісів зменшить витрати на підтримку та оновлення фізичної інфраструктури, забезпечуючи при цьому гнучкість та масштабованість системи. Автоматизація обробки запитів та звернень клієнтів дозволить швидше та ефективніше реагувати на їхні потреби, підвищуючи рівень задоволеності та лояльності клієнтів.

Інтеграція інформаційних систем забезпечить доступ до актуальної інформації для всіх підрозділів філії, що сприятиме покращенню координації та якості обслуговування. Оновлення мережевого обладнання та впровадження

систем моніторингу дозволить забезпечити безперебійну роботу мережі, швидке виявлення та усунення проблем. Впровадження сучасних технологій управління мережею забезпечить надійність та стабільність її функціонування в будь-яких умовах.

Модернізація мережевої інфраструктури та впровадження заходів кібербезпеки забезпечать відповідність корпоративної мережі всім необхідним нормативним вимогам та стандартам галузі. Забезпечення прозорості та підзвітності процесів обробки та зберігання даних сприятиме підвищенню довіри клієнтів та партнерів.

Таким чином, реалізація запропонованих заходів щодо модернізації корпоративної мережі Ковельської філії Водоканалу забезпечить значне підвищення ефективності, безпеки та якості роботи підприємства, що позитивно вплине на його конкурентоспроможність та розвиток.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Побудова корпоративних мереж передачі даних. 2021. URL:https.//www.telesphera.net/blog/corporate-networking.html (дата звернення 10.05.2024).

2. Особливості побудови і використання сучасних корпоративних комп'ютерних мереж. 2021. URL: https.//conferences.vntu.edu.ua/public/files/1/fitki_2021_netpub.pdf (дата звернення 15.05.2024).

3. Корпоративна мережа. 2019. URL: http.//surl.li/iaybm (дата звернення 15.05.2024).

4. Принципи побудови і призначення комп'ютерних мереж. 2021. URL: http.//surl.li/iadst (дата звернення: 15.05.2024).

5. Загальні принципи побудови корпоративної мережі.2020. URL:https.//studfile.net/preview/5470625/ (дата звернення 10.05.2024).

6. How a VPN (Virtual Private Network) Works. 2021. URL:https.//computer.howstuffworks.com/vpn.htm (дата звернення 15.05.2024).

7. Як не заплутатися у дротах. Типи мережевих кабелів. 2023. URL: https.//maxnet.ua/blog/kak-ne-zaputatsya-v-provodakh-tipy-setevykh- kabeley/ (дата звернення 15.05.2024).

8. Як не заплутатися у дротах. Типи мережевих кабелів. 2022. URL:https.//maxnet.ua/blog/kak-ne-zaputatsya-v-provodakh-tipy-setevykh- kabeley/ (дата звернення 15.05.2024).

9. У чому відмінність «білої» та «сірої» IP-адреси? 2021. URL: http.//surl.li/iadsh (дата звернення 15.05.2024).

10. Cybersecurity, everywhere you need it. 2023. URL: https.//www.fortinet.com/ (дата звернення 10.05.2024).

11. Signed Syslog Messages. 2020. URL: https.//datatracker.ietf.org/doc/html/rfc5848 (дата звернення 15.05.2024).

12. Polo Alto . 2020. URL:https.//techexpert.ua/it-products/palo-alto/63 (дата звернення 15.05.2024).

13. Cisco UCS B200 M5 Blade Server Data Sheet. 2023. URL:https.//www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-b- series-blade-servers/datasheet-c78-739296.html (дата звернення 15.05.2024).

14. Gigabit Ethernet. 2020. URL:https.//wiki.cuspu.edu.ua/index.php/Gigabit_Ethernet (дата звернення: 15.05.2024).

15. Cisco ISR4331-SEC/K9 . 2023. URL:https.//itel.ua/ru/isr4331- seck9 (дата звернення 15.05.2024).

16. Cisco Cisco Catalyst 2960 .2023. URL:https.//itel.ua/ua/isr4331- seck9т (дата звернення 10.05.2024).

17. Word2Vec Tutorial Part I: The Skip-Gram Model. URL : https://radio-shop.com.ua/uk/osnovni-parametry-ostsylohrafiv (дата звернення: 23.03.2024).

18. Electronics for Beginners: A Practical Introduction to Schematics, Circuits, and Microcontrollers. O'Reilly Online Learning. URL: https://www.oreilly.com/library/view/electronics-for-beginners/9781484259795/ (date of access: 23.03.2024).

19. ABCs of Electronics: An Easy Guide to Electronics Engineering. O'Reilly Online Learning. URL: https://www.oreilly.com/library/view/abcs-of-electronics/9798868801341/ (date of access: 23.03.2024).

20. Circuit Design and Simulation Quick Start Guide: Create Schematics and Layout Electronic Components. URL: https://www.oreilly.com/library/view/circuit-design-and/9781484295823/ (date of access: 23.03.2024).

21. PCB Design for Absolute Beginners: Layout Printed Circuit Boards in a Web Browser. URL: https://www.oreilly.com/library/view/pcb-design-for/9781484280409/ (date of access: 23.03.2024).

22. Practical Electronic Design for Experimenters. URL: https://www.oreilly.com/library/view/practical-electronic-design/9781260456165/ (date of access: 23.03.2024).

23. DIY Microcontroller Projects for Hobbyists. URL: https://www.oreilly.com/library/view/diy-microcontroller-projects/9781800564138/ (date of access: 23.03.2024).