

Ім'я користувача:  
приховано налаштуваннями конфіденційності

ID перевірки:  
1016377945

Дата перевірки:  
20.06.2024 12:55:20 EEST

Тип перевірки:  
Doc vs Library + My Database

Дата звіту:  
20.06.2024 12:56:29 EEST

ID користувача:  
100011372

Назва документа: Пришляк Дмитро ТК-42 плагіат\_

Кількість сторінок: 46 Кількість слів: 8157 Кількість символів: 63907 Розмір файлу: 464.50 KB ID файлу: 1016186472

## 42.8% Схожість

Найбільша схожість: 10.6% з джерелом з Бібліотеки (ID файлу: 6004273)

Пошук збігів з Інтернетом не проводився

42.8% Джерела з Бібліотеки

151

Сторінка 48

## 0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

## 0% Вилучень

Немає вилучених джерел

## Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи

2

## 1 ЗАГАЛЬНА ХАРАКТЕРИСТИКА ЛОКАЛЬНОЇ МЕРЕЖІ ТА ВИМОГИ ДО НЕЇ.

### 1.1 Особливості побудови сучасних локальних комп'ютерних мереж.

Сучасні локальні комп'ютерні мережі (ЛКМ) є критично важливими для забезпечення ефективної комунікації та обміну даними в межах організації. Вони об'єднують комп'ютери та інші пристрої для спільного використання ресурсів, таких як файли, принтери та інтернет-з'єднання. Побудова таких мереж вимагає врахування кількох ключових аспектів, що визначають їх продуктивність, надійність і безпеку.

Однією з головних особливостей сучасних ЛКМ є використання структурованих кабельних систем (СКС). СКС забезпечує гнучкість і масштабованість мережевої інфраструктури, дозволяючи легко додавати нові пристрої або змінювати конфігурацію мережі. Основою СКС є стандарти, такі як ANSI/TIA-568 та ISO/IEC 11801, що визначають технічні вимоги до кабелів, роз'ємів і монтажних практик. Важливим аспектом побудови ЛКМ є вибір топології. Найпоширенішими топологіями є «зірка» та її розширення «дерево». Топологія «зірка» передбачає підключення всіх пристроїв до центрального комутатора або маршрутизатора, що забезпечує високу надійність і легкість управління мережею. Топологія «дерево» дозволяє будувати більш складні структури, підключаючи кілька рівнів комутаторів.

Сучасні ЛКМ активно використовують технології віртуалізації, такі як віртуальні локальні мережі (VLAN) та програмно-визначені мережі (SDN). VLAN дозволяють логічно розділити фізичну мережу на кілька ізольованих сегментів, підвищуючи безпеку та керованість мережі. SDN надає можливість централізованого управління та динамічного налаштування мережевої інфраструктури. Безпека є критичним компонентом ЛКМ. Для захисту мережі

використовуються міжмережеві екрани (фаєрволи), системи виявлення та запобігання вторгнень (IDS/IPS), а також шифрування даних і автентифікація користувачів. Регулярні аудити безпеки та впровадження політик інформаційної безпеки допомагають знизити ризики несанкціонованого доступу та втрати даних. Масштабованість є ще однією важливою характеристикою сучасних ЛКМ. Вони повинні легко адаптуватися до зростання кількості користувачів і збільшення обсягу передаваних даних. Використання модульних мережевих пристроїв дозволяє додавати нові компоненти без значних витрат та збоїв у роботі мережі. Крім того, сучасні стандарти, такі як Gigabit Ethernet та 10 Gigabit Ethernet, забезпечують високу пропускну здатність, необхідну для обробки великих обсягів даних.

Автоматизація управління мережею також є ключовим елементом. Сучасні системи управління мережею (NMS) дозволяють автоматизувати моніторинг стану мережі, виявлення та усунення несправностей, управління конфігурацією мережевих пристроїв, що підвищує надійність і ефективність роботи мережі.

Таким чином, побудова сучасних локальних комп'ютерних мереж вимагає комплексного підходу, який включає використання структурованих кабельних систем, вибір оптимальної топології, впровадження технологій віртуалізації, забезпечення безпеки та масштабованості, а також автоматизацію управління мережею. Такий підхід дозволяє створити надійну, ефективну та безпечну мережеву інфраструктуру, що відповідає сучасним вимогам бізнесу.

## 1.2 Технології побудови локальних комп'ютерних мереж

Технології побудови локальних комп'ютерних мереж (LAN) є фундаментом сучасної інфраструктури підприємств, забезпечуючи надійний і

швидкий обмін даними між різними пристроями. Основними складовими технологій побудови LAN є топології мережі, методи передачі даних, мережеві протоколи та обладнання.

Локальна мережа передавання даних (LAN)- це мережа з'єднаних між собою з допомогою спеціальних апаратно-програмних засобів комп'ютерів, розташованих на невеликій території. Метою створення LAN є доступ до розміщених на інших комп'ютерах мережі розподілених ресурсів: інформаційних, програмних та технічних.

До основних компонентів локальних мереж відносяться:

- комп'ютери;
- програмне забезпечення мережі (мережеві операційні системи і мережеві додатки);
- комунікаційне обладнання;
- структуровані кабельні системи.

В локальних мережах можуть використовуватися комп'ютери двох типів:

- Рядовий комп'ютер (клієнт) – це робоча станція, яка через мережу отримує доступ до розподілених ресурсів і призначена для розв'язування прикладних задач користувача.
- Центральний комп'ютер (сервер) – це потужний, як правило, комп'ютер, який містить розподілені ресурси, доступні для інших комп'ютерів (клієнтів).

В залежності від того, який тип комп'ютерів містить мережа, розрізняють два типи локальних мереж:

- Однорангові мережі (мережа типу “клієнт-клієнт”);
- Мережі з центральним комп'ютером (мережа типу “клієнт - сервер”).

На рис. 1.1 наведений приклад локальної мережі з центральним комп'ютером. При цьому центральний комп'ютер ЦК (сервер), рядові

комп'ютери ПК (клієнти) і друкуючий принтер ДП під'єднані до кабельної системи (фізичного середовища) з допомогою мережєвих адаптерів МА. У загальному випадку клієнтом називають комп'ютер, який формує повідомлення-запит на доступ до розподілених ресурсів, а сервером – комп'ютер, який виконує запит (виділяє необхідний ресурс).



Рисунок 1.1 – Фрагмент локальної мережі з центральним комп'ютером

Мережєві операційні системи складають програмну платформу комп'ютерних мереж і в значній мірі визначають ефективність їх роботи цілому. До системних програмних компонентів мережі відносяться:

- протокольні модулі, які визначають і регулюють спосіб взаємодії між вузлами і модулями мережі;
- комунікаційні програми, які забезпечують передачу даних між компонентами мережі;
- програми апаратного рівня, які керують роботою технічних засобів мережі.

Програмні мережєві додатки зорієнтовані на задачі користувачів і забезпечують реалізацію мережєвих служб. Мережєвий додаток реалізується двома розподіленими програмами: програмою-клієнтом і програмою-сервером. Програма-клієнт функціонує на комп'ютері-клієнті і формує запит на обслуговування, а програма-сервер функціонує на комп'ютері, який

виконує запит. Комунікаційні пристрої локальних мереж відповідають стандартам конкретних базових технологій і підтримують передавання даних по конкретному фізичному середовищі. Вони призначені для здійснення комутації між вузлами мережі, відновлення якості електричних сигналів, збільшення мережі, фізичної та логічної структуризації локальних мереж.

До основних апаратних комунікаційних засобів локальних мереж відносяться мережеві адаптери (карти), повторювачі, концентратори, мости, комутатори, шлюзи і маршрутизатори.

Мережеві адаптери призначені для під'єднання комп'ютерів до кабельної системи мережі (див. рис. 1.1) і підтримують протоколи канального та фізичного рівнів певної мережевої технології. Кожний мережевий адаптер має свою унікальну MAC-адресу, яка автоматично присвоюється комп'ютеру, який використовує цей адаптер. Мережевий адаптер перетворює

Повторювач – це комунікаційний пристрій, який використовується для фізичного з'єднання двох сегментів фізичного середовища і відновлення якості (характеристик) електричних сигналів (рис. 1.2). Використання повторювача дозволяє виконати фізичну структуризацію побудованої на коаксиальному кабелі мережі, подвоїти її довжину, а також збільшити число під'єднаних до неї комп'ютерів.



Рисунок 1.2 – Приклад структуризації LAN з допомогою повторювача

Концентратор (hub) – це багатопортовий повторювач призначений для фізичного з'єднання декількох сегментів мережі (рис. 1.3). Фізична

структуризація мережі з допомогою концентраторів дозволяє змінити структуру мережі, її топологію, збільшити діаметр та число під'єднаних до мережі комп'ютерів, покращити надійність передавання даних. Сучасні концентратори можуть відключати від мережі порти з некоректно працюючим комп'ютером.



Рисунок 1.3– Приклад структуризації LAN за допомогою концентратора.

Міст – це комунікаційний пристрій з вбудованим процесором, призначений для ізоляції трафіка одного сегменту мережі від іншого на основі аналізу апаратної адреси отримувача повідомлення. Мережевий трафік – це інформаційний потік, який визначається об'ємом інформації, що передається по мережі одночасно і характеризує її завантаженість. Мережевий трафік складається з потоку кадрів, кожний з яких містить поле службової інформації та поле даних. Поле службової інформації обов'язково містить апаратні адреси отримувача і відправника кадру. Адресна таблиця моста містить інформацію про закріплені за сегментами мережі комп'ютери.

Комутатор (switch) – це високошвидкісний багатопортовий мультипроцесорний міст. Кожний порт комутатора керується окремим мікропроцесором, має свою буферну пам'ять та формує власні адресну таблицю. Кадр, який поступає в один з портів комутатора направляється тільки в той вихідний порт, в якому знаходиться адресат. Якщо вихідний порт

зайнятий передаванням іншої інформації, то кадр записується у буферну пам'ять та ставиться у чергу на вивід. Сучасні комутатори виконують цілий ряд додаткових функцій, направлених на підвищення продуктивності та надійності роботи мережі і захисту інформації. Комутатори 3-го рівня виконують протоколи мережевого рівня стеку комунікаційних протоколів і тому використовуються для ізоляції мережевого трафіку на основі аналізу IP-адрес пакетів.

Шлюз (gateway)– це комунікаційний пристрій, який об'єднує мережі, побудовані за різними технологіями і з різними типами протоколів.

Маршрутизатор (router)- це багатофункціональний комунікаційний пристрій, який підтримує протоколи мережевого рівня і призначений для об'єднання як локальних, так іглобальних мереж, побудованих за різними мережевими технологіями. В локальних мережах маршрутизатори використовують для їх структуризації шляхом поділу мереж, які використовують стек комунікаційних протоколів, на підмережі.

Структурована кабельна система являє собою комунікаційну систему, яка дозволяє легко будувати необхідну конфігурацію мережі із стандартних кабелів, які з'єднуються стандартними конекторами і комутуються з допомогою стандартних кросових панелей. Міжнародні стандарти описують вимоги до побудови кабельних систем, їх структури, типів і довжин кабелів, способів їх прокладання, типів розеток та способів розпаювання контактів, розташування комп'ютерів, монтажних шаф та розміщення в них комунікаційного обладнання (концентраторів, комутаторів, маршрутизаторів, комутаційних панелей і т.п.).

У сучасних LAN комунікаційне обладнання разом із структурованими кабельними системами належить до основного обладнання мережі і за своєю вартістю зрівнялося з вартістю комп'ютерів і програмного забезпечення.

### 1.3 Мережеві технології TokenRing та FDDI

#### 1.3.1 Мережа TokenRing

Мережа Token-Ring (маркерне кільце) була запропонована компанією IBM в 1985 році (перший варіант з'явився в 1980 році). Вона призначалася для об'єднання в мережу всіх типів комп'ютерів, що випускають IBM. Уже той факт, що її підтримує компанія IBM, найбільший виробник комп'ютерної техніки, говорить про те, що їй необхідно приділити особливу увагу. Але не менш важливо й те, що Token-Ring є в цей час міжнародним стандартом IEEE 802.5 (хоча між Token-Ring й IEEE 802.5 є незначні відмінності). Це ставить дану мережу на один рівень по статусі з Ethernet.



Рисунок 1.4– Мережа TokenRing.

Розроблялася Token-Ring як надійна альтернатива Ethernet. І хоча зараз Ethernet витісняє всі інші мережі, Token-Ring не можна вважати безнадійно застарілою. Більше 10 мільйонів комп'ютерів в усьому світі об'єднані цією мережею. Компанія IBM зробила все для максимально широкого поширення своєї мережі: була випущена докладна документація аж до принципів схем адаптерів. У результаті багато компаній, наприклад, 3COM, Novell, Western

Digital, Proteon й інші приступилися до виробництва адаптерів. До речі, спеціально для цієї мережі, а також для іншої мережі IBM PC Network була розроблена концепція NetBIOS. Якщо в створеній раніше мережі PC Network програми NetBIOS зберігалися в убудованій в адаптер постійній пам'яті, то в мережі Token-Ring уже застосовувалася емулююча NetBIOS програма. Це дозволило більш гнучко реагувати на особливості апаратури і підтримувати сумісність із програмами більш високого рівня.

Мережа Token-Ring має топологію кільце, хоча зовні вона більше нагадує зірку. Це пов'язано з тим, що окремі абоненти (комп'ютери) приєднуються до мережі не прямо, а через спеціальні концентратори або багатостанційні пристрої доступу (MSAU або MAU – Multistation Access Unit). Фізично мережа утворює зірково-кільцеву топологію. У дійсності ж абоненти поєднуються все-таки в кільце, тобто кожний з них передає інформацію одному сусідньому абонентові, а приймає інформацію від іншого.

Концентратор (MAU) при цьому дозволяє централізувати завдання конфігурації, відключення несправних абонентів, контроль роботи мережі й т.д.. Ніякої обробки інформації він не робить. Для кожного абонента в складі концентратора застосовується спеціальний блок підключення до магістралі (TCU – Trunk Coupling Unit), що забезпечує автоматичне включення абонента в кільце, якщо він підключений до концентратора й справний. Якщо абонент відключається від концентратора або ж він несправний, то блок TCU автоматично відновлює цілісність кільця без участі даного абонента. Спрацьовує TCU по сигналу постійного струму (так званий “фантомний” струм), що приходить від абонента, що бажає включитися в кільце. Абонент може також відключитися від кільця й провести процедуру самотестування. “Фантомний” струм ніяк не впливає на інформаційний сигнал, тому що сигнал у кільці не має постійної складової.

Конструктивно концентратор являє собою автономний блок з десятьма розніманнями на передній панелі. Вісім центральних рознімань (1...8) призначені для підключення абонентів (комп'ютерів) за допомогою адаптерних (Adapter cable) або радіальних кабелів. Два крайніх рознімання: вхідний RI (Ring In) і вихідний RO (Ring Out) служать для підключення до інших концентраторів за допомогою спеціальних магістральних кабелів (Path cable). Пропонуються настінний і настільний варіанти концентратора. Існують як пасивні, так й активні концентратори MAU. Активний концентратор відновлює сигнал, що приходить від абонента (тобто працює, як концентратор Ethernet). Пасивний концентратор не виконує відновлення сигналу, тільки перекомутує лінії зв'язку.

Концентратор у мережі може бути єдиним, у цьому випадку в кільце замикаються тільки абоненти, підключені до нього. Зовні така топологія виглядає, як зірка. Якщо ж потрібно підключити до мережі більше восьми абонентів, то кілька концентраторів з'єднуються магістральними кабелями й утворюють зірково-кільцеву топологію. Кільцева топологія дуже чутлива до обривів кабелю кільця. Для підвищення живучості мережі, в Token-Ring передбачений режим так званого згортання кільця, що дозволяє обійти місце обриву. У нормальному режимі концентратори з'єднані в кільце двома паралельними кабелями, але передача інформації виконується при цьому тільки по одному з них. У випадку одиночного ушкодження (обриву) кабелю мережа здійснює передачу по обох кабелях, обходячи тим самим ушкоджену ділянку. При цьому навіть зберігається порядок обходу абонентів, підключених до концентраторів. Правда, збільшується сумарна довжина кільця. У випадку множинних ушкоджень кабелю мережа розпадається на кілька частин (сегментів), не зв'язаних між собою, але зберігаючих повну працездатність. Максимальна частина мережі залишається при цьому зв'язаною, як і колись. Звичайно, це вже не рятує мережу в цілому, але дозволяє при правильному розподілі абонентів по концентраторах зберігати значну частину функцій ушкодженої мережі. Кілька концентраторів можуть

конструктивно поєднуватися в групу, кластер (cluster), усередині якого абоненти також з'єднані в кільце. Застосування кластерів дозволяє збільшувати кількість абонентів, підключених до одного центра, наприклад, до 16 (якщо в кластер входить два концентратори).

Як середовище передачі в мережі IBM Token-Ring спочатку застосовувалася кручена пара, як неекранована (UTP), так й екранована (STP), але потім з'явилися варіанти апаратури для коаксіального кабелю, а також для оптоволоконного кабелю в стандарті FDDI.

Основні технічні характеристики класичного варіанта мережі Token-Ring:

- максимальна кількість концентраторів типу IBM 8228 MAU – 12;
- максимальна кількість абонентів у мережі – 96;
- максимальна довжина кабелю між абонентом і концентратором – 45 метрів;
- максимальна довжина кабелю між концентраторами – 45 метрів;
- максимальна довжина кабелю, що з'єднує всі концентратори – 120 метрів;
- швидкість передачі даних – 4 Мбіт/с й 16 Мбіт/с.

Всі наведені характеристики відносяться до випадку використання неекранованої крученої пари. Якщо застосовується інше середовище передачі, характеристики мережі можуть відрізнятися. Наприклад, при використанні екранованої крученої пари (STP) кількість абонентів може бути збільшена до 260 (замість 96), довжина кабелю – до 100 метрів (замість 45), кількість концентраторів – до 33, а повна довжина кільця, що з'єднує концентратори – до 200 метрів. Оптоволоконний кабель дозволяє збільшувати довжину кабелю до двох кілометрів.

### 1.3.2 Мережа FDDI

Мережа FDDI (від англійського Fiber Distributed Data Interface, оптоволоконний розподілений інтерфейс даних) – це одна з новітніх розробок

стандартів локальних мереж. Стандарт FDDI був запропонований Американським національним інститутом стандартів ANSI (специфікація ANSI X3T9.5). Потім був прийнятий стандарт ISO 9314, що відповідає специфікаціям ANSI. Рівень стандартизації мережі досить високий.

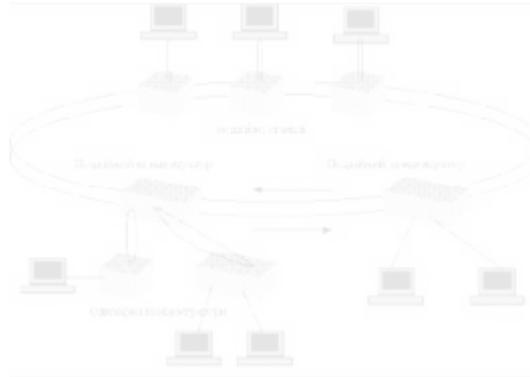


Рисунок 1.5– Мережа FDDI.

На відміну від інших стандартних локальних мереж, стандарт FDDI споконвічно орієнтувався на високу швидкість передачі (100 Мбіт/с) і на застосування найбільш перспективного оптоволоконного кабелю. Тому в цьому випадку розроблювачі не були стиснуті рамками старих стандартів, що орієнтувалися на низькі швидкості й електричний кабель.

Вибір оптоволоконна як середовища передачі визначив такі переваги нової мережі, як висока перешкодозахищеність, максимальна таємність передачі інформації й прекрасна гальванічна розв'язка абонентів. Висока швидкість передачі, що у випадку оптоволоконного кабелю досягається набагато простіше, дозволяє вирішувати багато завдань, недоступних менш швидкісним мережам, наприклад, передачу зображень у реальному масштабі часу. Крім того, оптоволоконний кабель легко вирішує проблему передачі даних на відстань декількох кілометрів без ретрансляції, що дозволяє

будувати більші по розмірах мережі, що охоплюють навіть цілі міста й мають при цьому всі переваги локальних мереж (зокрема, низький рівень помилок). Все це визначило популярність мережі FDDI, хоча вона поширена ще не так широко, як Ethernet й Token-Ring.

За основу стандарту FDDI був узятий метод маркерного доступу, передбачений міжнародним стандартом IEEE 802.5 (Token-Ring). Несуттєві відмінності від цього стандарту визначаються необхідністю забезпечити високу швидкість передачі інформації на великі відстані. Топологія мережі FDDI – це кільце, найбільш підходяща топологія для оптоволоконного кабелю. У мережі застосовується два різнонаправлених оптоволоконних кабелі, один із яких звичайно перебуває в резерві, однак таке рішення дозволяє використати й повнодуплексну передачу інформації (одночасно у двох напрямках) з подвоєною ефективною швидкістю в 200 Мбіт/с (при цьому кожний із двох каналів працює на швидкості 100 Мбіт/с). Застосовується й зірково-кільцева топологія з концентраторами, включеними в кільце (як в Token-Ring).

Основні технічні характеристики мережі FDDI:

- Максимальна кількість абонентів мережі – 1000.
- Максимальна довжина кільця мережі – 20 кілометрів.
- Максимальна відстань між абонентами мережі – 2 кілометри.
- Середовище передачі – багатомодовий оптоволоконний кабель (можливе застосування електричної крученої пари).
- Метод доступу – маркерний.
- Швидкість передачі інформації – 100 Мбіт/с (200 Мбіт/с для дуплексного режиму передачі).

Обмеження на загальну довжину мережі в 20 км зв'язане не із загасанням сигналів у кабелі, а з необхідністю обмеження часу повного проходження сигналу по кільцю для забезпечення гранично припустимого часу доступу. А максимальна відстань між абонентами (2 км при багатомодовому кабелі) визначається саме загасанням сигналів у кабелі (воно

не повинне перевищувати 11 дБ). Передбачена також можливість застосування одномодового кабелю, і в цьому випадку відстань між абонентами може досягати 45 кілометрів, а повна довжина кільця – 200 кілометрів.

Є також реалізація FDDI на електричному кабелі (CDDI – Copper Distributed Data Interface або TPDDI – Twisted Pair Distributed Data Interface). При цьому використовується кабель категорії 5 з розніманнями RJ-45. Максимальна відстань між абонентами в цьому випадку повинна бути не більше 100 метрів. Вартість устаткування мережі на електричному кабелі в кілька разів менше. Але ця версія мережі вже не має настільки очевидних переваг перед конкурентами, як споконвічна оптоволоконна FDDI. Електричні версії FDDI стандартизовані набагато гірше оптоволоконних, тому сумісність устаткування різних виробників не гарантується.

Стандарт FDDI для досягнення високої гнучкості мережі передбачає включення в кільце абонентів двох типів:

- Абоненти (станції) класу А (абоненти подвійного підключення, DAS – Dual-Attachment Stations) підключаються до обох (внутрішнього і зовнішнього) кілець мережі. При цьому реалізується можливість обміну зі швидкістю до 200 Мбіт/с або резервування кабелю мережі (при ушкодженні основного кабелю використовується резервний). Апаратура цього класу застосовується в самих критичних з погляду швидкодії частинах мережі.
- Абоненти (станції) класу В (абоненти одинарного підключення, SAS – Single-Attachment Stations) підключаються тільки до одного (зовнішнього) кільця мережі. Вони більш прості й дешеві, у порівнянні з адаптерами класу А, але не мають їхніх можливостей. У мережу вони можуть включатися тільки через концентратор або обхідний комутатор, що відключає їх у випадку аварії.

FDDI визначає чотири типи портів абонентів:

- Порт А призначений тільки для пристроїв подвійного підключення, його вхід підключається до первинного (зовнішнього) кільця, а вихід – до вторинного (внутрішнього) кільця.
- Порт В призначений тільки для пристроїв подвійного підключення, його вхід підключається до вторинного (внутрішнього) кільця, а вихід – до первинного (зовнішнього) кільця. Порт А звичайно з'єднується з портом В, а порт В – з портом А.
- Порт М (Master) призначений для концентраторів і з'єднує два концентратори між собою або концентратор з абонентом при одному кільці. Порт М як правило з'єднується з портом S.
- Порт S (Slave) призначений тільки для пристроїв одинарного підключення (концентраторів й абонентів). Порт S звичайно з'єднується з портом М.

Стандарт FDDI передбачає також можливість реконфігурації мережі з метою збереження її працездатності у випадку ушкодження кабелю.

#### 1.4 Мережева технологія Ethernet

Найбільше поширення серед стандартних мереж одержала мережа Ethernet. Уперше вона з'явилася в 1972 році (розроблювачем виступила відома фірма Xerox). Мережа виявилася досить вдалою, і внаслідок цього її в 1980 році підтримали такі найбільші компанії, як DEC й Intel (об'єднання цих компаній назвали DIX по перших буквах їхніх назв). Їхніми стараннями в 1985 році мережа Ethernet стала міжнародним стандартом, її прийняли найбільші міжнародні організації по стандартах: комітет 802 IEEE (Institute of

Electrical and Electronic Engineers) і ECMA (European Computer Manufacturers Association).



Рисунок 1.6– Кабель UTP з роз'ємом 8P8C, що використовується в Ethernet-мережах .

Стандарт одержав назву IEEE 802.3 (по-англійському читається як “eight oh two dot three”). Він визначає множинний доступ до моноканалу типу шина з виявленням конфліктів і контролем передачі. Цьому стандарту задовольняли й деякі інші мережі, тому що рівень його деталізації невисокий. У результаті мережі стандарту IEEE 802.3 нерідко були несумісні між собою як по конструктивним, так і по електричних характеристиках. Однак останнім часом стандарт IEEE 802.3 вважається стандартом саме мережі Ethernet.

Основні характеристики первісного стандарту IEEE 802.3:

- топологія – шина;
- середовище передачі – коаксіальний кабель;
- швидкість передачі – 10 Мбіт/с;
- максимальна довжина мережі – 5 км;
- максимальна кількість абонентів – до 1024;
- довжина сегмента мережі – до 500 м;

- кількість абонентів на одному сегменті – до 100;
- метод доступу – CSMA/CD;
- передача вузькополосна, тобто без модуляції (моноканал).



Рисунок 1.7– Роз'єм Ethernet на неттопі Gigabyte BR1X.

Мережа Ethernet зараз найбільш популярна у світі (більше 90% ринку), приблизно такою вона й залишиться в найближчі роки. Цьому в чималому ступені сприяло те, що із самого початку характеристики, параметри, протоколи мережі були відкриті, у результаті чого величезне число виробників в усьому світі стали випускати апаратуру Ethernet, повністю сумісну між собою.

У класичній мережі Ethernet застосовувався 50-омний коаксіальний кабель двох видів (товстий і тонкий). Однак останнім часом (з початку 90-х років) найбільше поширення одержала версія Ethernet, що використовує як середовище передачі кручені пари. Визначений також стандарт для застосування в мережі оптоволоконного кабелю. Для обліку цих змін у споконвічний стандарт IEEE 802.3 були зроблені відповідні додавання. В 1995 році з'явився додатковий стандарт на більш швидку версію Ethernet, що

працює на швидкості 100 Мбіт/с (так званий Fast Ethernet, стандарт IEEE 802.3u), що використовує як середовище передачі кручену пару або оптоволоконний кабель. В 1997 році з'явилася й версія на швидкості 1000 Мбіт/с (Gigabit Ethernet, стандарт IEEE 802.3z). Крім стандартної топології шина усе ширше застосовуються топології типу пасивна зірка й пасивне дерево. При цьому передбачається використання репітерів (повторювачі) і репітерних концентраторів, що з'єднують між собою різні частини (сегменти) мережі. У результаті може сформуватися деревоподібна структура на сегментах різних типів.

Як сегмент (частина мережі) може виступати класична шина або одиничний абонент. Для шинних сегментів використовується коаксіальний кабель, а для променів пасивної зірки (для приєднання до концентратора одиночних комп'ютерів) – кручена пара й оптоволоконний кабель. Головна вимога до отриманої в результаті топології – щоб у ній не було замкнутих шляхів (петель). Фактично виходить, що всі абоненти з'єднані у фізичну шину, тому що сигнал від кожного з них поширюється відразу в усі сторони й не повертається назад (як у кільці). Максимальна довжина кабелю мережі в цілому (максимальний шлях сигналу) теоретично може досягати 6,5 кілометрів, але практично не перевищує 3,5 кілометрів.

У мережі Fast Ethernet не передбачена фізична топологія шина, використовується тільки пасивна зірка або пасивне дерево. До того ж в Fast Ethernet набагато більш жорсткі вимоги до граничної довжини мережі. Адже при збільшенні в 10 разів швидкості передачі й збереженні формату пакета його мінімальна довжина стає в десять разів коротше. У такий спосіб в 10 разів зменшується припустима величина подвійного часу проходження сигналу по мережі (5,12 мкс проти 51,2 мкс в Ethernet). Для передачі інформації в мережі Ethernet застосовується стандартний манчестерський код. Доступ до мережі Ethernet здійснюється по випадковому методу CSMA/CD, що забезпечує рівноправність абонентів. Довжина кадрів Ethernet

(тобто пакета без преамбули) повинна бути не менш 512 бітових інтервалів або 51,2 мкс (саме така гранична величина подвійного часу проходження в мережі). Передбачено індивідуальну, групову й широкомовну адресацію.

У пакет Ethernet входять наступні поля:

- Преамбула складається з 8 байт, перші сім являють собою код 10101010, а останній байт – код 10101011. У стандарті IEEE 802.3 восьмий байт називається ознакою початку кадру (SFD – Start of Frame Delimiter) і утворює окреме поле пакета.
- Адреси одержувача (приймача) і відправника (передавача) включають по 6 байт. Ці адресні поля обробляються апаратурами абонентів.
- Поле керування (L/T – Length/Type) містить інформацію про довжину поля даних. Воно може також визначати тип використовуваного протоколу. Прийнято вважати, що якщо значення цього поля не більше 1500, то воно вказує на довжину поля даних. Якщо ж його значення більше 1500, то воно визначає тип кадру. Поле керування обробляється програмно.
- Поле даних повинне містити в собі від 46 до 1500 байт даних. Якщо пакет повинен містити менш 46 байт даних, то поле даних доповнюється байтами заповнення. Відповідно до стандарту IEEE 802.3, у структурі пакета виділяється спеціальне поле заповнення (pad data – незначні дані), що може мати нульову довжину, коли даних досить (більше 46 байт).
- Поле контрольної суми (FCS – Frame Check Sequence) містить 32-розрядну циклічну контрольну суму пакета (CRC) і служить для перевірки правильності передачі пакета.

Таким чином, мінімальна довжина кадру (пакета без преамбули) становить 64 байти (512 біт). Саме ця величина визначає максимально припустиму подвійну затримку поширення сигналу по мережі в 512 бітових інтервалів (51,2 мкс для Ethernet або 5,12 мкс для Fast Ethernet). Стандарт припускає, що

преамбула може зменшуватися при проходженні пакета через різні мережні пристрої, тому вона не враховується. Максимальна довжина кадру дорівнює 1518 байтам (12144 біта, тобто 1214,4 мкс для Ethernet, 121,44 мкс для Fast Ethernet). Це важливо для вибору розміру буферної пам'яті мережного встаткування й для оцінки загальної завантаженості мережі.

Для мережі Ethernet, що працює на швидкості 10 Мбіт/с, стандарт визначає чотири основних типи сегментів мережі, орієнтованих на різні середовища передачі інформації:

- 10BASE5 (товстий коаксіальний кабель);
- 10BASE2 (тонкий коаксіальний кабель);
- 10BASE-T (кручена пара);
- 10BASE-FL (оптоволоконний кабель).

Найменування сегмента містить у собі три елементи: цифра "10" означає швидкість передачі 10 Мбіт/с, слово BASE – передачу в основній смузі частот (тобто без модуляції високочастотного сигналу), а останній елемент – припустиму довжину сегмента: "5" – 500 метрів, "2" – 200 метрів (точніше, 185 метрів) або тип лінії зв'язку: "Т" – кручена пари (від англійського "twisted-pair"), "F" – оптоволоконний кабель (від англійського "fiber optic"). Точно так само для мережі Ethernet, що працює на швидкості 100 Мбіт/с (Fast Ethernet) стандарт визначає три типи сегментів, що відрізняються типами середовища передачі:

- 100BASE-T4 (зчетверена кручена пари);
- 100BASE-TX (здвоєна кручена пари);
- 100BASE-FX (оптоволоконний кабель).

Тут цифра "100" означає швидкість передачі 100 Мбіт/с, буква "Т" – кручену пару, буква "F" – оптоволоконний кабель. Типи 100BASE-TX й 100BASE-FX іноді поєднують під ім'ям 100BASE-X, а 100BASE-T4 й 100BASE-TX – під ім'ям 100BASE-T.

Мережа Ethernet не відрізняється ні рекордними характеристиками, ні оптимальними алгоритмами, вона уступає по ряду параметрів іншим стандартним мережам. Але завдяки потужній підтримці, найвищому рівню стандартизації, величезним обсягам випуску технічних засобів, Ethernet вигідно виділяється серед інших стандартних мереж, і тому будь-яку іншу мережну технологію прийнято порівнювати саме з Ethernet.

Розвиток технології Ethernet іде по шляху все більшого відходу від первісного стандарту. Застосування нових середовищ передачі й комутаторів дозволяє істотно збільшити розмір мережі. Відмова від манчестерського коду (у мережі Fast Ethernet й Gigabit Ethernet) забезпечує збільшення швидкості передачі даних і зниження вимог до кабелю. Відмова від методу керування CSMA/CD (при повнодуплексному режимі обміну) дає можливість різко підвищити ефективність роботи й зняти обмеження з довжини мережі. Проте, всі нові різновиди мережі також називаються мережею Ethernet.

### 1.5 Вибір технології побудови локальної мережі

Для організації корпоративної мережі можна застосовувати різноманітні технології канального рівня. В процесі жорсткої конкуренції між різними технологіями перемогу здобуло сімейство технологій Ethernet. В останні роки технології цього сімейства фактично стали стандартом побудови корпоративних мереж. Ці технології відносно прості і дешеві. На сьогоднішній день сімейство технологій Ethernet включає декілька технологій, які забезпечують ієрархію швидкостей від 10 Мбіт / с до 10 Гбіт / с. Для створення мереж на базі технології Ethernet можна використовувати два типи кабелю – мідну виту пару та оптичний кабель. Також існує варіант реалізації цієї технології для безпроводної мережі.

Сьогодні існують наступні класи технології Ethernet:

- 10 Base XX – забезпечує швидкість передачі до 10 Мбіт/с;
- 100 Base XX – забезпечує швидкість передачі до 100 Мбіт/с;
- 1000 Base XX – забезпечує швидкість передачі до 1000 Мбіт/с;
- 10 GBase XX – забезпечує швидкість передачі до 10 Гбіт/с.

Технологія Ethernet 10 GBase XX найбільш нова технологія, в більшості своїй працює на основі оптичних кабелів, однак у 2007 році була розроблена специфікація 10 GBase T (IEEE 802.3an) яка дозволила використовувати мідну екрановану виту пару.

Ethernet і Fast Ethernet мережі використовують протокол доступу до фізичної середовища - CSMA/CD (Carrier-sense Multiple Access with Collision Detection). Це дозволяє одночасно передавати дані тільки лише одному пристрою. Якщо два пристрої спробують передати дані одночасно відбувається зіткнення (колізія) між пакетами. Передавач виявляє колізію і на деякий час припиняє передачу, після чого пробує надіслати пакет знову.

Завдяки сумісності із протоколом IP, простоті розгортання і, що найважливіше, оптимальному співвідношенню ціна/якість, системи на базі Ethernet набувають ключового значення в мережах доступу.

Основний недолік мереж Ethernet обумовлений методом доступу до середовища передачі - при наявності в мережі великої кількості вузлів, які намагаються передавати інформацію одночасно зростає кількість колізій, а пропускна спроможність мережі падає. У таблиці 1.2 наведено основні риси та варіанти реалізації сімейства технологій Ethernet.

Таблиця 1. – Характеристики сімейства технологій Ethernet.

	Ethernet	FastEthernet	GigabitEthernet	10 Gigabit Ethernet
Швидкість, Мбіт/с	10	100	1000	10 000
Середовище передачі	Вита пара, коаксіальний кабель, ОПТОВОЛОКНО	Вита пара, ОПТОВОЛОКНО	Вита пара, ОПТОВОЛОКНО	Вита пара, ОПТОВОЛОКНО
Стандарти для реалізації	10 Base2 10 BaseT 10 Base5 10 Base FL 10 Base F	100 Base TX 100 Base T4 100 Base-FX 100 Base-SX 100 Base T2	1000 Base-TX 1000 Base-LX 1000 Base-SX 1000 Base-CX 1000Base-T	10 GBase CX4 10 GBase SR 10 GBase LR 10 GBase SW 10 GBase T
Топологія	Шина, зірка	Зірка	Зірка	Зірка

Для побудови локальної мережі для НВП «Каскад» було вибрано технологію Ethernet. Це найпоширеніший і найбільш надійний стандарт для локальних мереж, що забезпечує високу швидкість передачі даних, масштабованість і сумісність з більшістю мережевих пристроїв. Використання комутаторів дозволить ефективно керувати мережевими ресурсами, а впровадження оптоволоконних з'єднань між ключовими вузлами забезпечить мінімальні затримки і високу пропускну здатність. Крім того, Ethernet підтримує різноманітні протоколи безпеки, що дозволяє захистити мережу від несанкціонованого доступу і забезпечити стабільну роботу в умовах високих навантажень.

### 1.6 Побудова комп'ютерної мережі з використанням структурованої кабельної системи

Структурована кабельна система – це комунікаційна система, за допомогою якої простіше побудувати мережу з використанням стандартних кабелів, що поєднуються конекторами і комутуються з застосуванням кросових панелей. Міжнародні стандарти висувають вимоги до побудови структури кабельних систем, типів і довжин використаних кабелів, способів прокладання кабелю, типів зовнішніх розеток, розташування комп'ютерів в приміщенні, монтажних шаф в серверних та розміщення всередині них комунікаційного обладнання (концентраторів, комутаторів, маршрутизаторів і т.п.).

У сучасних ЛКМ мережеве обладнання разом із структурованими кабельними системами відноситься до основного обладнання мережі і за своєю вартістю практично рівне вартості комп'ютерів і ПЗ.

В основі будь-якої СКС покладена топологія дерева, яку іноді називають ієрархічною зіркою. Функції вузлів СКС виконує мережеве обладнання різних видів, а саме зовнішні розетки, які використовуються користувачами СКС, та панелі різних видів, з якими працює персонал обслуговування. Мережеве обладнання з'єднується між собою кабелями (оптоволоконний, коаксіальний, вита пара).

Всі кабелі, які входять до службових приміщень, обов'язково підводяться на згадані вище панелі, на яких за допомогою шнурів здійснюються всі підключення в процесі поточного використання СКС. Стандарти дозволяють також організацію резервних шляхів передачі даних. Все це в поєднанні зі застосованою деревовидною топологією у випадку, що

стосується СКС, забезпечує гнучкість та надійність СКС, а також можливість легкого переналаштування та перерозподілу кабельної системи під конкретні потреби. Службові приміщення необхідні для побудови СКС та інформаційної безпеки в цілому. В загальному випадку вони діляться на апаратні та кросові.

В службових приміщеннях разом зі згрупованим мережним обладнанням СКС розміщується мережеве обладнання загального використання для працівників підприємства. Такі приміщення обладнуються фальшивими підлогами, пожежними системами, вентиляції та контролю доступу. Рівень встановлюваних всерверній різноманітних мережевих пристроїв та систем технічного забезпечення повинен відповідати рівню встановленого в ній комп'ютерного та телекомунікаційного обладнання.

Принципи керування СКС цілком та повністю залежать від її структури. Розрізняють одноточкове та багатоточкове керування. Під багатоточковим керуванням розуміють керування СКС, яка побудована за архітектурою ієрархічної зірки, тобто містить магістральну систему хоча б одного рівня. Основним показником багатоточкового керування є необхідність виконання перепідключення мінімум двох кабелів (або елементів, що їх замінюють) в загальному випадку зміни налаштування. Використання цього принципу гарантує найбільшу гнучкість керування та ширші можливості застосування СКС.

Архітектура одноточкового керування використовується в тоді, коли необхідно максимально спрощене керування кабельною системою. Її основним індикатором є пряме з'єднання всіх зовнішніх розеток робочих місць з мережевим обладнанням в єдиному службовому приміщенні. Така ж архітектура може використовуватись для СКС, що встановлені в одному будинку та не мають магістральних підмереж. Одним із оптимальних способів підвищення апаратно-економічної ефективності СКС офісних будинків є мінімальне використання різних типів кабелів, які використовуються для їх побудови.

В СКС згідно стандарту ISO/IEC 11801 допускаються лише:

- симетричні електричні кабелі на основі екранованої або неекранованої пари з хвильовим опором 100, 120 та 150 Ом;
- одномодові та багатомодові оптоволоконні кабелі.

Кабелі з витих пар використовуються в першу чергу для створення горизонтальної проводки. По цьому кабелю передаються як телефонні сигнали танизкошвидкісна інформація, так і високошвидкісні дані. Зазвичай оптоволоконні кабелі застосовують на зовнішніх магістралях. Процес проектування комплексу інформаційних систем підприємства, в тому числі СКС як складової його частини, у відповідності з прийнятою в промисловорозвинутих країнах різновидами розділяється на дві основні фази: архітектурна та телекомунікаційна.

Основним завданням архітектурної фази є:

- визначити структуру структурованої кабельної системи, що відповідає технічним та економічним характеристикам;
- адаптувати приміщення та конструкції на рівні рішення будинку під вимоги СКС.

Телекомунікаційна фаза характеризується розробкою конкретної структури СКС, до складу якої входить перелік обладнання, план та розміщення.

### 1.7 Призначення розробки та вимоги до апаратного та програмного забезпечення мереж

Призначення розробки мережі для НВП «Каскад» полягає у створенні надійної, масштабованої та безпечної мережевої інфраструктури, яка забезпечить ефективну взаємодію між усіма підрозділами підприємства,

підвищить продуктивність праці, забезпечить безперебійну роботу та захист інформаційних ресурсів. Мережа повинна підтримувати різні типи користувачів, включаючи офісних працівників, інженерів, технічний персонал та адміністративний відділ, забезпечуючи їм доступ до необхідних ресурсів та сервісів.

Апаратні вимоги включають наявність сучасних серверів з високою продуктивністю та достатнім об'ємом оперативної пам'яті і сховища даних, маршрутизаторів, комутаторів, бездротових точок доступу для забезпечення повного покриття офісних та виробничих приміщень, мережевих кабелів категорії 6 або вищої для забезпечення високошвидкісного з'єднання, а також резервного обладнання для забезпечення безперервної роботи мережі у випадку збоїв.

Програмні вимоги включають використання надійної операційної системи для серверів (наприклад, Windows Server або Linux), системи віртуалізації для оптимального використання апаратних ресурсів, сучасного програмного забезпечення для управління мережею, включаючи інструменти для моніторингу та адміністрування, антивірусного програмного забезпечення та програм для захисту від несанкціонованого доступу. Також необхідно забезпечити сумісність з існуючим програмним забезпеченням, яке використовується на підприємстві, та можливість його подальшого оновлення і масштабування.

Забезпечення надійного та швидкого доступу до мережі вимагає наявності ширококутового інтернет-з'єднання з резервними каналами для мінімізації простоїв. Інтеграція з хмарними сервісами може забезпечити додаткову гнучкість і резервування даних. Необхідно передбачити використання VPN для захищеного доступу до корпоративних ресурсів для віддалених співробітників.

Мережа повинна бути спроектована з урахуванням можливостей для подальшого розширення та модернізації, включаючи **впровадження нових**

технологій, таких як Інтернет речей (IoT), для підвищення ефективності виробничих процесів.

## 2 ПЛАНУВАННЯ СТРУКТУРИ МЕРЕЖІ

### 2.1 План приміщень

Науково-виробниче підприємство "Каскад" є провідною організацією, яка спеціалізується на розробці, виробництві та впровадженні інноваційних технологій та обладнання в різних галузях промисловості. Компанія зосереджується на створенні високоякісних продуктів, що відповідають сучасним стандартам та потребам ринку."Каскад" об'єднує науково-дослідний потенціал та виробничі потужності, що дозволяє здійснювати повний цикл розробки – від ідеї та прототипу до серійного виробництва і впровадження готових рішень. Завдяки висококваліфікованому персоналу, сучасному обладнанню та строгому контролю якості, підприємство забезпечує надійність і ефективність своєї продукції.

Підприємство активно співпрацює з науковими установами, залучаючи до спільних проектів провідних фахівців і новітні розробки. Це сприяє постійному вдосконаленню технологій та розширенню асортименту продукції, що охоплює різні сфери, такі як енергетика, телекомунікації, машинобудування та інші.

Приміщення даного підприємства складається з шістьох, кабінетів (рис.2.1), що мають такі параметри:

Кабінет А:

- довжина 7 м;
- ширина 5 м;
- висота 3 м.
- вікна 1
- кондиціонери 1

Кабінет В:

- довжина 7 м;
- ширина 4 м;
- висота 3 м.
- вікна 0
- кондиціонери 1

Кабінет S:

- довжина 7 м;
- ширина 5 м;
- висота 3 м.
- вікна 1
- кондиціонери 1

Кабінет 1:

- довжина 9 м;
- ширина 9 м;
- висота 3 м.
- вікна 2
- кондиціонери 2

Кабінет 2:

- довжина 10 м;
- ширина 9 м;
- висота 3 м.
- вікна 2
- кондиціонери 2

Кабінет 3:

- довжина 19 м;
- ширина 5 м;

- висота 3 м.
- вікна 3
- кондиціонери 2.

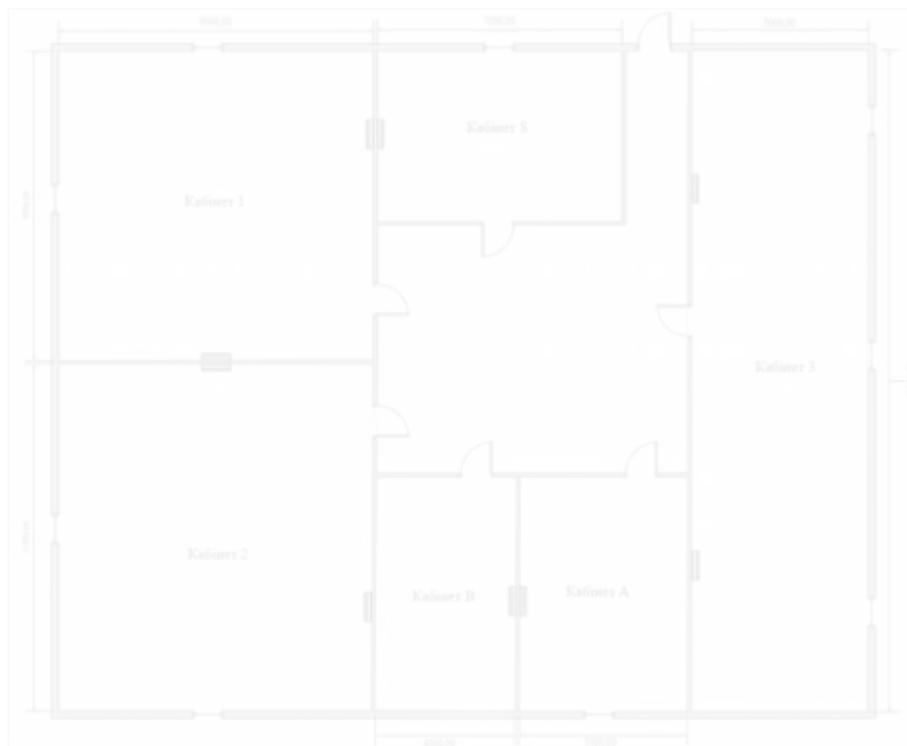


Рисунок 2.1 – Вихідний план приміщення

В приміщенні є 9 вікон, що забезпечують природне освітлення та лампи для штучного освітлення. Для забезпечення вентиляції передбачені кондиціонери. Так, розташування сервера в окремій кімнаті (S) мережевого адміністратора є раціональним вибором з різних причин, а саме:

- Шум. Сервери можуть генерувати значний рівень шуму в процесі роботи, особливо при високому навантаженні. Розміщення сервера

окремо від інших робочих станцій допоможе знизити рівень шуму в робочому середовищі і покращити комфорт для користувачів.

- Технічне обслуговування: Важливо мати постійний доступ до сервера для технічного обслуговування, налаштування і ремонту. Розташування сервера в окремій кімнаті, призначеній для мережевого адміністратора, дозволить забезпечити зручний доступ до нього і зменшити втрати часу на рух між вузлами мережі.
- Захист інформації: Розташування сервера в окремій кімнаті допоможе обмежити фізичний доступ до нього. Це є важливим аспектом з точки зору безпеки і захисту конфіденційної інформації. Захищений доступ до сервера зменшить ризик несанкціонованого доступу або пошкодження обладнання.

Враховуючи ці фактори, розташування сервера в окремій кімнаті, яка задовольняє вимогам щодо шуму, ізоляції та обмеженого доступу, є раціональним вибором для забезпечення оптимального функціонування мережі. На рис. 2.1 зображено план приміщень НВП «Каскад».

## 2.2 Мережна архітектура

Спроектвана локальна мережа розроблена з використанням топології «ієрархічна зірка». Така локальна мережа має центральний компонент – маршрутизатор. «Ієрархічна зірка» - це популярна та ефективна топологія, її часто застосовують через легкість обслуговування кінцевих пристроїв.

Прокладання кабельної проводки:

Для прокладання кабельної проводки (рис 2.3) я рекомендую застосувати для з'єднання кабелів з кабелями інших підсистем або активним обладнанням комутатори TP-Link TL-SG108PE та конвектори RJ-45.



Рисунок 2.2 – Прокладання кабельної проводки

### 2.3 Мережні ресурси

Мережа має наступне обладнання:

- 13 персональних комп'ютерів;
- 2 принтери;
- 1 сервер;
- 5 комутаторів;

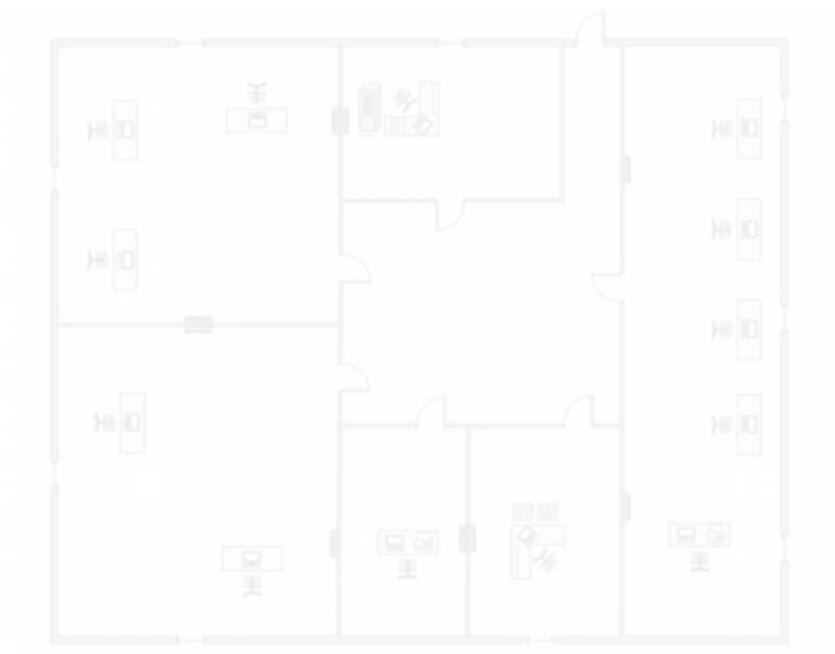


Рисунок 2.3 – розміщення обладнання

Вибране обладнання розміщене безпосередньо в місцях використання, щовідображено на рисунку 2.3. В якості робочогообладнаннядля працівників обрано персональні комп'ютери. Для друку документації використовуються принтери.

### 3 ВИБІР ТА ОБҐРУНТУВАННЯ АПАРАТНИХ І ПРОГРАМНИХ ЗАСОБІВ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

#### 3.1 Вибір активного обладнання

Вибір активного обладнання для комп'ютерної мережі підприємства включає визначення та обґрунтування використання маршрутизаторів, комутаторів, точок доступу та інших мережевих пристроїв. Нижче наведено перелік вибраного активного обладнання:

##### Персональний комп'ютер

Враховуючи особливості локальної мережі, оптимальним вибором стане комп'ютер HP Desktop Pro G2 MT(7EM90ES) (10 495 грн).

##### Принтер

Для друку та сканування матеріалів та документації обрано струменеві принтери HP DeskJet 2320 (7WN42B) (1599 грн).

##### Сервер

Сервер Dell PowerEdge R610 дозволяє швидко працювати з задачами, необхідними для малого та середнього бізнесу, забезпечує швидке розгортання, обробку та використання даних (6815 грн). Основні особливості: – продумана конструкція; – енергоефективність; – спрощене управління інфраструктурою; – широкі можливості віртуалізації.

##### Комутатор

Комутатор – це обов'язкова складова будь-якої локальної мережі, що забезпечує з'єднання між компонентами мережі та дозволяє передавати дані з однієї робочої станції в іншу. Комутатор TP-Link TL-SG108PE був обраний відштовхуючись від кількості робочих станцій, що будуть до нього під'єднані, а також за загальними характеристиками: – наявність PoE-портів; – 8 портів RJ-45 10/100/1000 Мбіт/с; – підтримка PoE 802.3af на 4 портах; –

пропускна здатність 16 Гбіт/с; – таблиця MAC-адрес:4к; – розмір буфера: 1,5 Мбіт.

### 3.2 Технологія монтажу СКС

Для монтажу структурованої кабельної системи (СКС) для НВП «Каскад» оптимальним вибором буде використання технології Cat6 UTP (неекранована вита пара категорії 6). Ця технологія забезпечує високу швидкість передачі даних до 10 Гбіт/с і є надійною для сучасних офісних та виробничих середовищ.

Процес монтажу СКС починається з планування. Спочатку необхідно провести огляд приміщень та визначити місця встановлення робочих станцій, серверів, комутаторів, точок доступу Wi-Fi та іншого обладнання. На основі цього створюється схема розташування кабельних трас та комутаційних центрів.

Після цього відбувається прокладання кабелів. Кабелі Cat6 UTP прокладаються через кабельні канали або лотки. Важливо уникати згинів кабелів під гострим кутом та забезпечити достатню відстань від джерел електромагнітних завад. Кабелі ведуть до телекомунікаційних шаф, де будуть встановлені комутатори та інше активне мережеве обладнання.

У телекомунікаційних шафах встановлюються патч-панелі, до яких підключаються кабелі. Кожен кабель маркується згідно зі схемою, що полегшує подальше обслуговування та модернізацію системи. Кінці кабелів обробляються та підключаються до відповідних портів патч-панелей за допомогою інструментів для обжимання.

Далі встановлюються настінні або підлогові телекомунікаційні розетки в робочих місцях. До них підключаються інші кінці кабелів Cat6 UTP. Розетки також маркуються для зручності користувачів і технічного персоналу.

Після монтажу всіх кабелів та розеток проводиться тестування системи. Використовуючи спеціальне тестове обладнання, перевіряється цілісність кабельних з'єднань, відсутність перехресних завод та відповідність кабелів стандартам Cat6. Виявлені несправності виправляються до досягнення повної відповідності системи вимогам.

На завершення встановлюється активне мережеве обладнання: комутатори, маршрутизатори, сервери, точки доступу Wi-Fi. Вони підключаються до патч-панелей за допомогою патч-кордів. Після цього проводиться конфігурація мережевого обладнання та налаштування мережевих сервісів.

Таким чином, технологія монтажу СКС Cat6 UTP забезпечує високу продуктивність, надійність та гнучкість локальної мережі для НВП «Каскад», що відповідає сучасним вимогам та стандартам.

### 3.3 Рекомендації щодо перевірки працездатності мережі

Перевірка працездатності мережі починається з візуального огляду обладнання, щоб переконатися, що всі пристрої, такі як маршрутизатори, комутатори та точки доступу, увімкнені та функціонують правильно. Особливу увагу слід звернути на індикатори на пристроях, які можуть сигналізувати про наявність помилок або попереджень. Далі потрібно перевірити фізичні з'єднання, уважно оглянувши всі кабелі на предмет пошкоджень або розривів. Важливо переконатися, що кабелі правильно підключені до відповідних портів.

Наступним кроком є тестування кабельної системи за допомогою кабельних тестерів, які допоможуть перевірити цілісність кабелів та їх відповідність стандартам. Це включає перевірку кожного порту на патч-панелях та розетках. Після цього варто провести перевірку конфігурації мережі, щоб упевнитися у правильності налаштувань IP-адрес, шлюзів, DHCP та DNS. Необхідно також перевірити конфігурації маршрутизаторів та комутаторів, звертаючи увагу на правильність налаштувань VLAN, маршрутизації та безпеки.

Для перевірки зв'язності між пристроями мережі виконується пінг-тестування, під час якого здійснюється пінг основних мережевих вузлів, таких як сервери, маршрутизатори та інтернет-шлюз. Далі, слід перевірити швидкість та пропускну здатність мережі за допомогою інструментів для тестування швидкості, таких як Speedtest, щоб оцінити затримки, втрати пакетів та стабільність з'єднання.

Моніторинг мережі є важливим аспектом, тому варто використовувати системи моніторингу, такі як Nagios або Zabbix, для спостереження за станом мережі в реальному часі. Налаштування сповіщень про будь-які збої або аномалії допоможе швидко реагувати на проблеми. Безпека мережі також потребує перевірки: необхідно переконатися, що всі захисні механізми, такі як фаєрволи, антивіруси та системи запобігання вторгнень (IPS/IDS), працюють належним чином. Для виявлення потенційних загроз варто виконати сканування вразливостей. Перевірка бездротової мережі включає тестування рівня сигналу та зони покриття Wi-Fi точок доступу, а також перевірку швидкості та стабільності бездротового з'єднання. На завершення, результати всіх тестів та перевірок потрібно задокументувати для майбутнього аналізу. Важливо також оновлювати документацію мережі відповідно до проведених змін та перевірок, щоб забезпечити точність та актуальність інформації про мережу. Таким чином, дотримання цих

рекомендацій сприятиме забезпеченню стабільної та ефективної роботи комп'ютерної мережі підприємства.

## 4 СТРАТЕГІЯ АДМІНІСТРУВАННЯ Й КЕРУВАННЯ

### 4.1 Загальні положення

Адміністрування та керування є ключовими елементами ефективного функціонування будь-якої організації. Стратегія адміністрування й керування включає в себе комплекс заходів, спрямованих на досягнення поставлених цілей організації через раціональне використання ресурсів, оптимізацію процесів та підвищення ефективності діяльності. Основними принципами стратегії є прозорість, відповідальність, інноваційність, орієнтація на результат та безперервне вдосконалення.

Важливим аспектом адміністрування є організаційна структура, яка визначає розподіл обов'язків, повноважень та відповідальності між працівниками. Ефективна структура сприяє кращій координації та комунікації, що дозволяє оперативно реагувати на зміни в зовнішньому середовищі.

Керування включає в себе планування, організацію, мотивацію та контроль. Планування передбачає встановлення цілей та визначення шляхів їх досягнення. Організація забезпечує створення умов для виконання планів, а мотивація - стимулює працівників до досягнення високих результатів. Контроль дозволяє оцінювати виконання поставлених завдань та коригувати дії в разі відхилень.

Стратегія адміністрування й керування також передбачає впровадження сучасних інформаційних технологій, що сприяють автоматизації процесів, підвищенню оперативності та точності даних, а також забезпечують доступ до необхідної інформації в режимі реального часу.

Для успішної реалізації стратегії важливо забезпечити навчання та розвиток персоналу, що включає підвищення кваліфікації, розвиток професійних навичок та підготовку майбутніх лідерів. Це сприяє формуванню компетентної та мотивованої команди, здатної ефективно вирішувати завдання організації.

Загалом, стратегія адміністрування й керування спрямована на створення умов для стабільного розвитку організації, підвищення її конкурентоспроможності та досягнення довгострокових цілей.

#### 4.2 Захист інформації в мережі

Захист інформації в мережі є критично важливим елементом стратегії адміністрування та керування сучасної організації. В умовах швидкого розвитку інформаційних технологій та зростання кількості кіберзагроз, забезпечення конфіденційності, цілісності та доступності даних стає одним з пріоритетних завдань. Ефективний захист інформації в мережі включає комплекс заходів, спрямованих на попередження несанкціонованого доступу, втрату або пошкодження даних. Це досягається шляхом впровадження сучасних технологій, дотриманням політик безпеки та регулярним навчанням персоналу. Одним з ключових аспектів захисту інформації є використання надійних методів аутентифікації та авторизації. Це включає в себе застосування багатофакторної аутентифікації, складних паролів та обмеження доступу до інформаційних ресурсів відповідно до ролей і обов'язків працівників.

Шифрування даних є ще одним важливим елементом стратегії захисту інформації. Шифрування забезпечує захист конфіденційної інформації під час передачі даних по мережі та при їх збереженні на носіях інформації. Використання сучасних алгоритмів шифрування дозволяє знизити ризики перехоплення або несанкціонованого доступу до даних. Системи виявлення та

запобігання вторгненням (IDS/IPS) є ефективним засобом захисту від мережеских атак. Вони дозволяють виявляти підозрілу активність у мережі, оперативно реагувати на потенційні загрози та запобігати можливим атакам. Регулярне оновлення програмного забезпечення та систем є важливим для забезпечення захисту від відомих вразливостей. Виробники програмного забезпечення постійно випускають оновлення, які усувають виявлені вразливості та підвищують загальний рівень безпеки системи.

Навчання та підвищення обізнаності працівників є невід'ємною частиною стратегії захисту інформації. Працівники повинні знати основні правила безпеки, уміти розпізнавати фішингові атаки та дотримуватись політик безпеки, встановлених в організації. Розробка планів реагування на інциденти дозволяє оперативно діяти у разі порушення безпеки інформації. Такий план повинен включати процедури виявлення, оцінки, реагування та відновлення після інциденту, а також забезпечувати мінімізацію можливих збитків.

Загалом, стратегія захисту інформації в мережі спрямована на створення комплексної системи безпеки, яка забезпечує надійний захист даних від різноманітних загроз та сприяє стабільному функціонуванню організації в умовах сучасного інформаційного середовища.

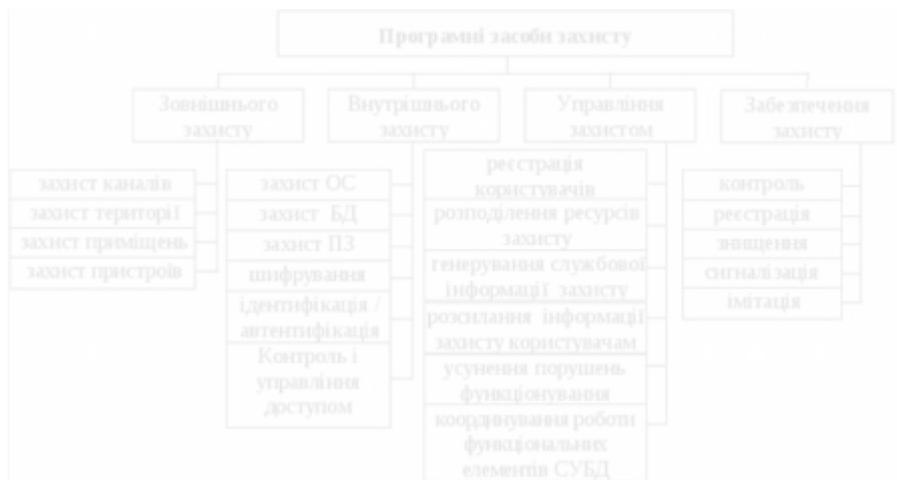


Рисунок 4.1 – Програмні засоби захисту

### 4.3 Облікові картки користувачів

Облікові картки користувачів є невід’ємною частиною системи адміністрування та керування в будь-якій організації. Вони забезпечують ідентифікацію, аутентифікацію та авторизацію користувачів, що дозволяє контролювати доступ до ресурсів та інформації. Ефективне управління обліковими картками користувачів сприяє підвищенню рівня безпеки та продуктивності організації. Створення та ведення облікових карток користувачів повинно базуватися на чітко визначених політиках та процедурах. Це включає в себе процеси створення, модифікації та видалення облікових записів, а також управління правами доступу. Важливо, щоб кожен користувач мав обмежений доступ відповідно до своїх обов’язків та ролі в організації, що зменшує ризики несанкціонованого доступу до конфіденційної інформації.

Основою для управління обліковими картками є надійна система аутентифікації. Використання багатофакторної аутентифікації (MFA) значно підвищує рівень безпеки, оскільки вимагає від користувача підтвердження своєї особи через декілька незалежних факторів. Це може бути комбінація

пароля, токена, біометричних даних або мобільного додатку. Регулярний аудит та моніторинг облікових записів користувачів дозволяє своєчасно виявляти та реагувати на потенційні загрози. Це включає перевірку активності користувачів, аналіз логів доступу та виявлення аномальної поведінки. В разі виявлення підозрілої активності слід оперативно вживати заходів для запобігання можливим порушенням безпеки. Управління паролями є важливим аспектом роботи з обліковими картками користувачів. Встановлення політик щодо складності та регулярної зміни паролів сприяє захисту від несанкціонованого доступу. Користувачам рекомендується використовувати унікальні паролі для різних систем та сервісів, а також зберігати їх у надійних менеджерах паролів.

Автоматизація процесів управління обліковими картками користувачів допомагає знизити ризик людських помилок та підвищити ефективність адміністрування. Використання спеціалізованих програмних рішень дозволяє автоматизувати створення, оновлення та видалення облікових записів, а також управління правами доступу на основі ролей. Важливим елементом стратегії є навчання та підвищення обізнаності користувачів щодо питань безпеки. Користувачі повинні знати про ризики, пов'язані з неправильною обробкою своїх облікових даних, та дотримуватись встановлених правил безпеки. Регулярні тренінги та інформаційні кампанії сприяють підвищенню рівня обізнаності та відповідальності серед працівників.

Загалом, ефективне управління обліковими картками користувачів є важливим аспектом стратегії адміністрування та керування. Воно забезпечує належний рівень безпеки, контролює доступ до ресурсів та сприяє стабільному функціонуванню організації в умовах зростаючих кіберзагроз.



Рисунок 4.2 – Зразок облікової карти користувача

#### 4.4 Журнал подій безпеки

Журнал подій безпеки є важливим інструментом для забезпечення надійного контролю та моніторингу інформаційної безпеки в організації. Він фіксує всі значущі події, пов'язані з безпекою, що дозволяє виявляти, аналізувати та реагувати на потенційні загрози вчасно та ефективно. Ведення журналу подій безпеки включає реєстрацію різних видів активності, таких як успішні та невдалі спроби входу в систему, зміни конфігурацій, доступ до критично важливих даних, підозрілі дії користувачів та інші події, що можуть свідчити про порушення безпеки. Це допомагає забезпечити повну прозорість та аудит всіх дій, що впливають на стан інформаційної безпеки.

Для ефективного використання журналу подій безпеки важливо визначити, які події мають бути зареєстровані, та встановити відповідні політики логування. Це дозволить зосередитися на найважливіших аспектах безпеки та уникнути перевантаження системи надмірною кількістю

даних. Регулярний аналіз журналу подій безпеки дозволяє виявляти аномалії та потенційні загрози на ранніх етапах. Використання спеціалізованих інструментів для автоматичного аналізу та кореляції подій значно підвищує ефективність цього процесу. Такі інструменти можуть генерувати попередження та звіти, які допомагають швидко ідентифікувати та реагувати на інциденти безпеки. Забезпечення цілісності та доступності журналу подій безпеки є критично важливим. Це включає захист від несанкціонованого доступу, модифікації або видалення записів. Зберігання журналу повинно здійснюватися у безпечному місці з обмеженим доступом, а також передбачати резервне копіювання для відновлення у разі втрати даних.

Важливим аспектом є також визначення періоду зберігання даних у журналі подій безпеки. Залежно від вимог законодавства, політик організації та потреб у аудиті, дані можуть зберігатися протягом певного часу, після чого вони можуть бути архівовані або видалені. Навчання персоналу, відповідального за моніторинг та аналіз журналу подій безпеки, сприяє підвищенню рівня безпеки в організації. **Працівники повинні мати необхідні знання та навички для ефективного використання інструментів моніторингу, аналізу подій та реагування на інциденти.**

Загалом, журнал подій безпеки є невід'ємною частиною стратегії адміністрування та керування безпекою. Він забезпечує систематичний підхід до моніторингу, аналізу та реагування на загрози, що сприяє захисту інформаційних ресурсів та забезпеченню стабільного функціонування організації.



Рисунок 4.3– Зразок журналу подій на Windows 10

#### 4.5 Установка пароля й політика облікових карток

Установка пароля та розробка політики облікових карток є важливими аспектами стратегії адміністрування та керування безпекою в будь-якій організації. Вони допомагають забезпечити надійний захист інформаційних ресурсів та запобігти несанкціонованому доступу до даних.

Установка пароля є першим кроком у забезпеченні безпеки облікових записів користувачів. Пароль повинен бути складним і надійним, складатися з комбінації різних символів (букв верхнього та нижнього регістрів, цифр, спеціальних символів) та мати достатню довжину. Рекомендується використовувати методи генерації паролів, що забезпечують випадковість та унікальність паролю.

Політика облікових карток визначає правила та процедури, які регулюють створення, використання та управління обліковими записами користувачів. Вона включає в себе такі аспекти, як встановлення вимог щодо

складності паролів, періодична зміна паролів, обмеження прав доступу та інші важливі аспекти безпеки. Важливим елементом політики облікових карток є вимога до користувачів стосовно захисту своїх паролів та облікових даних. Користувачам рекомендується не ділитися своїм паролем з іншими особами, не використовувати один і той же пароль для різних облікових записів та зберігати паролі у безпечному місці. Політика облікових карток також передбачає процедури створення та видалення облікових записів, а також управління правами доступу. Це включає в себе ретельну перевірку ідентичності користувача під час створення облікового запису, а також регулярне оновлення прав доступу на основі зміни ролі чи обов'язків користувача. Для успішної реалізації політики облікових карток важливо забезпечити належне навчання та обізнаність персоналу. Працівники повинні бути ознайомлені з правилами та процедурами щодо управління обліковими записами, а також знати рекомендації щодо створення та захисту паролів.

Загалом, установка пароля та розробка політики облікових карток є ключовими аспектами стратегії адміністрування та керування безпекою. Вони допомагають забезпечити надійний захист інформаційних ресурсів та зменшити ризик несанкціонованого доступу до даних.

## Схожість

Джерела з Бібліотеки

151

1	Студентська робота	ID файлу: 6004273	Навчальний заклад: National University of Water Management	3 Джерело	10.6%
2	Студентська робота	ID файлу: 1016110143	Навчальний заклад: National University of Life and Environm	6 Джерело	5.81%
3	Студентська робота	ID файлу: 1006774530	Навчальний заклад: National Aviation University		5.19%
4	Студентська робота	ID файлу: 1015727131	Навчальний заклад: Poltava National Technical Yuri Kond	2 Джерело	4.25%
5	Студентська робота	ID файлу: 1010164355	Навчальний заклад: Kharkiv National Air Force University	3 Джерело	4.17%
6	Студентська робота	ID файлу: 8288965	Навчальний заклад: Ternopil Volodymyr Hnatiuk National Pe	3 Джерело	3.89%
7	Студентська робота	ID файлу: 12277055	Навчальний заклад: National University Ostroh Academy	3 Джерело	3.52%
8	Студентська робота	ID файлу: 1008423586	Навчальний заклад: National University of Water Management an...		2.91%
9	External file	ID файлу: EF-100000068219	Навчальний заклад: Lviv Polytechnic National University	7 Джерело	2.3%
10	Студентська робота	ID файлу: 5975562	Навчальний заклад: National Technical University of Ukraine "Kyiv Po...		2.04%
11	Студентська робота	ID файлу: 2044020	Навчальний заклад: Lviv Polytechnic National University	3 Джерело	1.59%
12	Студентська робота	ID файлу: 1008320634	Навчальний заклад: National Aviation University	4 Джерело	1.52%
13	Студентська робота	ID файлу: 1016178921	Навчальний заклад: National University of Water Management an...		1.51%
14	Студентська робота	ID файлу: 1005799224	Навчальний заклад: National University of Water Manag	15 Джерело	1.46%
15	Студентська робота	ID файлу: 1003100842	Навчальний заклад: Cherkasy State Technological University		1.29%
16	Студентська робота	ID файлу: 1015050608	Навчальний заклад: Lutsk National Technical University		1.2%
17	Студентська робота	ID файлу: 1013801115	Навчальний заклад: National Aviation University		1.18%
18	Студентська робота	ID файлу: 1000578356	Навчальний заклад: National University of Life and Environm	5 Джерело	1.09%
19	Студентська робота	ID файлу: 1004021180	Навчальний заклад: Cherkasy State Technological University		1.01%
20	Студентська робота	ID файлу: 1015727677	Навчальний заклад: National Aviation University	22 Джерело	0.96%

21	External file	ID файлу: EF-10000068221	Навчальний заклад: Lviv Polytechnic National University	2 Джерело	0.78%
22	Студентська робота	ID файлу: 1005736576	Навчальний заклад: National Aviation University		0.56%
23	External file	ID файлу: EF-100000054298	Навчальний заклад: Lviv Polytechnic National University	4 Джерело	0.42%
24	Студентська робота	ID файлу: 1008433307	Навчальний заклад: National Technical University of Ukraine "Kyiv..."		0.39%
25	Студентська робота	ID файлу: 1004060170	Навчальний заклад: National Aviation University	2 Джерело	0.34%
26	Студентська робота	ID файлу: 1016143138	Навчальний заклад: National University of Water Management an...		0.32%
27	Студентська робота	ID файлу: 6686134	Навчальний заклад: National Technical University of Ukraine "Kyiv Po..."		0.29%
28	Студентська робота	ID файлу: 1003784885	Навчальний заклад: National University of Life and Environmenta...		0.27%
29	Студентська робота	ID файлу: 2061389	Навчальний заклад: National University of Water Managemen...	5 Джерело	0.26%
30	Студентська робота	ID файлу: 1008058446	Навчальний заклад: Donetsk National Technical Universit...	3 Джерело	0.23%
31	Студентська робота	ID файлу: 1016160124	Навчальний заклад: Lviv Polytechnic National University	4 Джерело	0.21%
32	Студентська робота	ID файлу: 1015240268	Навчальний заклад: Lviv Polytechnic National University		0.21%
33	Студентська робота	ID файлу: 1003955831	Навчальний заклад: National Aviation University		0.17%
34	Студентська робота	ID файлу: 1015290461	Навчальний заклад: Taras Shevchenko National University of Kyiv		0.15%
35	Студентська робота	ID файлу: 1015636915	Навчальний заклад: National University Ostroh Academy	9 Джерело	0.13%
36	Студентська робота	ID файлу: 2077803	Навчальний заклад: National University of Water Managemen...	2 Джерело	0.13%
37	Студентська робота	ID файлу: 1016183533	Навчальний заклад: Yuriy Fedkovych Chernivtsi National	2 Джерело	0.13%
38	Студентська робота	ID файлу: 1016173866	Навчальний заклад: National Aviation University	2 Джерело	0.13%
39	Студентська робота	ID файлу: 1016109733	Навчальний заклад: Lviv Polytechnic National University		0.12%
40	Студентська робота	ID файлу: 1015759249	Навчальний заклад: National Technical University of Ukra...	4 Джерело	0.11%
41	Студентська робота	ID файлу: 1015338603	Навчальний заклад: National University of Water Managemen...	4 Джерело	0.11%
42	Студентська робота	ID файлу: 1016148501	Навчальний заклад: Lviv Polytechnic National University		0.11%

43	Студентська робота	ID файлу: 1015701661	Навчальний заклад: V.I. Vernadsky Taurida National University	0.11%
44	Студентська робота	ID файлу: 1009725562	Навчальний заклад: Lviv Polytechnic National University	0.1%
45	Студентська робота	ID файлу: 1014402603	Навчальний заклад: State University Kyiv National Econo <a href="#">4 Джерело</a>	0.1%
46	Студентська робота	ID файлу: 1015310552	Навчальний заклад: National Aviation University	0.1%
47	Студентська робота	ID файлу: 1015649542	Навчальний заклад: Lviv Polytechnic National University	0.1%
48	External file	ID файлу: EF-100000058855	Навчальний заклад: Lviv Polytechnic National University <a href="#">2 Джерело</a>	0.1%
49	Студентська робота	ID файлу: 1016133105	Навчальний заклад: Lviv Polytechnic National University	0.1%
50	Студентська робота	ID файлу: 6050750	Навчальний заклад: Lviv Polytechnic National University	0.1%
51	Студентська робота	ID файлу: 1007995541	Навчальний заклад: Donetsk National Technical University	0.1%
52	Студентська робота	ID файлу: 1016134054	Навчальний заклад: National Technical University of Ukraine "Kyj...	0.1%