Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Навчально-науковий центр заочної форми навчання
(повна назва)

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти перший (бакалаврський)

Побудова локальної мережі підприємства

(тема)

Виконав:
здобувач *4* року навчання,
групи *ТРІМІиз-22-1*
Ісмаілова Айнур Лаіг кизи
(власне ім'я, прізвище)

Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва спеціальності)

Тип програми *освітньо-професійна*
(освітньо-професійна або освітньо-наукова)

Освітня програма *Інформаційно-мережна інженерія*
(повна назва освітньої програми)

Керівник *доц. Наталія ХАРЧЕНКО*
(посада, власне ім'я, прізвище)

Допускається до захисту
В.о. завідувача кафедри _____ *Дарія ЧЕБОТАРЬОВА*
(підпис) (власне ім'я, прізвище)

2026 р.

Не містить відомостей заборонених до відкритого публікування.

Здобувач / Ісмаілова Айнур Лаіг кизи /

Керівник / Наталія Харченко /

Харківський національний університет радіоелектроніки

Навчально-науковий центр заочної форми навчання
Кафедра *Інформаційно-мережної інженерії*
Рівень вищої освіти *перший (бакалаврський)*
Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва)
Тип програми *освітньо-професійна*
Освітня програма *«Інформаційно-мережна інженерія»*
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)
«____»_____ 2026 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві *Ісмаіловій Айнур Лаіг кизи*
(прізвище, ім'я, по батькові)

1. Тема роботи *Побудова локальної мережі підприємства*

затверджена наказом університету від 18 травня 2026 р. № 73 Стз

2. Термін подання здобувачем роботи до екзаменаційної комісії 14 липня 2026 р.

3. Вихідні дані до роботи *Провести аналіз основних етапів планування комп'ютерних мереж, визначити основні вимоги до них. Обґрунтувати вибір мережевої архітектури, провести вибір необхідного обладнання. Проаналізувати методи адміністрування мережею та розробити комплекс заходів із забезпечення інформаційної безпеки. Штат організації налічує 23 особи; для кожного співробітника передбачено забезпечення персональним комп'ютером. Локальна мережа розміщується на одному поверсі у 11 кімнатах, необхідно встановити 1 виділений сервер, до якого організувати спільний доступ. Також організувати в рамках локальної мережі підключення 10 принтерів, до яких також організувати спільний доступ.*

4. Перелік питань, що потрібно опрацювати в роботі
Вступ
1. Теоретичні основи планування та побудови локальних мереж
2. Організація локальної мережі для ТОВ «НОЙНЕР»
3. Адміністрування локальної мережі підприємства
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) *назва, мета, актуальність і завдання кваліфікаційної роботи; топології мереж; мережеве обладнання та кабелі; постановка завдання: ТОВ «НОЙНЕР»; план приміщень і розміщення сервера; топологія мережі організації; схема підключення принтерів; розрахунок кабелю та кабель-каналів; розподіл IP-адрес; структурована кабельна система; адміністрування та захист інформації; висновки*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ.*	*18.05.26*	*виконано*
2	*Підбір літератури за темою роботи.*	*19.05-15.06.26*	*виконано*
3	*Теоретичні основи планування та побудови локальних мереж*	*16.06-26.06.26*	*виконано*
4	*Організація локальної мережі для ТОВ «НОЙНЕР»*	*27.06-03.07.26*	*виконано*
5	*Адміністрування локальної мережі підприємства*	*04.07-10.07.26*	*виконано*
6	*Оформлення презентаційного матеріалу, підготовка до захисту в ЕК*	*11.07-14.07.26*	*виконано*

Дата видачі завдання _18_ ___травня__ 2026 р.

Здобувач _____
(підпис)

Керівник роботи _____ доц. Наталія Харченко
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка 70 с., 16 рис., 4 табл., 14 джерел, 5 додатків.

Об'єкт дослідження – корпоративна локальна комп'ютерна мережа малого підприємства.

Мета роботи – розробити локальну мережу для ТОВ «НОЙНЕР».

Розглянуто загальні принципи побудови локальних мереж, надано характеристику базовим технологіям ЛМ, проаналізовано існуючі топології та структуру ЛМ, зроблено огляд існуючого мережевого обладнання, розглянуто типи з'єднувальних ліній та описано мережеві операційні системи.

Виконано опис програмно-апаратного комплексу локальної мережі організації, проаналізовано структуру локальної мережі, надано рекомендації щодо планування інформаційної безпеки.

КОРПОРАТИВНА МЕРЕЖА, ПЛАНУВАННЯ ЛОКАЛЬНИХ МЕРЕЖ, МЕРЕЖНЕ ОБЛАДНАННЯ, СПІЛЬНИЙ ДОСТУП, IP-АДРЕСА, АДМІНІСТРУВАННЯ.

THE ABSTRACT

Explanatory slip 70 p., 16 fig., 4 tab., 14 sources, 5 attach.

Object of research – a small business's internal computer network.

The purpose of the work - develop a local area network for NOINER LLC.

This paper examines the general principles of local area network (LAN) design, describes the basic technologies used in LANs, analyzes existing LAN topologies and structures, reviews current networking equipment, discusses types of connection lines, and describes network operating systems.

A description of the organization’s local area network hardware and software infrastructure is provided, the structure of the local area network is analyzed, and recommendations for information security planning are offered.

CORPORATE NETWORK, LOCAL AREA NETWORK PLANNING, NETWORK EQUIPMENT, SHARING, IP ADDRESS, ADMINISTRATION.

ЗМІСТ

С.

ПЕРЕЛІК СКОРОЧЕНЬ 9
ВСТУП 10
1 ТЕОРЕТИЧНІ ОСНОВИ ПЛАНУВАННЯ ТА ПОБУДОВИ ЛОКАЛЬНИХ МЕРЕЖ 12
1.1 Обладнання, що використовується для побудови комп'ютерних мереж 12
1.2 Принципи побудови локальних мереж 13
1.3 Способи організації комп'ютерної мережі 14
1.4 Топології локальних мереж 16
1.5 Огляд мережевих технологій 19
1.6 Кабелі, що застосовуються в локальних мережах 21
1.7 Мережне обладнання 23
2 ОРГАНІЗАЦІЯ ЛОКАЛЬНОЇ МЕРЕЖІ ДЛЯ ТОВ «НОЙНЕР» 26
2.1 Постановка завдання 26
2.2 Функціональна схема локальної обчислювальної мережі 26
2.3 Планування структури локальної мережі 27
2.3.1 Комп'ютерна мережа 27
2.3.2 Способи управління мережею 28
2.3.3 Планування мережі в приміщеннях 29
2.3.4 Розміщення сервера 30
2.3.5 Планування мережевої архітектури 31
2.3.6 Організація спільного доступу 33
2.3.7 Розрахунок кількості кабелю та кабель-каналу 34
2.4 Структура локальної комп'ютерної мережі (ЛКМ) організації ТОВ «НОЙНЕР» 37
2.4.1 Кабельна система мережі 37
2.4.2 Організація робочого місця 39
2.5 Розподіл IP-адрес 39
3 АДМІНІСТРУВАННЯ ЛОКАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТВА 41
3.1 Організація мережі на базі Windows Server 41

3.1.1 MICROSOFT WINDOWS SERVER 41
3.1.2 Служби Windows Server 45
3.2 Основні адміністративні блоки 49
3.2.1 Налаштування сервера 49
3.2.2 Встановлення WINDOWS SERVER 50
3.2.3 Управління в середовищі WINDOWS SERVER 51
3.3 Захист інформації в мережі 52
3.4 Аналіз можливостей системи розмежування доступу WINDOWS SERVER 53
ВИСНОВКИ 56
ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ 57
ДОДАТОК А ПЛАН ПРИМІЩЕНЬ ТОВ «НОЙНЕР» 59
ДОДАТОК Б СХЕМА ПІДКЛЮЧЕННЯ ПРИНТЕРІВ ОРГАНІЗАЦІЇ 60
ДОДАТОК В КАБЕЛЬНА СИСТЕМА ОРГАНІЗАЦІЇ 61
ДОДАТОК Г ПЕРЕВІРКА ПРАЦЕЗДАТНОСТІ МЕРЕЖІ ЗА ДОПОМОГОЮ ПРОГРАМИ ЕМУЛЯЦІЇ МЕРЕЖІ NETEMUL 62
ДОДАТОК Д СЛАЙДИ ПРЕЗЕНТАЦІЇ 63

ПЕРЕЛІК СКОРОЧЕНЬ

CAN – (Campus Area Network) кампусна мережа;

CSMA/CD – (Carrier Sense Multiple Access with Collision Detection) множинний доступ із контролем несучої та виявленням колізій;

GAN – (Global Area Network) глобальна мережа;

LAN – (Local Area Network) локальна мережа;

MAN – (Metropolitan Area Network) мережі міського масштабу;

STP – (Shielded Twisted Pair) екранована кручена пара;

UTP – (Unshielded Twisted Pair) неекранована кручена пара;

WAN – (Wide Area Network) широкомасштабна мережа;

ЛОМ – локальна обчислювальна мережа;

СКС – структурована кабельна система.

ВСТУП

Комп’ютерна мережа є фундаментальним інструментом функціонування сучасного офісу. Об'єднання IT-інфраструктури компанії у локальну мережу (LAN) створює значні можливості для оптимізації бізнес-процесів та забезпечує високу окупність інвестицій.

Ключові переваги впровадження локальної мережі:

1. Економічна ефективність. Спільне використання периферійного обладнання (принтерів, сканерів, мережевих накопичувачів) мінімізує витрати на закупівлю техніки для кожного робочого місця. Централізація ресурсів дозволяє суттєво зменшити капітальні витрати на оснащення офісу.

2. Підвищення продуктивності. Оперативний обмін даними між співробітниками скорочує часові витрати на виконання поточних завдань, що позитивно впливає на загальні показники ефективності персоналу.

3. Робота у багатокористувацькому середовищі. Впровадження мережі є обов’язковою умовою для функціонування корпоративних систем, що забезпечує одночасну роботу з централізованою базою даних.

4. Оптимізація інтернет-з’єднання. Спільний доступ до мережі Інтернет через корпоративний шлюз є економічно доцільнішим за індивідуальні підключення. Крім того, це дозволяє впровадити ефективні інструменти моніторингу та контролю трафіку.

5. Віддалений доступ. Налаштування корпоративної мережі забезпечує безпечний доступ до робочих файлів та корпоративної пошти поза межами офісу, що є критично важливим для мобільності бізнесу.

6. Комунікаційні можливості. Розгортання внутрішніх засобів зв’язку (локальні месенджери, відеоконференції) забезпечує ефективну взаємодію між підрозділами навіть у межах масштабних офісних просторів.

7. Системне адміністрування. Мережева архітектура надає адміністраторам інструменти для централізованого контролю, обслуговування та віддаленої технічної підтримки користувачів.

Професійно спроєктована та налаштована локальна мережа є не просто технічною потребою, а стратегічним активом, що забезпечує стабільність, безпеку та масштабованість бізнес-процесів.

Метою роботи є розробка структури локальної мережі для ТОВ «НОЙНЕР» на основі аналізу теоретичних та практичних матеріалів.

Для досягнення поставленої мети передбачено вирішення таких завдань:

- обґрунтування вибору мережевої технології;
- підбір необхідного мережевого обладнання;
- проєктування схеми кабельної системи;
- розробка комплексу заходів із забезпечення інформаційної безпеки мережі.

Реалізація проєкту сприятиме оптимізації внутрішнього документообігу, підвищенню продуктивності праці та скороченню часу на опрацювання інформації. Отриманий у такий спосіб резерв часу дозволить зосередитися на розробці нових економічних та інвестиційних ініціатив, що забезпечить окупність та рентабельність інфраструктурних змін.

Інтеграція підприємства у глобальну мережу Internet відкриває широкі можливості доступу до актуальної ділової, фінансової та аналітичної інформації. Водночас виникає потреба в мінімізації ризиків, пов'язаних із захистом конфіденційної інформації від несанкціонованого доступу, що є критично важливим аспектом функціонування локальної обчислювальної мережі.

Обрана тема є актуальною, оскільки цифровізація офісної інфраструктури через впровадження локальних мереж є стратегічною необхідністю для розвитку сучасних малих підприємств.

1 ТЕОРЕТИЧНІ ОСНОВИ ПЛАНУВАННЯ ТА ПОБУДОВИ ЛОКАЛЬНИХ МЕРЕЖ

Комп'ютерна мережа - це сукупність двох або більше обчислювальних пристроїв, з’єднаних між собою за допомогою дротових або бездротових каналів зв'язку, що забезпечує обмін даними між ними [1].

Локальна мережа (LAN, Local Area Network) об'єднує комп'ютери, розміщені в межах одного приміщення або будівлі. Масштаб такої мережі визначається пропускною здатністю кабельних систем та технічними характеристиками мережевого обладнання.

Інтеграція кількох локальних мереж утворює кампусну мережу (CAN, Campus Area Network), яка охоплює сусідні будівлі або корпуси одного підприємства чи освітнього закладу. Мережі міського масштабу (MAN, Metropolitan Area Network) забезпечують взаємодію між різними кампусними або локальними мережами в межах одного міста. Широкомасштабні мережі (WAN, Wide Area Network) об'єднують сегменти мереж на рівні регіонів або областей [1].

Глобальна мережа (GAN, Global Area Network) передбачає об'єднання кількох широкомасштабних мереж у межах країни або континенту. Вершиною цієї ієрархії є мережа мереж - Інтернет, до складу якої входять Всесвітня павутина (World Wide Web), системи електронної пошти та інші інфраструктури для зберігання й передачі інформації [1].

1.1 Обладнання, що використовується для побудови комп'ютерних мереж

Для організації мережевої взаємодії необхідно об'єднати два або більше комп'ютерів у локальну мережу. Незалежно від обраного методу комунікації, процес потребує застосування відповідного обладнання. У разі використання прямого кабельного з'єднання необхідні багатожильний кабель та відповідні конектори.

Для побудови локальної обчислювальної мережі в межах офісу, будинку чи іншого приміщення необхідно використовувати мережеві адаптери та кабельні системи відповідної довжини. Залежно від масштабу та топології

мережі, до інфраструктури можуть бути включені хаби, комутатори та репітери. Локальна мережа (LAN) є комунікаційною системою, що забезпечує високошвидкісний обмін даними між комп'ютерами на обмеженій території. На відміну від неї, глобальна мережа (WAN) охоплює значні географічні відстані. Обидва типи мереж мають спільні принципи програмного забезпечення, проте суттєво відрізняються за архітектурою телекомунікаційних каналів та технічними засобами зв'язку [2].

1.2 Принципи побудови локальних мереж

Проєктування локальних комп'ютерних мереж вимагає комплексного підрахунку низки чинників, зокрема масштабу мережі, просторового розподілу вузлів та забезпечення належного рівня конфіденційності даних, що передаються. З метою вибору оптимальної архітектури мережі в кожному конкретному випадку необхідно оперувати базовою термінологією та класифікацією мережевих систем [2].

До ключових понять, що визначають характеристики комп’ютерних мереж, належать:

- мережеві компоненти;
- способи організації мережі, що регламентують доступ до даних у межах середовища передачі;
- функціональні ролі вузлів у мережі;
- топологія комп'ютерної мережі;
- технологія передачі даних;
- типи кабельних систем та фізичне середовище з'єднання;
- принципи міжмережевої взаємодії та маршрутизації.

Мережеві компоненти

Фундаментальними елементами локальної мережі є вузли (Node), об'єднані між собою кабельною інфраструктурою, яка формує окремі сегменти (Segment).

Вузли мережі, як правило, представлені робочими станціями або серверами, проте можуть включати додаткове мережеве обладнання, зокрема:

- мережеві принтери;
- концентратори (hubs);

- комутатори (switches);
- мости (bridges);
- маршрутизатори (routers).

1.3 Способи організації комп'ютерної мережі

Залежно від функціонального призначення кожного пристрою в мережі, комп'ютерні мережі класифікують на три основні типи [3]:

- однорангові;
- мережі з виділеним сервером;
- комбіновані.

В одноранговій мережі (рис. 1.1) всі робочі станції наділені рівними правами доступу. Кожен користувач самостійно визначає параметри спільного використання ресурсів свого комп'ютера, зокрема файлів, периферійних пристроїв тощо. Взаємодія вузлів у межах такої архітектури здійснюється шляхом ідентифікації пристроїв за унікальними іменами або адресами, що забезпечує стабільне функціонування мережевої інфраструктури [3].

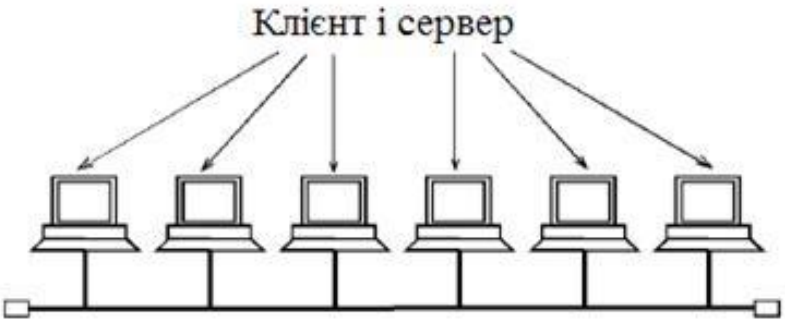


Рисунок 1.1 - Однорангова мережа

У мережах із виділеним сервером (рис. 1.2) керування правами доступу до мережевих ресурсів та процесами адресації, що передбачають присвоєння унікальних ідентифікаторів кожному вузлу, покладено на виділений сервер. За допомогою спеціалізованого програмного забезпечення сервер забезпечує унікальність мережевих адрес, гарантує цілісність передачі даних між відправником і отримувачем, а також обмежує несанкціонований доступ інших користувачів до інформації. Процеси адміністрування прав доступу та розподілу адрес здійснюються кваліфікованими фахівцями - мережевими

адміністраторами [3].

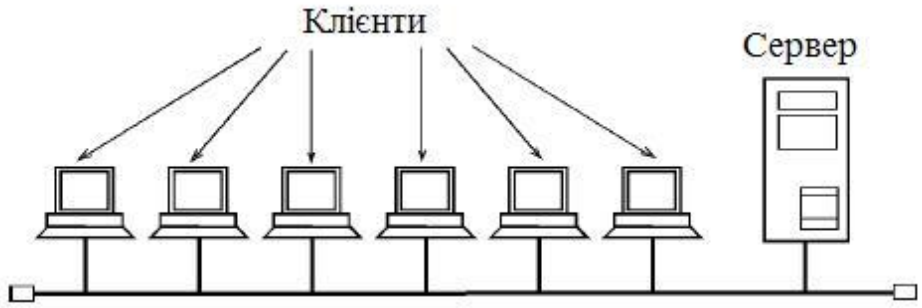


Рисунок 1.2 - Мережа з виділеним сервером

Залежно від виконуваних функцій, комп’ютер у локальній мережі класифікується як:

- робоча станція (Workstation);
- сервер (Server).

Робоча станція використовує виключно доступні їй ресурси локальної мережі.

Сервер реалізує запити робочих станцій, забезпечуючи спільний доступ до мережевих ресурсів, зокрема дискового простору, обчислювальних потужностей процесора, периферійного обладнання (принтерів, модемів тощо).

Фундаментально мережева взаємодія базується на рівні програмного забезпечення: серверне програмне забезпечення приймає запити від клієнтських додатків, здійснює їх обробку та генерує відповідну реакцію.

Класифікація серверів за функціональним призначенням

Найменування сервера зазвичай відображає його основну спеціалізацію:

- файловий сервер;
- сервер друку;
- поштовий сервер;
- сервер новин;
- Web-сервер;
- сервер баз даних;
- факс-сервер.

Класифікація за характером використання

Сервери поділяються на виділені та невиділені.

Виділений сервер спеціалізується виключно на наданні ресурсів у спільне користування. Такий сервер не призначений для прямої взаємодії з користувачем, тому може експлуатуватися без інтерфейсних пристроїв (монітора, клавіатури). Обладнання та програмне забезпечення таких систем характеризуються підвищеною надійністю та продуктивністю. До поширених операційних систем для виділених серверів належать:

- NetWare (Novell);
- LAN Server (IBM);
- LAN Manager (Microsoft);
- сімейство Windows Server (Microsoft).

Невиділений сервер поєднує функції сервера та робочої станції. Він дозволяє надавати окремі ресурси локального комп’ютера для спільного мережевого доступу. Прикладами операційних систем для невиділених серверів є:

- NetWare Lite (Novell);
- LANtastic (Artisoft);
- сімейство Windows NT Workstation та Windows (Microsoft).

Особливості мережевих архітектур

В одноранговых мережах комп'ютери функціонують як робочі групи, де кожен вузол одночасно виступає в ролі клієнта та невиділеного сервера. Попри простоту адміністрування, такі мережі мають обмежений рівень інформаційної безпеки.

На противагу їм, мережі з виділеним сервером забезпечують вищий рівень надійності та захищеності даних, централізовано розміщених на сервері.

1.4 Топології локальних мереж

Комп’ютери та інші компоненти локальної мережі можуть бути об’єднані за допомогою різних конфігурацій. Схему фізичного розміщення мережевих вузлів називають топологією (Topology). Вона визначається геометричною структурою ліній зв’язку або взаємним розташуванням підключених пристроїв. Топологія мережі є ключовою характеристикою, що застосовується для

класифікації та порівняльного аналізу комп'ютерних мереж [3].

Виділяють три базові топології побудови локальних мереж:

- зірка (Star);
- кільце (Ring);
- шина (Bus).

Зірка (Star)

У мережі з топологією «зірка» (рис. 1.3) усі робочі станції підключені до центрального вузла (хаба). Передача даних здійснюється через цей центральний елемент, який спрямовує інформацію безпосередньо отримувачу. Прямі з'єднання між окремими комп'ютерами у такій мережі відсутні; обмін даними відбувається виключно через центральний пристрій. Роль хаба найчастіше виконує концентратор - багатопортовий репітер (повторювач). Його основна функція полягає у прийнятті сигналу на одному з портів та його негайній ретрансляції на всі інші порти [4].

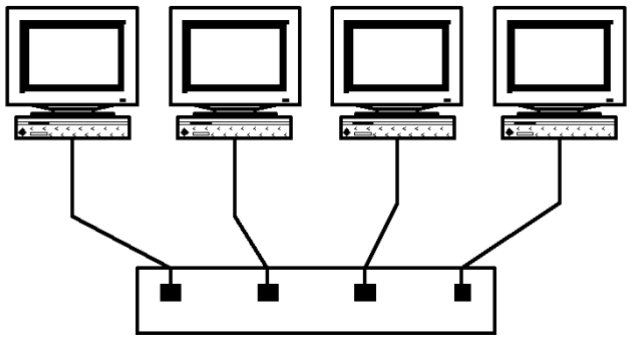


Рисунок 1.3 - Топологія «зірка»

Побудова мережі з топологією «зірка» характеризується простотою реалізації та високою ефективністю. У разі пошкодження кабелю, що з'єднує окремий вузол із центральним комутатором, функціонування решти сегментів мережі зберігається. Проте вихід з ладу центрального пристрою призводить до повної зупинки обміну даними між усіма вузлами мережі.

Переваги топології «зірка» [4]:

- локалізація несправності в окремому кабельному сегменті не впливає на працездатність усієї мережі;
- продуктивність мережі залишається стабільною навіть при підключенні значної кількості пристроїв;

- високий рівень інформаційної безпеки, оскільки дані передаються адресно і не надходять на інші робочі станції.

Недоліки топології «зірка» [4]:

- значна витрата кабельної продукції для підключення вузлів;

- критична залежність працездатності мережі від надійності центрального вузла;

- суттєві фінансові витрати при масштабуванні мережі.

Кільцева топологія

Топологія типу «кільце» передбачає відсутність кінцевих точок з'єднання, формуючи замкнену структуру, у якій кожен вузол з'єднаний із двома сусідніми [4].

У мережах такої архітектури передача даних здійснюється послідовно в одному напрямку. Доступ до середовища передачі даних регулюється за допомогою спеціального маркера: робоча станція має право надсилати інформацію лише після отримання цього сигналу.

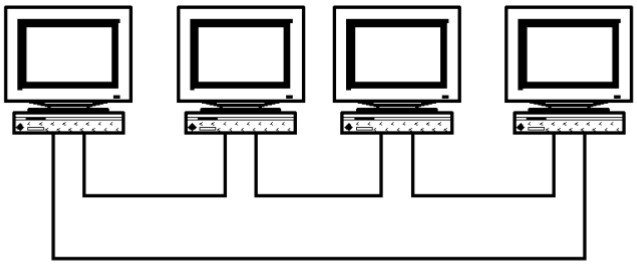


Рисунок 1.4 – Топологія «кільце»

Переваги кільцевої топології [4]:

- мінімальний рівень зниження продуктивності при масштабуванні мережі та підключенні великої кількості вузлів.

Недоліки кільцевої топології [4]:

- низька відмовостійкість: пошкодження лінії зв'язку в будь-якому сегменті призводить до виходу з ладу всієї локальної мережі;

- обмежений рівень інформаційної безпеки: оскільки дані проходять через усі вузли мережі, існує ризик несанкціонованого перехоплення конфіденційної інформації пристроями, які не є її адресатами.

Топологія «шина»

Топологія «шина» передбачає використання єдиного спільного каналу передачі даних (переважно на основі коаксіального кабелю), до якого підключені всі вузли локальної мережі [4].

Принцип функціонування мережі з топологією «шина» (рис. 1.5) полягає в наступному: під час відправлення даних одним із комп'ютерів сигнал поширюється кабелем в обох напрямках. Хоча дані отримують усі підключені пристрої, обробляє їх виключно той вузол, якому вони адресовані. Передача даних у такій структурі може здійснюватися одночасно в обох напрямках. Для запобігання відбиттю сигналу на протилежних кінцях шини встановлюються спеціальні термінатори (узгоджувальні елементи).

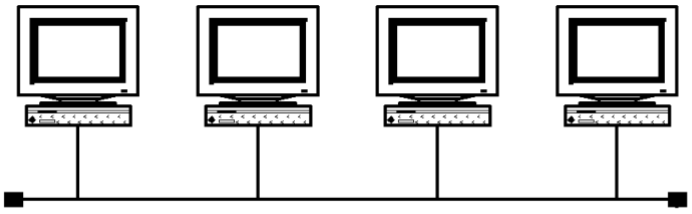


Рисунок 1.5 – Топологія «шина»

Переваги топології «шина» [4]:

- простота масштабування мережевої інфраструктури;
- економічна ефективність за рахунок відносно низької вартості необхідного обладнання.

Недоліки топології «шина» [4]:

- критична вразливість: пошкодження магістрального кабелю призводить до відмови всієї локальної мережі;
- зниження продуктивності при збільшенні кількості підключених вузлів;
- низький рівень інформаційної безпеки.

1.5 Огляд мережевих технологій

Поняття технології та топології локальних мереж часто ототожнюються, проте вони мають принципово різні значення. Топологія мережі визначає її геометричну конфігурацію та схему фізичних з’єднань між вузлами. Натомість

мережева технологія охоплює сукупність стандартів, що регламентують процеси передачі даних, а також специфікації апаратної реалізації мережевих адаптерів та закладених у них протоколів обміну інформацією.

Мережевий адаптер - це спеціалізований електронний пристрій, призначений для забезпечення обміну даними між комп'ютерами в межах мережі. Конструктивно адаптер зазвичай виконаний у формі друкованої плати, що встановлюється у відповідний слот розширення материнської плати (наприклад, PCI або PCIe) та обладнана зовнішніми роз'ємами для підключення кабельної системи. Варто зазначити, що в сучасних комп'ютерних системах мережеві контролери переважно інтегровані безпосередньо в системну плату [5].

До найбільш значущих та поширених мережевих технологій належать:

- Ethernet;
- ARCNET;
- IBM Token Ring;
- FDDI;
- 100VG-AnyLAN.

Технологія *Ethernet*, розроблена компанією Xerox у 1973 році, забезпечує реалізацію мереж із топологіями «зірка» або «шина». Використання коаксіального кабелю передбачає шинну конфігурацію, тоді як застосування витої пари дозволяє реалізувати топологію «зірка». Завдяки оптимальному співвідношенню ціни та якості, масштабованості та широкій підтримці з боку виробників обладнання, Ethernet став домінуючим стандартом у галузі. Відповідно, подальший аналіз побудови мереж у межах цього матеріалу буде зосереджений переважно на технології Ethernet [5].

Технологія *ARCNET*, створена корпорацією Datapoint, аналогічно до Ethernet, підтримувала топології «зірка» та «шина». Вона широко застосовувалася в мережах Novell NetWare 2.x. Попри історичну значущість, на сьогодні ця технологія вважається застарілою і практично не використовується в сучасних інфраструктурах [5].

Технологія *Token Ring*, представлена компанією IBM у 1986 році, базується на змішаній топології (фізична «зірка» з логічним «кільцем»). Вузли підключаються до пристрою, що має назву MAU (Multistation Access Unit), який виконує функції центрального концентратора. Завдяки дуплексній системі

передачі даних, мережа функціонує як логічне кільце, фізично структуроване за принципом «зірки» [5].

Попри технологічні особливості, системи Token Ring суттєво програють рішенням на базі Ethernet у питанні економічної доцільності: вартість мережевих адаптерів та активного обладнання Token Ring може в 3–5 разів перевищувати аналоги для Ethernet. Обмежене коло виробників та вища складність обслуговування стали ключовими факторами, що зумовили витіснення Token Ring з ринку на користь більш гнучких та доступних Ethernet-технологій [5].

Порівняльна характеристика розглянутих технологій передачі показано в табл. 1.1.

Таблиця 1.1 - Параметри базових варіантів стандартних мереж

Параметр мережі	Ethernet	Token-Ring	Arcnet	FDDI	100VG-AnyLAN
Стандарт	IEEE 802.3	IEEE 802.5	Datapoint	ISO 9314	IEEE 802.12
Топологія	Шина	Кільце	Шина	Кільце	Зірка
Швидкість передачі	10 (100) Мбіт/с	(16) Мбіт/с	2,5 Мбіт/с	100 Мбіт/с	100 Мбіт/с
Довжина	5 км	120 м	6 км	20 км	1 км
Середа	КК	КП	КК	ОВ	КП
Метод управління	CSMA/CD	Маркер	Маркер	Маркер	Центр
Код	Манчестер	Біфазний	Arcnet	4B/5B	5B/6B
Кількість	До 1024	До 260	До 255	До 1000	До 1024
КК - коаксіальний кабель, КП - кабель на кручених парах, ОВ - оптоволоконний кабель					

1.6 Кабелі, що застосовуються в локальних мережах

Для організації комп’ютерних мереж найчастіше застосовуються кабельні системи на основі мідних провідників. Поряд із ними існують волоконно-оптичні системи (Fiber-optic cable), які характеризуються вищою пропускною здатністю та мінімальними втратами сигналу. Зважаючи на вищу вартість оптичного обладнання, його використання є доцільним для передачі значних обсягів даних на великі відстані, зокрема при побудові магістральних мереж міського, міжміського чи міжнародного рівнів. Альтернативні методи передачі даних, такі як радіозв’язок та технології на основі інфрачервоного

випромінювання, наразі не набули широкого поширення [6].

Електричні кабельні системи базуються на використанні двох основних типів середовищ передачі: екранованого коаксіального кабелю з хвильовим опором 50 Ом та витої пари.

Вита пара, що складається з двох ізольованих скручених мідних провідників, у базовому виконанні не призначена для безпосереднього з'єднання комп'ютерів і застосовується переважно в межах комутаційного обладнання. Для мережевої взаємодії використовуються багатожильні кабелі, що об’єднують декілька пар (від 3 до 1000 і більше) у спільній ізоляційній оболонці. Залежно від діапазону робочих частот, виті пари класифікуються за відповідними категоріями, наведеними в таблиці 1.2.

Таблиця 1.2 – Категорії кручених пар

Категорія	Клас	Смуга частот, МГц
1	A	до 0,1
2	B	до 1
3	C	до 16
4		до 20
5	D	до 100
6	E	до 200
7	F	до 600

Кабель типу «кручена пара» класифікується на екранований (STP - Shielded Twisted Pair) та неекранований (UTP - Unshielded Twisted Pair). Конструкція екранованої крученої пари передбачає різні варіанти екранування, що забезпечує підвищений рівень захисту від електромагнітних завад порівняно з неекранованими аналогами, проте зумовлює вищу вартість виробу. У кабельних системах стандарту Ethernet найпоширенішим рішенням є використання неекранованого кабелю категорії 5, що складається з чотирьох кручених пар [6].

Бездротові мережі

Бездротові мережеві технології охоплюють широкий діапазон рішень - від глобальних систем передачі даних до локальних радіо- та інфрачервоних каналів зв'язку. Ці технології інтегруються в широкий спектр пристроїв: від стаціонарних комп'ютерів та ноутбуків до портативних мобільних пристроїв.

Вони забезпечують мобільність користувачів, дозволяючи отримувати доступ до електронної пошти, ресурсів Інтернету в громадських місцях або синхронізувати дані в домашніх умовах [7].

Застосування бездротових технологій дозволяє оптимізувати витрати на створення інфраструктури, виключаючи необхідність прокладання кабельних ліній зв’язку при збереженні функціональності дротових мереж. Обмін даними здійснюється за допомогою внутрішніх або зовнішніх адаптерів, які транслюють інформаційні пакети у вигляді радіосигналів у визначеному частотному діапазоні.

1.7 Мережне обладнання

Для детального аналізу процесу міжмережевого обміну даними розглянемо взаємодію двох локальних мереж (А та Б), поєднаних через спільну точку доступу - вузол (Node) (рис. 1.6). У даному мережевому вузлі розміщується спеціалізоване обладнання або комп’ютер з двома мережевими адаптерами, що виконує одну з наступних функцій [7]:

- повторювач (Repeater);
- комутатор (Switch);
- міст (Bridge);
- маршрутизатор (Router), що іноді визначається як міжмережевий шлюз (Gateway).

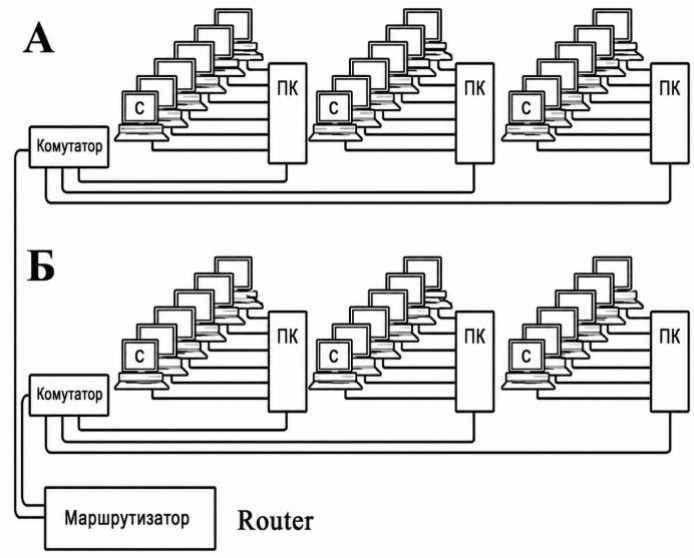


Рисунок 1.6 - Об'єднання двох підмереж

Вибір мережевого обладнання для вузлових точок зумовлений рівнем необхідної мережевої інтеграції.

Повторювач (репітер) застосовується для поєднання віддалених сегментів однієї мережі. Його функція полягає у підсиленні сигналу в обох напрямках, що забезпечує прозорість передачі даних для підключених пристроїв [8].

Міст є більш функціональним пристроєм, призначеним для з'єднання локальних мереж, що базуються на єдиній технології. На відміну від повторювача, міст забезпечує фільтрацію трафіку, пропускаючи лише ті дані, які адресовані пристроям в іншому сегменті, одночасно виконуючи підсилення сигналу. Використання мостів дозволяє усунути обмеження щодо максимальної кількості кабельних сегментів. Попри поширеність у середовищі Novell NetWare, у сучасних системах Windows вони використовуються рідше, поступаючись місцем маршрутизаторам [8].

Маршрутизатор (міжмережевий шлюз) виконує складніші функції. Він володіє індивідуальною адресою в кожній підмережі та забезпечує взаємодію між мережами з різними технологічними стандартами (наприклад, Ethernet та Token Ring), а також різними фізичними середовищами передачі даних. Масштабованість мереж, об’єднаних за допомогою маршрутизаторів, є практично необмеженою; саме такий принцип лежить в основі архітектури мережі Інтернет [8].

Як правило, роль маршрутизатора виконує комп’ютер з двома мережевими адаптерами, підключеними до відповідних сегментів. Для забезпечення безперервності зв’язку такий вузол має функціонувати постійно.

Принцип передачі даних у межах однієї мережі (наприклад, мережі А або В) реалізується шляхом прямої доставки пакетів: приймальний пристрій ідентифікує власну адресу, незалежно від топології мережі (шина, зірка чи кільце) або використовуваної технології. Маршрутизатор у такому процесі не задіюється (рис. 1.7).

У випадку, якщо комп’ютер з однієї мережі (мережа А) ініціює передачу даних до пристрою в іншій мережі (мережа В), відправник виявляє, що адреса отримувача виходить за межі діапазону локальної мережі. У такому разі пакет перенаправляється на шлюз - функціональний компонент маршрутизатора,

який здійснює подальшу маршрутизацію.

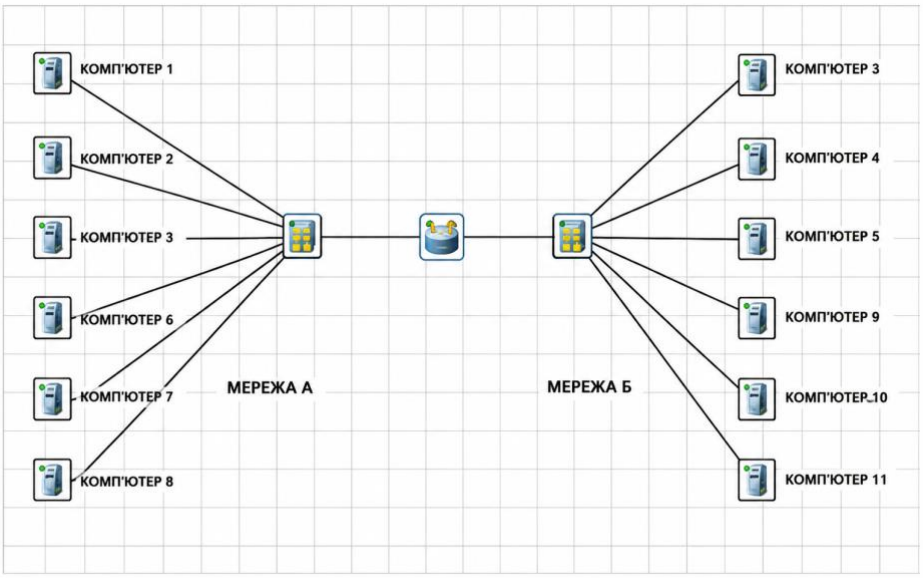


Рисунок 1.7 – Приклад маршрутизації між мережами

Отримавши пакет даних, маршрутизатор аналізує власну таблицю маршрутизації (Routing Table) та ініціює його перенаправлення через шлюз B. Після доставки пакета в цільову мережу через зазначений шлюз, дані успішно отримуються кінцевим пристроєм.

Наведена схема є спрощеною моделлю. У реальних умовах маршрутизатор може підтримувати з’єднання з кількома мережами одночасно, а кінцевий отримувач не обов’язково має бути безпосередньо підключений до сегмента мережі, через який здійснюється передача.

Після ознайомлення з теоретичними засадами побудови локальних мереж, перейдемо до практичної реалізації локальної мережі для ТОВ «НОЙНЕР».

У першому розділі проаналізовано теоретичні засади проєктування локальних обчислювальних мереж (ЛОМ), зокрема розглянуто мережеві технології, необхідне апаратне забезпечення, фундаментальні принципи побудови та методи організації мережевої інфраструктури. Також висвітлено питання мережевих топологій, типи кабельних з’єднань, принципи міжмережевої взаємодії та маршрутизації трафіку.

2 ОРГАНІЗАЦІЯ ЛОКАЛЬНОЇ МЕРЕЖІ ДЛЯ ОРГАНІЗАЦІЇ ТОВ «НОЙНЕР»

2.1 Постановка завдання

Метою кваліфікаційної роботи є проєктування локальної комп'ютерної мережі для ТОВ «НОЙНЕР».

Для досягнення поставленої мети необхідно вирішити такі завдання:

– обґрунтування вибору мережевої архітектури (метод доступу, топологія, тип кабельної системи);

– визначення методології управління мережевою інфраструктурою;

– конфігурація мережевого обладнання (визначення кількості серверів, комутаційного обладнання та периферійних пристроїв);

– оптимізація управління мережевими ресурсами та обліковими записами користувачів;

– розробка комплексу заходів із забезпечення інформаційної безпеки;

– техніко-економічне обґрунтування витрат на реалізацію проєкту.

Ключовим завданням роботи є розробка раціональної та гнучкої структурної схеми мережі підприємства, впровадження ефективних механізмів оновлення оперативної інформації на сервері, а також забезпечення належного рівня захисту даних.

2.2 Функціональна схема локальної обчислювальної мережі

Нижче представлено опис організаційно-штатної структури підрозділу. Вище керівництво здійснює директор підприємства. Структура підрозділу передбачає функціонування чотирьох відділів, один із яких перебуває у прямому підпорядкуванні начальника. Кожен із відділів включає відповідну кількість відділень, чисельність персоналу в яких визначена штатним розкладом.

Візуалізацію зазначеної структури наведено на рис. 2.1.

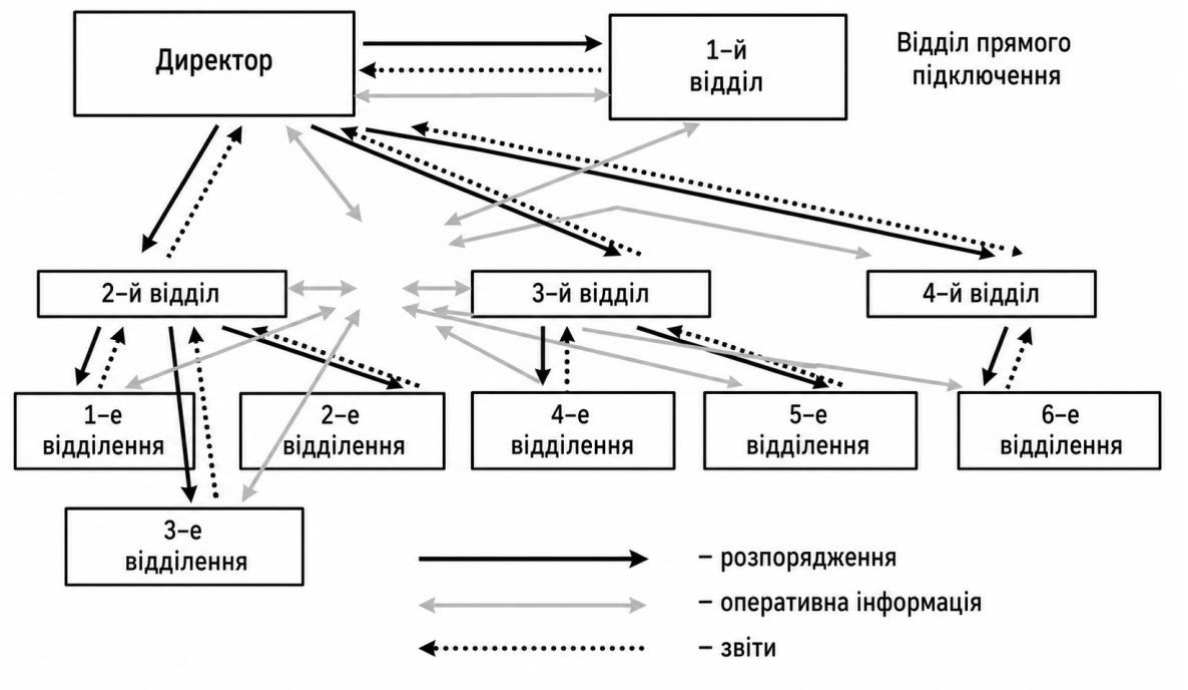


Рисунок 2.1 – Організаційна структура організації

Штат підрозділу налічує 23 особи; для кожного співробітника передбачено забезпечення персональним комп’ютером.

2.3 Планування структури локальної мережі

2.3.1 Комп'ютерна мережа

Комп’ютерна мережа являє собою сукупність обчислювальних пристроїв, розміщених на обмеженій території (в межах одного приміщення або комплексу близько розташованих будівель) та об'єднаних єдиними каналами зв’язку. На сучасному етапі більшість таких інфраструктур представлені локальними мережами (Local Area Network - LAN), що функціонують в межах офісного простору на основі архітектури «клієнт-сервер». Мережеве з’єднання включає два вузли, що здійснюють обмін даними, та середовище передачі інформації між ними. Попри розвиток бездротових технологій, їх застосування у побудові масштабних корпоративних мереж залишається обмеженим [9].

У межах моделі «клієнт-сервер» взаємодія розподіляється на два сегменти: клієнтський та серверний. Клієнт ініціює запити на отримання інформації або послуг, тоді як сервер забезпечує їх обробку та надання відповіді. У багатьох конфігураціях вузли можуть одночасно виконувати функції як клієнта, так і сервера. Процес проектування комп’ютерної мережі

передбачає вибір технологічних компонентів, що визначають подальшу сумісність програмного та апаратного забезпечення. Комп'ютерна мережа є базовим елементом сучасної бізнес-інфраструктури, де корпоративна мережа виступає лише одним із прикладних рішень. Відповідно, при виборі мережевих компонентів слід враховувати ширший контекст інфраструктурних вимог. Технології для Intranet повинні інтегруватися в наявну мережу як доповнення, не спричиняючи при цьому радикальних змін у її архітектурі [10].

2.3.2 Способи управління мережею

Конфігурація мережі кожної організації формується відповідно до специфіки її діяльності та оперативних завдань. Ключовим етапом проектування є визначення загальної кількості користувачів, оскільки цей показник є базовим для подальшого технічного планування інфраструктури.

Вибір топології мережі зумовлений кількістю робочих станцій та ієрархічною моделлю управління компанією:

1. Для організацій з горизонтальною структурою, що передбачає вільний обмін даними між співробітниками, найбільш ефективним рішенням є однорангова мережа.

2. Для компаній із вертикальною структурою управління, що потребують чіткої регламентації доступу до інформаційних ресурсів, доцільним є впровадження архітектури з виділеним сервером. Це забезпечує можливість централізованого адміністрування прав доступу та належний рівень безпеки.

У межах поточної роботи необхідно інтегрувати в локальну мережу 23 робочі станції, розподілені за такими функціональними підрозділами:

- керівництво підприємства - 1 робоча станція;
- відділ прямого підпорядкування - 2 робочі станції;
- секретаріат - 1 робоча станція;
- відділ №2: відділення 1 (3 станції), відділення 2 (2 станції), відділення 3 (4 станції);
- відділ №3: відділення 4 (3 станції), відділення 5 (4 станції);
- відділ №4: відділення 6 (3 станції).



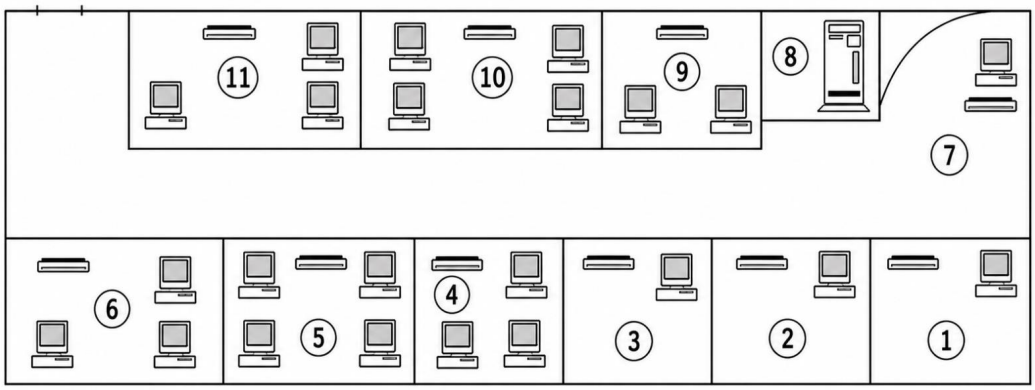
Рисунок 2.2 – Вибір типу мережі

Аналіз критеріїв вибору типу мережі свідчить про доцільність впровадження серверної архітектури, що зумовлено вертикальною структурою підприємства та необхідністю розмежування доступу до інформаційних ресурсів.

Важливим етапом проектування є розробка попередньої схеми мережі. Під час планування необхідно враховувати обмеження довжини кабельних сегментів. Якщо для мереж у межах одного приміщення цей чинник може бути несуттєвим, то при масштабуванні мережі на кілька рівнів будівлі виникає потреба у використанні додаткового мережевого обладнання, зокрема репітерів або комутаторів. З огляду на те, що інфраструктура організації розташована в межах одного поверху, а відстань між сегментами мережі не перевищує допустимих значень, застосування репітерів не є необхідним.

2.3.3 Планування мережі в приміщеннях

План приміщень (рис. 2.3) має вагомий вплив на вибір топології мережі, що потребує детального врахування під час проектування.



1. Кабінет директора підприємства.
2, 3. Відділ прямого підключення.
4. Відділення 4-го відділу.
5, 6. Відділення 4-го та 3-го відділів.
7. Секретарі.
8. Кімната системного адміністратора.
9, 10, 11. Відділення 1-го, 2-го та 3-го відділів.

Рисунок 2.3 – План приміщення

Після визначення місця встановлення сервера можна відразу визначити, яка кількість кабелю буде потрібна.

2.3.4 Розміщення сервера

На відміну від розгортання одноранговоі мережі, побудова локальної мережі на базі сервера потребує врахування стратегічного розміщення обладнання. Вибір місця встановлення зумовлений такими ключовими факторами [10]:

- акустичний комфорт: через високий рівень шуму під час роботи серверного обладнання доцільно розміщувати його окремо від робочих місць персоналу;

- експлуатаційна доступність: необхідно забезпечити безперешкодний доступ для проведення технічного обслуговування;

- інформаційна безпека: з метою захисту даних доступ до фізичного носія сервера має бути суворо обмеженим.

На основі аналізу приміщень було визначено оптимальну локацію, що не потребує перепланування простору. Приміщення № 8 обрано як найбільш відповідне встановленим вимогам. Це рішення аргументоване мінімальним рівнем шуму та високим ступенем ізоляції, що забезпечує належний контроль доступу (рис. 2.3).

Крім того, таке розміщення спрощує процедури технічного

обслуговування: встановлення сервера в кабінетах керівництва створювало б незручності через безперервний робочий процес, а в кабінеті відділу кадрів неможливо забезпечити належний захист від сторонніх осіб. Розміщення обладнання в інших приміщеннях визнано нераціональним через невідповідність жодній із наведених умов.

2.3.5 Планування мережевої архітектури

Мережева архітектура являє собою сукупність топології, методів доступу та технічних стандартів, необхідних для функціонування мережевої інфраструктури.

Вибір топології зумовлений плануванням приміщень, у яких розгортається локальна обчислювальна мережа (ЛОМ). Також значний вплив на прийняття рішень мають економічні чинники, зокрема витрати на придбання та монтаж мережевого обладнання, вартість якого суттєво варіюється залежно від технічних вимог підприємства.

Топологія типу «зірка» є високоефективною структурою, у якій кожен вузол, включно із сервером, підключається окремим сегментом кабелю до центрального концентратора або комутатора. Ключовою перевагою такої архітектури є відмовостійкість: збої в роботі окремих робочих станцій або пошкодження кабельних ліній не впливають на стабільність функціонування всієї мережі. На рисунку 2.4 відображено топологію мережі організації.

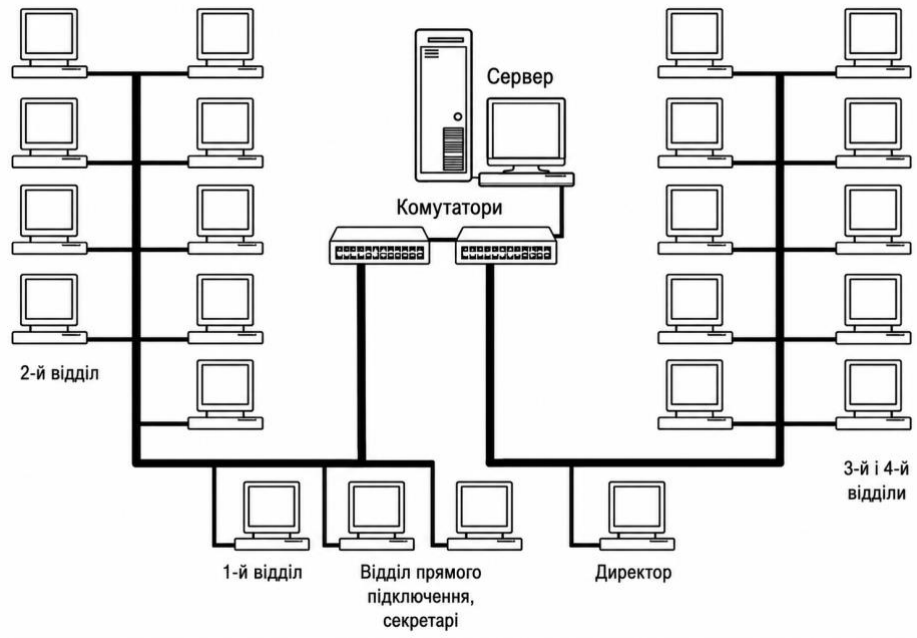


Рисунок 2.4 – Топологія мережі організації

Ключовим аспектом функціонування локальних мереж є методи доступу, що визначають протокол взаємодії робочих станцій з мережевими ресурсами.

Технологія CSMA/CD (Carrier Sense Multiple Access with Collision Detection - множинний доступ із контролем несучої та виявленням колізій) забезпечує рівноправний доступ усіх вузлів до мережевого середовища. Алгоритм передбачає попередню перевірку вільності каналу перед ініціацією передачі даних. Після завершення транзакції станція верифікує доставку пакета адресату. У разі невдачі реалізується механізм повторних спроб до моменту успішного підтвердження отримання інформації [1].

Враховуючи ефективність цього методу в масштабах малих та середніх підприємств, а також його інтеграцію в архітектуру Fast Ethernet, вибір даного рішення є доцільним для потреб організації.

Технологія Ethernet була ініційована корпорацією Xerox наприкінці 70-х років. Згодом до розробки приєдналися Digital Equipment Corporation (DEC) та Intel Corporation. Оновлена специфікація Ethernet v.2.0 була опублікована у 1982 році, що заклало основу для стандарту IEEE 802.3, розробленого інститутом IEEE [2].

На сьогодні стандартом де-факто є технологія Fast Ethernet (IEEE 802.3u), що використовує кабель типу «кручена пара» (100Base-TX), який вирізняється простотою монтажу та експлуатації.

Мережі на базі крученої пари зазвичай реалізуються за топологією «зірка». Попри необхідність використання більшої кількості кабельної продукції порівняно з коаксіальними аналогами, відносно низька вартість крученої пари та висока відмовостійкість роблять цей вибір оптимальним. Несправність окремої станції не порушує цілісність системи, проте вихід із ладу концентратора (хаба) призводить до зупинки роботи підключеного сегмента [5].

Важливою перевагою обраного рішення є масштабованість: використання каскадного з’єднання хабів дозволяє підключити до 1024 робочих станцій. При застосуванні неекранованої крученої пари (UTP) гранична довжина сегмента між концентратором та станцією обмежена 100 метрами (рекомендовано до 90 метрів), що відповідає архітектурним особливостям нашого підприємства.

2.3.6 Організація спільного доступу

Наступним етапом проектування мережевої інфраструктури є організація спільного доступу до периферійних пристроїв, зокрема принтерів, факсів та модемів.

Ці ресурси можуть бути інтегровані як у однорангові мережі, так і в мережі з виділеним сервером. В однорангових мережах реалізація спільного доступу має суттєві обмеження: функціонування периферійних пристроїв залежить від стану робочої станції, до якої вони підключені. У разі вимкнення такої станції доступ до відповідних служб для інших користувачів припиняється.

Натомість у мережах із виділеним сервером забезпечується стабільна робота периферії. Сервер функціонує в безперервному режимі (за винятком регламентних технічних робіт), що гарантує цілодобовий доступ робочих станцій до мережевих ресурсів.

Для підприємства, де наявні десять принтерів, розміщених у різних приміщеннях, розглянуто наступні методи підключення до локальної обчислювальної мережі (ЛОМ):

1. Підключення до робочої станції. Принтер під’єднується до найближчого комп’ютера, який виконує роль сервера друку. Недоліками цього методу є зниження продуктивності робочої станції під час обробки завдань друку, а також ризик втрати доступу до принтера в разі вимкнення цієї станції.

2. Безпосереднє підключення до мережевого сервера. Пристрій під’єднується до паралельного порту сервера. Це забезпечує постійну доступність принтера, проте вимагає врахування обмежень на довжину кабелю, що може призвести до додаткових витрат на монтаж комунікацій (прокладання в коробах або перекриттях).

3. Використання спеціального мережевого інтерфейсу. Принтер оснащується мережевою картою та підключається до мережі як окремий вузол. Сервер передає завдання на друк безпосередньо на мережеву адресу пристрою. Попри технічну ефективність, цей спосіб є капіталомістким через високу вартість мережевих інтерфейсних карт.

4. Застосування виділеного сервера друку. Пристрій являє собою окремий мережевий інтерфейс з портами для підключення одного або кількох принтерів. З огляду на специфіку поточних завдань, використання цього рішення визнано

недоцільним.

Зважаючи на економічні чинники та необхідність оптимізації витрат, найбільш доцільним для поточних умов є підключення принтерів до робочих станцій (рис. 2.5). Це рішення обґрунтоване тим, що принтери локалізовані поблизу тих робочих місць, де потреба в них є найбільш інтенсивною.

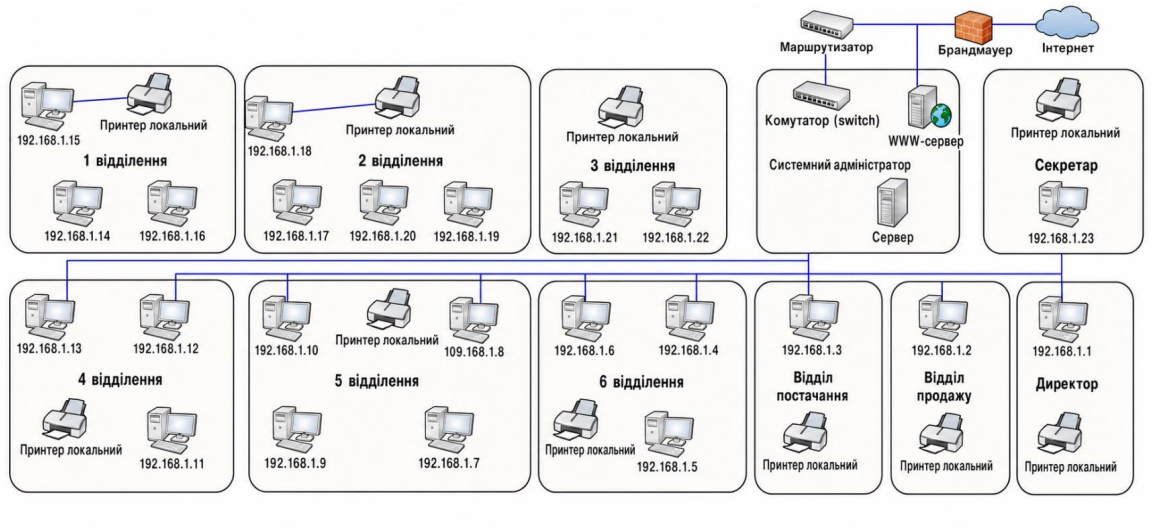


Рисунок 2.5 - Схема підключення принтерів організації

2.3.7 Розрахунок кількості кабелю та кабель-каналу

При розрахунку довжини горизонтального кабелю необхідно враховувати наступні вихідні положення. Кожна телекомунікаційна розетка з’єднується з комутаційним обладнанням кросової шафи поверху окремою кабельною лінією. Відповідно до вимог стандарту ISO/IEC 11801, довжина кабелів горизонтальної підсистеми не повинна перевищувати 90 метрів. Прокладання кабельних магістралей здійснюється в кабельних каналах з урахуванням усіх технологічних спусків, підйомів та поворотів траси [11].

Для обчислення необхідної кількості кабелю горизонтальної підсистеми застосовують два основні методи:

- метод підсумовування;

- емпіричний метод.

Метод підсумовування передбачає детальний розрахунок довжини кожної кабельної траси з наступним їх додаванням. До отриманого значення додається технологічний запас у розмірі до 10%, а також резерв довжини, необхідний для термінування кабелю в розетках та на комутаційних панелях. Перевагою цього методу є висока точність розрахунків. Проте, за відсутності спеціалізованого

програмного забезпечення, такий підхід є надмірно трудомістким, особливо для структурованих кабельних систем (СКС) з великою кількістю портів, що ускладнює порівняльний аналіз варіантів організації системи. Зазначений метод доцільно використовувати лише за наявності інструментів автоматизованого проектування (наприклад, CADdy), які забезпечують автоматизацію рутинних операцій з обліку геометрії трас та загальної довжини кожного кабельного з’єднання [11].

Розрахунок кількості кабелю методом підсумовування наведено в табл. 2.1.

Таблиця 2.1 - Розрахунок довжини кабелю методом підсумовування

№ приміщення	Кількість комп'ютерів	№ комп'ютера	Довжина кабелю (м)
1	1	1	30
2	1	2	35
3	1	3	40
4	3	4	50
		5	45
		6	45
5	4	7	60
		8	60
		9	55
		10	55
6	3	11	70
		12	65
		13	65
7	1	23	10
9	2	21	10
		22	15
10	4	17	20
		18	20
		19	25
		20	25
11	3	14	30
		15	30
		16	35
	23		895
З урахуванням 10% запасу			985

У межах даної роботи доцільним є використання емпіричного методу, що

ґрунтується на положеннях центральної граничної теореми теорії ймовірностей. Практичний досвід проектування підтверджує ефективність цього підходу для кабельних систем, що налічують понад 30 робочих місць. Сутність методу полягає у застосуванні узагальненої емпіричної формули для розрахунку загальної довжини горизонтального кабелю, необхідної для реалізації конкретної кабельної системи.

На основі сформульованих припущень середню довжину кабельних трас (Lav) визначено таким чином:

$$L_{av} = \frac{(L_{\max} + L_{\min})}{2} \cdot K_s + X, \tag{2.1}$$

де L_{min} та L_{max} - мінімальна та максимальна довжина кабельної траси від точки введення кабельних каналів у кросове приміщення до телекомунікаційної розетки найбільш наближеного та найбільш віддаленого робочого місця відповідно, розрахована з урахуванням траєкторії прокладання, включаючи всі спуски, підйоми, повороти, проходження міжповерхових перекриттів тощо;

K_s - коефіцієнт технологічного запасу, що становить 1,1 (10 %).

$$X = X1 + X2$$

Запас довжини для обробки кабелю з боку робочої зони (X1) становить 30 см. З боку кросового приміщення (X2) цей показник залежить від його габаритів і відповідає відстані від точки введення горизонтальних кабелів до найвіддаленішого комутаційного елемента, з урахуванням усіх вертикальних і горизонтальних переходів та поворотів траси. Після цього розраховується загальна кількість кабельних ліній (N_{cr}), які можна прокласти з однієї котушки:

$$N_{cr} = \frac{L_{cb}}{L_{av}}, \tag{2.2}$$

де L_{cb} - довжина кабелю в бухті (стандартні номінали: 305, 500 та 1000 м). Отриманий результат підлягає округленню в меншу сторону до найближчого цілого числа. На завершальному етапі розраховується загальна довжина кабелю

L_c, необхідна для реалізації кабельної системи:

$$L_c = L_{cb} \cdot \frac{N_{to}}{N_{cr}}, \tag{2.3}$$

де N_{t0} - кількість телекомунікаційних розеток.

За результатами емпіричних розрахунків встановлено наступні параметри: довжина максимального сегмента кабелю становить 70 метрів, мінімального - 10 метрів; загальна кількість кабельних ліній - 23 одиниці.

Згідно з наведеними вище формулами, розрахункова довжина необхідного кабелю становить 1012 метрів. З огляду на отримані дані, для реалізації проєкту доцільно придбати 4 бухти крученої пари UTP (по 305 метрів). Зазначений обсяг передбачає технологічний запас, необхідний для монтажних робіт та подальшої експлуатації мережі.

Розрахунок потреби в кабель-каналах здійснено на основі сумарного периметра приміщень, що становить 190,0 метрів. Кількість кутових елементів розрахована як 20% від загальної довжини кабель-каналів.

На основі проведених розрахунків можна зробити висновок про обґрунтованість отриманих показників з урахуванням допустимої похибки.

2.4 Структура локальної комп'ютерної мережі (ЛКМ) організації ТОВ «НОЙНЕР»

2.4.1 Кабельна система мережі

Офіс ТОВ «НОЙНЕР» розташований на другому поверсі будівлі та займає площу 150 кв. м. Планування приміщення передбачає наявність десяти кабінетів, сполучених центральним коридором. Кабельна мережа (рис. 2.6) прокладена в міжповерховому просторі між фальшпідлогою та плитами перекриття.

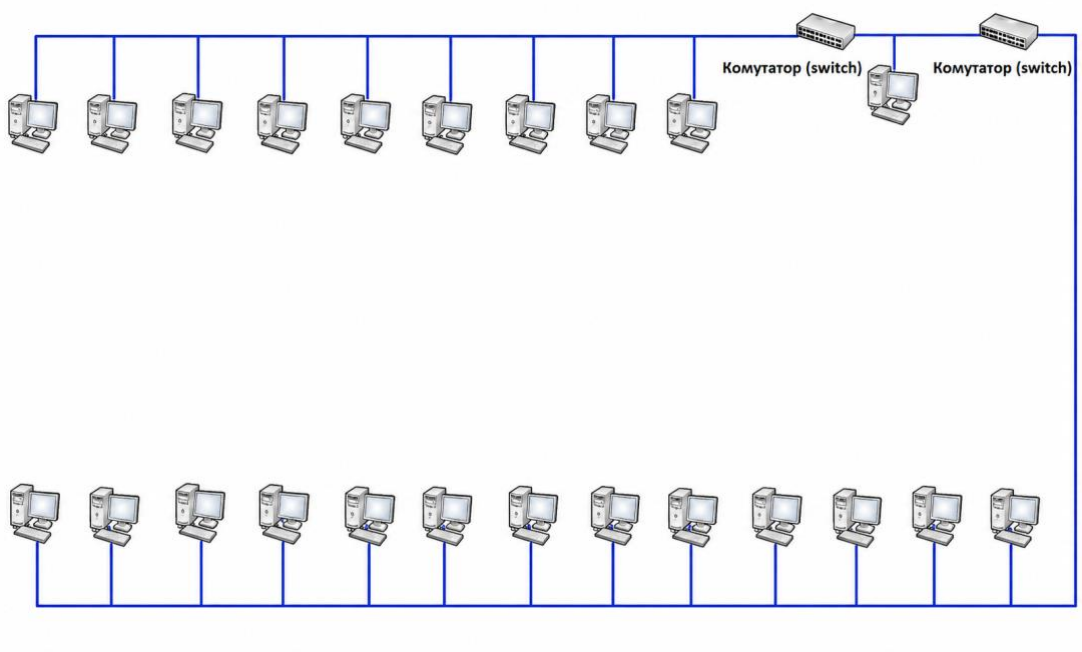


Рисунок 2.6 - Кабельна система організації

Структурована кабельна система (СКС) базуватиметься на компонентах компанії Siemons із використанням неекранованої витої пари (UTP) категорії 5, що відповідає міжнародним стандартам кабельних систем. Даний стандарт передбачає використання чотирьох мідних пар, дві з яких забезпечують передачу даних зі швидкістю 100 Мбіт/с, тоді як інші пари зарезервовані для додаткових функцій СКС.

Технологія монтажу СКС

Процес розгортання СКС є уніфікованим для всіх робочих місць. Розподіл ресурсів кабелю здійснюється наступним чином: дві пари використовуються для передачі та прийому даних, одна - для підключення цифрового телефонного апарата, і одна - для аналогового зв'язку (факс або модем). Монтажні роботи розпочинаються після затвердження проектної документації та передбачають прокладання кабельних трас між серверним приміщенням та робочими станціями користувачів [12].

Інтеграція з телефонією

Резервні пари кабелю залучаються для функціонування внутрішньої телефонної мережі. В агентстві експлуатується система цифрової телефонії на базі АТС Coral 1 (виробництва Tadiran, ECI Telecommunications, Ізраїль).

Передача мовного сигналу та цифрових даних здійснюється за двопровідною схемою, аналогічною до стандартів аналогової телефонії.

Топологія мережі

Архітектура СКС побудована за ієрархічним принципом «дерева», що логічно та топологічно відповідає структурі «зірка». Вузлом мережі виступає каскад комутаційного обладнання, розташований у серверній кімнаті. Як мережеві комутатори використовуються моделі D-Link DGS-1016D/F1, що забезпечують пропускну здатність 10/100/1000 Мбіт/с. Кожен комутатор має ємність 16 портів (див. рис. 2.7).



Рисунок 2.7 - Комутатор DGS-1016D

2.4.2 Організація робочого місця

Робоче місце користувача (кінцева точка СКС) обладнане двома розетками: стандарту RJ-45 (восьмиконтактний роз'єм для підключення комп'ютерного обладнання до мережі) та стандарту RJ-11 (шестиконтактний роз'єм для підключення телефонних апаратів). Блок розеток розміщений у підлоговому люку (floor box) - спеціалізованому монтажному відсіку, інтегрованому в конструкцію фальшпідлоги, призначеному для розміщення силових ліній та елементів СКС. Комутація термінального обладнання здійснюється за допомогою стандартних патч-кордів (RJ-45 та RJ-11 відповідно).

2.5 Розподіл IP-адрес

Розподіл IP-адрес локальної мережі приведено в таблиці 2.2

Таблиця 2.2 - Розподіл IP-адрес

Ім'я комп'ютера	IP-адреса	Маска мережі	№ комутатора
Директор	192.168.1.1	255.255.255.128	1
Відділ прямого підпорядкування	192.168.1.2	255.255.255.128	1
	192.168.1.3	255.255.255.128	1
6 відділення	192.168.1.4	255.255.255.128	1
	192.168.1.5	255.255.255.128	1
	192.168.1.6	255.255.255.128	1
5 відділення	192.168.1.7	255.255.255.128	1
	192.168.1.8	255.255.255.128	1
	192.168.1.9	255.255.255.128	1
	192.168.1.10	255.255.255.128	1
4 відділення	192.168.1.11	255.255.255.128	1
	192.168.1.12	255.255.255.128	1
	192.168.1.13	255.255.255.128	1
1 відділення	192.168.1.14	255.255.255.128	2
	192.168.1.15	255.255.255.128	2
	192.168.1.16	255.255.255.128	2
2 відділення	192.168.1.17	255.255.255.128	2
	192.168.1.18	255.255.255.128	2
	192.168.1.19	255.255.255.128	2
	192.168.1.20	255.255.255.128	2
3 відділення	192.168.1.21	255.255.255.128	2
	192.168.1.22	255.255.255.128	2
Секретар	192.168.1.23	255.255.255.128	2
Сервер	80.255.1.1	255.0.0.0	
Маршрутизатор	192.168.1.126	255.255.255.128	2
	80.255.1.2	255.0.0.0	
Рез. пул адрес	192.168.1.129 -192.168.1.255	255.255.255.128	(3)

Перевірка функціональності мережі була здійснена за допомогою програмного засобу мережевого моделювання NetEmul (додаток Г).

У другому розділі було вирішено комплекс завдань щодо проектування локальної обчислювальної мережі для ТОВ «НОЙНЕР».

На основі аналізу технічного завдання розроблено функціональну схему мережі, визначено її структурну організацію, зокрема обрано метод керування обміном даними, мережеву архітектуру та номенклатуру мережевих ресурсів. Виконано розрахунок необхідної кількості кабельної продукції та кабельних каналів відповідно до плану приміщень, а також здійснено розподіл IP-адрес для всіх елементів мережевої інфраструктури.

3 АДМІНІСТРУВАННЯ ЛОКАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

3.1 Організація мережі на базі Windows Server

3.1.1 MICROSOFT WINDOWS SERVER

Windows Server є високопродуктивною та надійною операційною системою корпоративного рівня [12]. Впровадження цієї платформи забезпечує доступ до передових технологічних рішень:

- диспетчер серверів (Server Manager): централізована консоль, що оптимізує процеси встановлення, налаштування та адміністрування серверних ролей. Можливість розгортання мінімалістичної конфігурації без графічного інтерфейсу дозволяє підвищити відмовостійкість системи та мінімізувати потребу в регулярному обслуговуванні;

- Windows PowerShell: потужний інструмент командного рядка, що включає понад 130 утиліт та вбудовану мову сценаріїв. Це забезпечує ефективну автоматизацію рутинних адміністративних завдань, зокрема при управлінні інфраструктурою з кількох серверів;

- Internet Information Services (IIS) та .NET Framework: інтегрована платформа для розробки та розгортання додатків, яка сприяє ефективному обміну даними, забезпечуючи їх наочну візуалізацію та якісну обробку;

- мережеві та кластерні технології: вдосконалені протоколи, що підвищують стабільність та масштабованість IT-інфраструктури.

У січні 2024 року компанія представила першу збірку Windows Server 2025 для адміністраторів, які беруть участь у програмі Windows Insider. Оновлена версія забезпечує підтримку технології hotpatching, впроваджує нове покоління Active Directory, а також розширює функціональні можливості SMB over QUIC, зокрема шляхом додавання опції використання альтернативних мережевих портів замість стандартного UDP/443 [13].

Windows Server 2025 демонструє суттєвий технологічний прогрес у сферах Hyper-V, інтеграції GPU, Storage Spaces Direct, програмно-визначених мереж (SDN) та кластеризації. Завдяки високій продуктивності та масштабованості, платформа є оптимальним рішенням для організацій, що впроваджують інструменти віртуалізації, а також систем, інтегрованих із технологіями штучного інтелекту та машинного навчання [13].

Остання версія Windows Server пропонує низку вдосконалень та нових функціональних можливостей. Нижче наведено ключові нововведення [13]:

- Hotpatching з підтримкою Azure Arc: користувачі хмарних середовищ отримують розширені можливості забезпечення безпеки, зокрема автоматизацію оновлень програмного забезпечення, а також інструменти резервного копіювання та відновлення;

- продуктивність сховищ NVMe: Windows Server 2025 забезпечує зростання продуктивності операцій введення-виведення (IOPS) до 60% порівняно з Windows Server 2022;

- підтримка блокового клонування: впровадження формату файлової системи ReFS у Dev Drive дозволяє суттєво підвищити швидкість операцій копіювання файлів;

- функціонал Active Directory (AD): оновлення включають розширені можливості відновлення об’єктів AD, опціональний розмір сторінки бази даних 32К, а також підвищений рівень захисту конфіденційних атрибутів та паролів облікових записів;

- Credential Guard: технологія активована за замовчуванням на сумісних пристроях для ефективного захисту від несанкціонованого викрадення облікових даних (NTLM-хешів, квитків Kerberos TGT та даних, що зберігаються застосунками);

- безпека файлових служб (SMB): впроваджено підтримку SMB over QUIC для захищеного доступу до файлів через мережу Інтернет, а також посилені механізми захисту від атак «груба сила», атак «людина посередині» (MitM), ретрансляції та підробки даних;

- Delegate Managed Service Accounts (dMSA): використання dMSA усуває потребу в ручному керуванні паролями, оскільки ці функції автоматизовано на рівні AD;

- прискорена мережа (AccelNet): оптимізація управління SR-IOV для віртуальних машин дозволяє знизити затримки, джиттер та навантаження на центральний процесор;

- DTrace: інтегрований інструмент для моніторингу та діагностики продуктивності системи в режимі реального часу.

- віртуалізаційна безпека (VBS) в анклавах: механізм забезпечує захист конфіденційних даних застосунків, мінімізуючи потребу в довірі до прав адміністратора та посилюючи стійкість до зовнішніх загроз;

- рішення для пароля локального адміністратора (LAPS): система автоматично генерує унікальні паролі для локальних адміністраторів на кожному вузлі, забезпечуючи їх безпечне зберігання в AD та періодичну ротацію.

Оперативне розгортання клієнтських операційних систем засобами WDS

Служба розгортання Windows (Windows Deployment Services, WDS), впроваджена у Windows Server, забезпечує ефективне розгортання клієнтських операційних систем у мережевому середовищі. Завдяки використанню протоколу TFTP процес інсталяції став значно швидшим. WDS підтримує методи розгортання ScheduleCast та AutoCast [14]:

- ScheduleCast дозволяє здійснювати розгортання за заздалегідь визначеним розкладом;

- AutoCast забезпечує постійну готовність образу до розгортання через багатоадресну розсилку (Multicast). Використання Multicast дозволяє оптимізувати пропускну здатність мережі під час одночасного обслуговування кількох клієнтів.

Забезпечення мережевої безпеки за допомогою Network Access Protection (NAP)

Технологія захисту доступу до мережі (Network Access Protection, NAP) від Microsoft є механізмом забезпечення відповідності вимогам політики безпеки. Вона вимагає від клієнтських пристроїв дотримання встановлених стандартів безпеки перед наданням доступу до серверних ресурсів [13].

У разі невідповідності заданим параметрам клієнтські пристрої можуть бути ізольовані в карантинній мережі або позбавлені доступу до ресурсів. Крім того, Windows Server забезпечує можливість автоматичного розгортання необхідних оновлень для приведення стану пристрою до вимог політики. NAP гарантує безпеку як локальних робочих станцій, так і віддалених пристроїв, що підключаються через LAN або VPN-канали.

Удосконалення функціональності термінальних служб (Terminal Services)

У Windows Server термінальні служби отримали низку значних покращень, серед яких [12]:

- RemoteApp: аналог опублікованих додатків у Citrix, що дозволяє запускати окремі застосунки в ізольованому вікні, а не транслювати весь робочий стіл. Це забезпечує безшовну інтеграцію з робочим середовищем користувача, де застосунок доступний безпосередньо через меню «Пуск» або робочий стіл;

- Terminal Services Gateway: забезпечує безпечне підключення віддалених користувачів до термінальних служб без необхідності використання традиційних VPN-тунелів;

- Terminal Services Web Access (рис. 3.1): надає доступ до термінальних служб через стандартний веб-браузер, що виключає потребу в наявності встановленого клієнтського програмного забезпечення або налаштованого VPN-з'єднання на віддаленому пристрої.

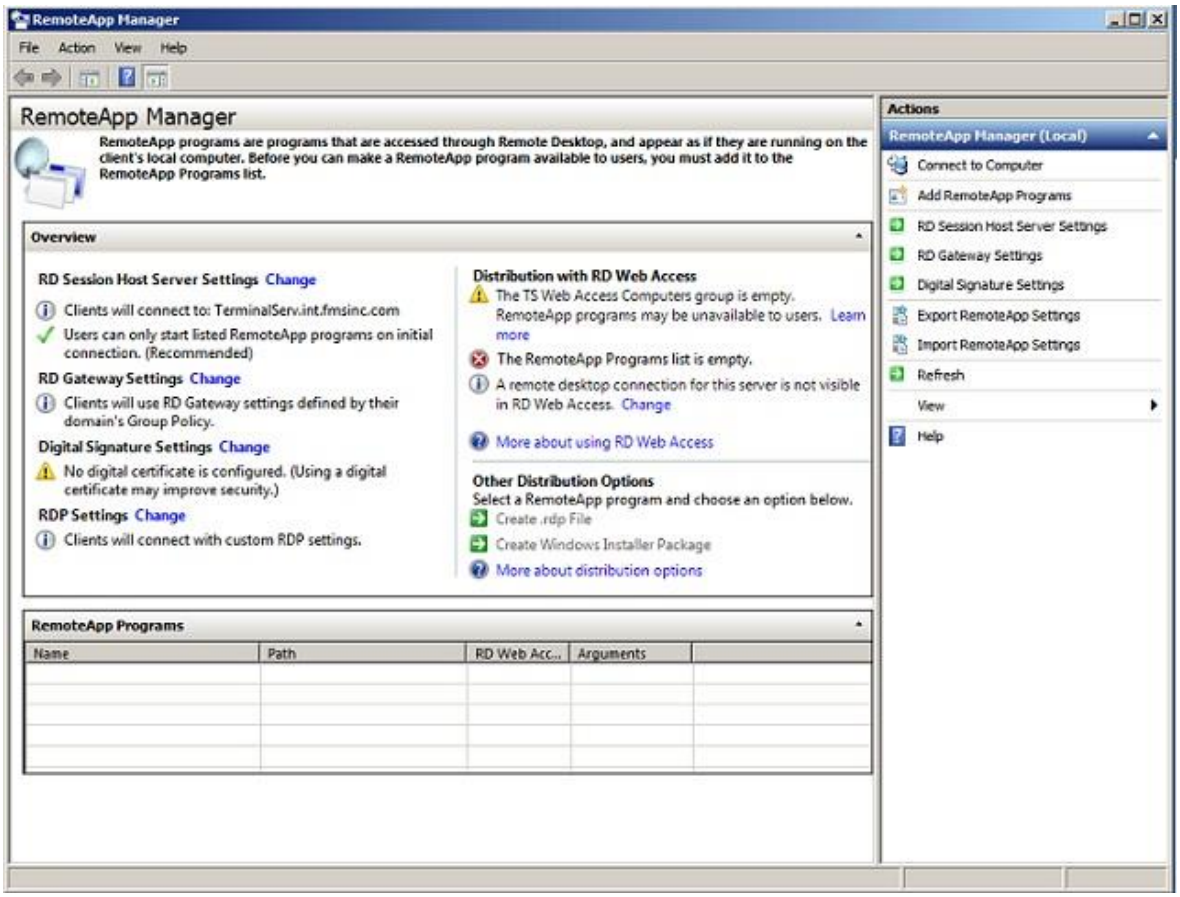


Рисунок 3.1 - Інтерфейс сервера мережевої політики

Розширені можливості віртуалізації у Windows Server

Технологія віртуалізації Windows Server є ключовим інструментом, що забезпечує запуск декількох ізольованих операційних систем на базі одного фізичного сервера. Це рішення дозволяє консолідувати інфраструктурні ресурси та оптимізувати витрати, а також створювати гнучкі середовища для розробки та тестування без значних капіталовкладень у апаратне забезпечення.

Інтеграція засобів віртуалізації безпосередньо в операційну систему Windows є стратегічним кроком Microsoft, спрямованим на зміцнення позицій компанії на ринку та створення конкурентної альтернативи рішенням VMware. Попри значну історію розвитку продуктів конкурента, впровадження вбудованих інструментів віртуалізації від Microsoft значно спрощує доступ кінцевих користувачів до сучасних технологій управління серверною інфраструктурою.

3.1.2 Служби Windows Server

DHCP (Dynamic Host Configuration Protocol) - це еволюція протоколу BOOTP (RFC 951 та 1084), призначена для автоматизованого розподілу IP-адрес та надання параметрів конфігурації стека TCP/IP, необхідних для коректної роботи мережевих клієнтів [10].

Область (Scope) DHCP: адміністративно визначений діапазон IP-адрес у межах певної фізичної підмережі. Області формують логічну структуру мережі та дозволяють серверу централізовано керувати параметрами конфігурації для клієнтів. Налаштування області є обов’язковим етапом для активації динамічного призначення адрес.

Пул адрес (Address Pool): сукупність IP-адрес у межах визначеної області, що залишаються доступними для динамічного призначення після виключення зарезервованих або статичних діапазонів.

Діапазони виключення (Exclusion Ranges): перелік IP-адрес усередині області, які вилучаються з процесу автоматичного розподілу, щоб запобігти їх видачі клієнтам.

Резервування (Reservation): механізм, що забезпечує закріплення конкретної IP-адреси за певним мережевим пристроєм, гарантуючи її незмінність у підмережі.

Суперобласті (Superscopes): адміністративний об’єкт у консолі керування

DHCP, який групує декілька областей для вирішення специфічних мережевих завдань та спрощення адміністрування.

Орендні договори (Leases): часовий інтервал, протягом якого клієнтський пристрій має право використовувати призначену IP-адресу. Згідно з протоколом, після спливу половини терміну оренди клієнт ініціює запит до сервера на її поновлення. Тривалість оренди безпосередньо впливає на інтенсивність мережевого трафіку, пов'язаного з оновленням параметрів конфігурації.

Опції DHCP - це додаткові параметри конфігурації, які DHCP-сервер призначає клієнтам під час надання оренди IP-адреси. Наприклад, параметри шлюзу за замовчуванням, серверів DNS або WINS можуть бути налаштовані як для окремих областей (scopes), так і глобально для всієї інфраструктури, керованої сервером. Крім того, DHCP-сервер Microsoft дозволяє створювати користувацькі опції відповідно до специфічних вимог мережі [10].

Використання протоколу DHCP суттєво оптимізує роботу системного адміністратора, централізуючи процес керування IP-адресацією. При підключенні до мережі клієнтський пристрій надсилає запит, після чого сервер автоматично призначає доступну IP-адресу з відповідного пулу. Процес ідентифікації та призначення IP-адреси складається з чотирьох етапів (механізм DORA):

1) DHCP Discover: клієнт надсилає широкомовний запит для пошуку сервера;

2) DHCP Offer: сервер надсилає пропозицію конфігурації;

3) DHCP Request: клієнт акцептує пропозицію;

4) DHCP Acknowledgement: сервер офіційно підтверджує надання параметрів.

Для забезпечення ефективного використання адресного простору сервер призначає IP-адресу на визначений термін (оренду). Після завершення половини терміну оренди клієнт ініціює запит на її поновлення. Якщо пристрій припиняє роботу в мережі або змінює сегмент, термін оренди завершується, і адреса повертається в пул для подальшого повторного використання [10].

Служба DHCP у Windows Server складається з трьох ключових компонентів [10]:

- DHCP-сервери: включають графічний інтерфейс адміністрування

(DHCP Snap-in) та базу даних для призначення адрес. Сервер підтримує понад 30 опцій згідно зі стандартом RFC 2132, що дозволяє автоматизувати налаштування параметрів TCP/IP, включаючи маску підмережі, шлюзи за замовчуванням та адреси серверів DNS/WINS. Після встановлення ролі сервера та активації областей (scopes) база даних DHCP формується автоматично;

- DHCP-клієнти: сервером можуть обслуговуватися пристрої на різних платформах. Зокрема, підтримку DHCP забезпечують усі версії клієнтських та серверних ОС Microsoft, починаючи від Windows NT та закінчуючи сучасними рішеннями, за умови використання відповідних TCP/IP-стеків;

- агенти ретрансляції (DHCP Relay Agents): оскільки протоколи DHCP та BOOTP базуються на широкомовних запитах, які за замовчуванням не проходять через маршрутизатори, для взаємодії між підмережами використовуються агенти ретрансляції. Агент перехоплює широкомовні повідомлення та переадресовує їх на цільові DHCP-сервери, що дозволяє уникнути потреби у розміщенні сервера в кожному фізичному сегменті мережі.

Слід зазначити, що ручне налаштування параметрів мережі на клієнтському пристрої має пріоритет над динамічними параметрами, отриманими від DHCP-сервера.

Ключові особливості DHCP:

- інтеграція з DNS: забезпечує коректне розпізнавання імен для мережевих ресурсів. Реалізовано можливість реєстрації як DHCP-серверів, так і клієнтів безпосередньо в DNS;

- моніторинг та управління: впроваджено систему сповіщень про стан заповнення пулу IP-адрес, що дозволяє адміністраторам оперативно реагувати на вичерпання ресурсів;

- підтримка багатоадресної розсилки (Multicast): реалізовано можливість призначення багатоадресних адрес, що є критично важливим для роботи конференц-зв’язку та систем потокового мовлення;

- захист від неавторизованих серверів: нові механізми виявлення конфліктів у мережевих сегментах дозволяють автоматично деактивувати нелегітимні DHCP-сервери для забезпечення стабільної роботи мережі;

- авторизація в Active Directory: підвищено рівень безпеки: сервер DHCP функціонує лише після успішної авторизації в каталозі Active Directory, що запобігає «підміні» серверів;

- кластеризація: підтримка DHCP-сервера як кластерного ресурсу в редакціях Windows Server забезпечує високу доступність сервісу.

- автоматичне налаштування клієнтів (APIPA): у разі недоступності DHCP-сервера клієнти автоматично переходять на тимчасову конфігурацію, продовжуючи фоновий пошук сервера кожні 5 хвилин.

- спеціалізовані опції та класи: підтримка користувацьких класів дозволяє адаптувати DHCP для специфічних корпоративних додатків та обладнання різних виробників.

Адміністрування DNS-сервера

Налаштування та коригування параметрів DNS-сервера необхідні у таких випадках:

1. Зміна імені або IP-адреси сервера.
2. Зміна доменного імені сервера.
3. Виведення DNS-сервера з експлуатації.
4. Зміна основного (primary) сервера зони.

Управління клієнтськими підключеннями

Конфігурація DNS для клієнтів Windows передбачає налаштування:

1. Імені хоста для мережевого підключення.
2. Імені батьківського домену для формування повного доменного імені (FQDN).
3. Основного та альтернативних DNS-серверів.
4. Пріоритетності списку пошуку доменів для неповних імен.

Адміністрування зон

Після створення зони доступне керування такими параметрами:

- статус активності зони;
- зміна або конвертація типу зони;
- політики динамічного оновлення;
- налаштування записів SOA, ресурсних записів, делегування, сповіщень та інтеграція з WINS;
- управління зонами зворотного перегляду (reverse lookup) для відповідності IP-адрес іменам хостів.

3.2 Основні адміністративні блоки

Об'єднання комп'ютерів у домени надає системним адміністраторам та користувачам дві ключові переваги. По-перше, сервери домену формують єдину адміністративну одиницю з централізованою службою безпеки та спільною базою даних облікових записів. Кожен домен має власну базу даних, що містить відомості про користувачів, групи та параметри політик безпеки. Функціонування серверів як первинних або резервних контролерів домену забезпечує реплікацію цієї бази даних. Такий підхід значно спрощує адміністрування: для кожного користувача створюється лише один обліковий запис, що позбавляє необхідності запам'ятовувати кілька паролів. Розширення адміністративних можливостей до рівня домену в Windows Server 2025 дозволяє оптимізувати робочий час як IT-фахівців, так і кінцевих користувачів.

Другою перевагою є покращення зручності роботи в мережі: при пошуку ресурсів користувачі бачать структуровану ієрархію доменів замість розрізнених серверів і периферійних пристроїв, що значно спрощує навігацію.

3.2.1 Налаштування сервера

Мережева операційна система функціонує на базі мережевого сервера, тоді як клієнтські робочі станції можуть працювати під управлінням різнорідних операційних систем. Для забезпечення інтеграції клієнтського обладнання в мережеве середовище необхідно інсталювати відповідні драйвери мережевих адаптерів. Механізм роботи цих драйверів аналогічний до роботи драйверів периферійних пристроїв, зокрема принтерів: програмне забезпечення мережевого адаптера забезпечує взаємодію прикладних програм із мережевим середовищем для передачі та прийому даних. Кожен вузол мережі оснащується одним або кількома мережевими інтерфейсними адаптерами для фізичного підключення до мережі.

Продуктивність локальної мережі прямо залежить від технічних характеристик сервера. При розгортанні Windows 2008 Server пріоритет слід надавати високопродуктивним апаратним рішенням. Вибір між готовими серверними платформами від виробників та індивідуальною збіркою залежить від технічних завдань та досвіду фахівців. Зважаючи на широку номенклатуру компонентів, при конфігурації сервера рекомендується враховувати такі вимоги

[14]:

1. Шинна архітектура: Використання шини PCI є стандартом завдяки 64-бітній розрядності, високій пропускній здатності та підтримці програмного налаштування (Plug and Play), що мінімізує конфлікти апаратних ресурсів.

2. Оперативна пам’ять: ОС Windows 2008 Server має високі вимоги до обсягу ОЗП. Для мережевого сервера рекомендований мінімальний обсяг пам’яті становить 2 ГБ.

3. Дискова підсистема: Оптимальним вибором є використання жорстких дисків та адаптерів інтерфейсу SCSI. Для високонавантажених серверів доцільно використовувати технологію Ultra Wide SCSI (швидкість передачі даних до 40 Мбіт/с), яка забезпечує стабільну роботу в мережах з інтенсивним трафіком.

4. Корпус та охолодження: Для запобігання перегріву компонентів рекомендується використовувати корпуси форм-фактору Big Tower або спеціалізовані серверні корпуси. Останні забезпечують ефективну вентиляцію, підтримку потужних блоків живлення та можливість подальшого масштабування системи.

5. Додаткове охолодження: При встановленні кількох жорстких дисків необхідно передбачити інсталяцію додаткових систем активного охолодження всередині системного блоку.

6. Мережева карта: Враховуючи постійне навантаження на сервер, він повинен бути оснащений потужним 32-бітним мережевим адаптером із підтримкою співпроцесора для розвантаження центрального процесора від завдань обробки мережевого трафіку.

3.2.2 Встановлення WINDOWS SERVER

Після підготовки комп'ютера можна розпочинати інсталяцію Windows. Якщо на жорсткому диску сервера відсутні розділи, завантаження здійснюється із системних дискет, що ініціює запуск програми встановлення для створення розділів та початку інсталяції. Для цього в налаштуваннях BIOS параметр «Boot Sequence» необхідно встановити у значення «A, C». Альтернативним способом є інсталяція за допомогою CD-ROM: комп'ютер автоматично завантажується з носія та запускає програму встановлення. У разі, якщо на сервері вже встановлена ОС, інсталяцію можна розпочати безпосередньо з компакт-диска.

Для цього слід відкрити папку «I386» та запустити інсталяційний файл «WINNT». Процес встановлення Windows Server 2025 складається з двох етапів: текстового режиму та графічного інтерфейсу.

3.2.3 Управління в середовищі WINDOWS SERVER

Після завершення інсталяції Windows Server 2025 розпочинається етап налаштування облікових записів користувачів.

Фундаментальним компонентом централізованого адміністрування в середовищі Windows Server 2025 є домен. Домен являє собою групу серверів під управлінням Windows Server, які функціонують як інтегрована система. В межах домену всі сервери використовують уніфіковану базу облікових записів, що дозволяє створювати запис користувача одноразово для його подальшої ідентифікації на всіх серверах доменної структури.

Довірчі відносини між доменами забезпечують наскрізну автентифікацію, завдяки чому користувач із єдиним обліковим записом отримує доступ до мережевих ресурсів у межах усієї інфраструктури. Ефективне планування доменів та довірчих зв’язків гарантує коректне розпізнавання облікових записів усіма комп’ютерами мережі, забезпечуючи можливість одноразової автентифікації для отримання доступу до будь-якого сервера.

Структурування комп’ютерів у домени надає суттєві переваги як для системних адміністраторів, так і для користувачів. Ключовою перевагою є формування єдиного адміністративного простору, що спільно використовує службу безпеки та базу облікових даних. Кожен домен підтримує централізований репозиторій, що містить відомості про користувачів, групи та параметри політик безпеки. Сервери домену функціонують як контролери, що містять копії цієї бази даних. Це дозволяє оптимізувати адміністрування облікових записів та спрощує процес автентифікації користувачів, скорочуючи часові витрати на управління мережевою інфраструктурою.

Додатковою перевагою є покращення юзабіліті мережевого середовища: при перегляді доступних ресурсів користувачі сприймають мережу як логічно впорядковану структуру доменів, що значно спрощує навігацію порівняно з пошуком окремих серверів або периферійних пристроїв.

3.3 Захист інформації в мережі

Дослідження та аналіз інцидентів, пов’язаних із несанкціонованим доступом та порушенням цілісності інформації, засвідчують доцільність їх класифікації на випадкові та навмисні [12].

Проєктування систем захисту інформації потребує детальної ідентифікації природи загроз, способів їх виникнення та механізмів реалізації в межах автоматизованої системи. З метою розв’язання цього завдання здійснюється систематизація загроз та шляхів впливу шляхом їх зведення до базових видів і форм, які репрезентативно відображають весь спектр потенційних ризиків в автоматизованій системі (рис. 3.2).

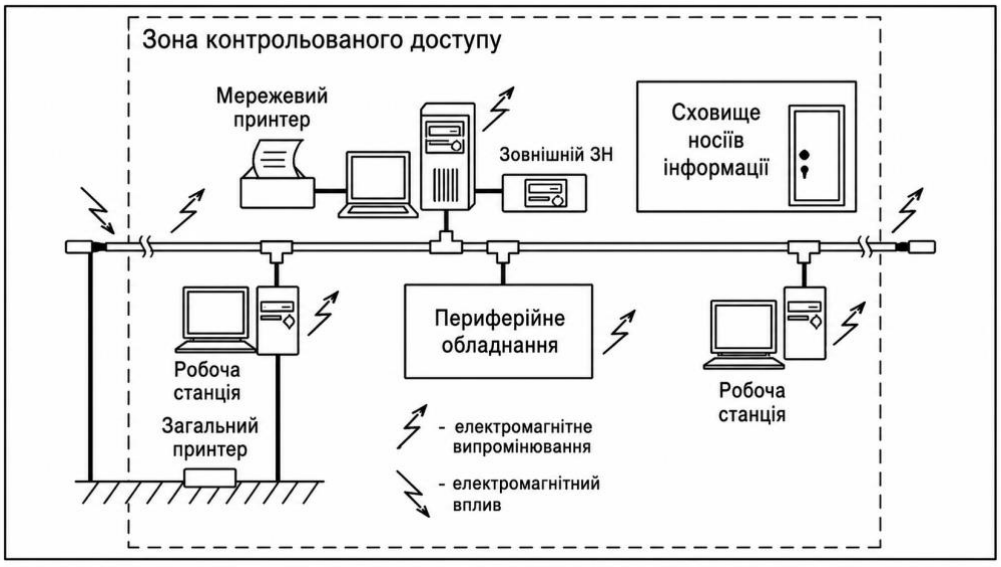


Рисунок 3.2 - Можливі канали несанкціонованого доступу

Аналіз досвіду проектування, впровадження та експлуатації автоматизованих систем засвідчує, що під час введення, зберігання, обробки та передачі інформація зазнає впливу різноманітних дестабілізуючих факторів.

До основних причин виникнення таких впливів належать:

- відмови та технічні збої обладнання;
- перешкоди в каналах зв’язку, зумовлені впливом зовнішнього середовища;
- помилки персоналу під час експлуатації системи;
- системні та інженерно-технічні прорахунки розробників;
- структурні, алгоритмічні та програмні недоліки;

- виникнення аварійних ситуацій;
- інші зовнішні та внутрішні чинники.

Умисні загрози зумовлені цілеспрямованими діями зловмисників, мотивованими соціальним невдоволенням, прагненням до матеріальної вигоди або реалізацією деструктивних амбіцій (зокрема, хакерством).

Враховуючи високу ймовірність несанкціонованих спроб доступу до мережі агентства, необхідно забезпечити комплексне впровадження превентивних заходів захисту.

Для обчислювальних систем визначено такі штатні канали доступу до інформаційних ресурсів:

- термінали користувачів, зокрема робочі станції в комп’ютерних класах;
- термінал системного адміністратора;
- термінал оператора функціонального контролю;
- засоби візуалізації інформації;
- засоби інсталяції програмного забезпечення;
- засоби документування (виведення) інформації;
- носії даних;
- зовнішні комунікаційні канали.

З метою забезпечення цілісності та конфіденційності інформації застосовуються п'ять основних рівнів захисту:

- технічні засоби;
- програмні засоби;
- криптографічні методи;
- організаційні заходи;
- законодавчо-нормативне забезпечення.

3.4 Аналіз можливостей системи розмежування доступу WINDOWS SERVER

Windows Server оснащений інтегрованими засобами забезпечення безпеки, ключові з яких розглянуті нижче.

Моніторинг мережевої активності

Windows Server пропонує широкий спектр інструментів для контролю

мережевої активності та ефективності використання ресурсів. Операційна система дозволяє здійснювати всебічний моніторинг сервера, включаючи аналіз споживання ресурсів, перегляд списку активних підключень користувачів та відкритих ними файлів. Також доступні функції аудиту журналів безпеки та системних подій, що дозволяють налаштовувати систему сповіщень адміністратора про виникнення критичних помилок.

Автентифікація на робочій станції

Під час ініціації сеансу на робочій станції під керуванням Windows 11 користувач має надати ім’я користувача, пароль та домен. Робоча станція надсилає ці облікові дані домену для ідентифікації. Сервер автентифікації перевіряє отримані дані в базі облікових записів домену. У разі успішного підтвердження відповідності даних, сервер надає дозвіл на вхід до системи та завантажує профіль користувача, включаючи персональні налаштування, домашній каталог та змінні середовища.

За замовчуванням право на вхід до системи мають лише облікові записи, що належать до груп адміністраторів, операторів сервера, операторів управління друком, операторів облікових записів та операторів резервного копіювання. Усім іншим користувачам мережі організації надаються індивідуальні імена користувачів та паролі.

Облікові записи користувачів

Для доступу до ресурсів мережі кожен користувач повинен мати обліковий запис у домені. Обліковий запис містить вичерпну інформацію про користувача, включаючи його ідентифікаційні дані та встановлені обмеження доступу до мережевих ресурсів. Для оптимізації адміністрування користувачів з аналогічними правами доступу доцільно об’єднувати у групи. Це дозволяє здійснювати централізоване керування правами та дозволами, застосовуючи налаштування до всієї групи одночасно.

Журнал подій безпеки

Windows Server надає інструментарій для налаштування параметрів аудиту, що забезпечує фіксацію визначених системних подій або спроб доступу до файлових ресурсів у журналі безпеки. Запис у журналі аудиту містить

відомості про тип виконаної дії, ідентифікатор користувача, а також дату та час події. Цей механізм дозволяє здійснювати моніторинг як успішних, так і невдалих спроб виконання операцій.

Ведення журналу безпеки є обов’язковим компонентом для корпоративних мережевих середовищ, оскільки це забезпечує можливість ідентифікації джерела в разі виявлення спроб несанкціонованого доступу.

Права користувачів

Права користувачів регламентують перелік дозволених системних операцій для суб’єкта доступу. До дій, що підлягають регулюванню, належать: вхід у систему на локальному комп’ютері, завершення роботи, зміна налаштувань часу, резервне копіювання та відновлення файлів сервера, а також виконання інших адміністративних завдань.

У межах домену Windows Server права користувачів призначаються та обмежуються на рівні домену. Якщо група є частиною домену, її учасники автоматично отримують визначені права на всіх первинних та резервних контролерах домену.

Проєктування структури локальної мережі виконано з урахуванням використання середовища Windows Server 2025. Окрему увагу приділено питанням забезпечення інформаційної безпеки локальної обчислювальної мережі ТОВ «НОЙНЕР».

ВИСНОВКИ

Процес проектування локальної обчислювальної мережі (ЛОМ) ТОВ «НОЙНЕР» передбачав комплексний аналіз теоретичних засад побудови мережевих інфраструктур, зокрема технологічних стандартів, апаратного забезпечення, топологій, методів комутації та протоколів маршрутизації.

У межах виконання проекту було обрано технологічний стандарт Ethernet (Fast Ethernet 100 Мбіт/с), розроблено функціональну та структурну схеми мережі, визначено архітектурні рішення, методи управління обміном даними та принципи розподілу мережевих ресурсів. Згідно з планом приміщень здійснено розрахунок необхідних кабельних систем та каналів зв’язку, а також проведено сегментацію IP-адрес для всіх мережевих вузлів.

Проектування інфраструктури базувалося на використанні серверної операційної системи Windows Server 2025 із впровадженням комплексних заходів щодо забезпечення інформаційної безпеки корпоративної мережі ТОВ «НОЙНЕР».

Впровадження спроектованої локальної мережі спрямоване на оптимізацію технічних показників, підвищення продуктивності праці персоналу ТОВ «НОЙНЕР» та створення технологічного фундаменту для подальшого масштабування бізнес-процесів підприємства.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Олещенко Л.М. Організація комп'ютерних мереж: конспект лекцій: навч. посіб. для студ. спеціальності 121 "Інженерія програмного забезпечення", спеціалізації "Програмне забезпечення комп'ютерних та інформаційно-пошукових систем" / КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 225 с.

2. Задерейко О.В. Комп’ютерні мережі [Електронний ресурс]: навчальний посібник / О.В. Задерейко, Н.І. Логінова, А.А. Толокнов. – Одеса, 2022. – 249 с.

3. Тарнавський Ю.А., Кузьменко І. М. Організація комп'ютерних мереж: підручник: для студ. спеціальності 121 "Інженерія програмного забезпечення" та 122 "Комп'ютерні науки" / КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2018. – 259 с.

4. Попов І.І., Максимов Н.В. Комп'ютерні мережі: навчальний посібник. - М.: ФОРУМ: ІНФРА - М, 2015. – 365 с.

5. Телекомунікаційні системи передавання інформації [Текст] / Климаш М.М. , Колодій Р.С. – Л.: 2018. – 632 с.

6. Загальні принципи організації мереж [Электронный ресурс] - Режим доступу: https://elib.lntu.edu.ua/sites/default/files/elib_upload/123%20%D0%BF%D0%BE%D1%81%D1%96%D0%B1%D0%BD%D0%B8%D0%BA%20%D0%BA%D0%BE%D0%BC%D0%BF'%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%20%D1%96%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D1%96%D1%8F/page36.html. (дата звернення 20.06.2026)

7. Оліфер, В.Г., Оліфер, Н.О. Комп'ютерні мережі. Принципи, технології, протоколи: Підручник для вузів. Видання четверте. [Текст] Видавництво: Пітер: 2020. - 1000 с.

8. Стен Шатт "Світ комп'ютерних мереж ", Київ, "BHV", 2009.

9. Комп’ютерні мережі : Навчальний посібник / В. Г. Хоменко, М. П. Павленко. – Донецьк : ЛАНДОН-ХХІ, 2011. – 316 с.

10. Технічна експлуатація засобів та систем зв’язку: навч. посіб. / Л. М. Сакович та ін.; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ, 2021. – 176 с.

11. Офіційний веб-сайт Cisco Systems. [Електронний ресурс]. URL: http://www.cisco.com/web/RU/index.html. (дата звернення 20.06.2026)

12. Основи організації мереж Cisco, том 1 [Текст]: Пер. з англ. – К.: Видавничий дім «Вільямс», 2002. – 512 с.

13. Пояснення VPN-протоколів: типи, відмінності та як вибрати [Електронний документ] - Режим доступу: https://freevpnplanet.com/ua/blog/vpn-protocols-what-are-they-and-where-they-are-used/ (дата звернення 20.06.2026)

14. Cisco Systems: документация [Електронний ресурс]. Режим доступа: http://www.cisco.com/en/US/docs. (дата звернення 27.06.2026)