МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК ТА ІНЖЕНЕРІЇ

До захисту допускається
Завідувач кафедри
_____ Скарга-Бандурова І.С.
«____»_____ 20__ р.

ДИПЛОМНИЙ ПРОЕКТ (РОБОТА) БАКАЛАВРА

ПОЯСНЮВАЛЬНА ЗАПИСКА

НА ТЕМУ:

Мережа офісів аптек ПП "Віталь". Розробка корпоративної мережі на базі VPN

Освітньо-кваліфікаційний рівень "бакалавр"
Спеціальність 123 – "комп'ютерна інженерія"

Керівник проекту:	_____ (підпис)	Л.В. Барбарук (ініціали, прізвище)
Консультант з охорони праці:	_____ (підпис)	Я.О. Критська (ініціали, прізвище)
Студент:	_____ (підпис)	В.О. Даниленко (ініціали, прізвище)
Група:		КІ-15бд

Сєвєродонецьк 2019

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Факультет Інформаційних технологій та електроніки
Кафедра Комп'ютерних наук та інженерії
Освітньо-кваліфікаційний рівень бакалавр
Напрям підготовки _____
(шифр і назва)
Спеціальність 123 – "комп'ютерна інженерія"
(шифр і назва)

ЗАТВЕРДЖУЮ:

Завідувач кафедри _____
_____ І.С. Скарга-Бандурова
«_____» _____20____р.

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) БАКАЛАВРА

Даниленку Владиславу Олександровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Мережа офісів аптек ПП "Вітал". Розробка корпоративної на базі VPN

керівник проекту (роботи) Барбарук Л.В., ст.викладач
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від "15 " 05 2019 р. № ____
2. Термін подання студентом роботи 15.06.2019
3. Вихідні дані до роботи Розташування комп'ютерів в офісі та апаратне забезпечення комп'ютерної мережі

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Аналіз систем технічної підтримки та формулювання технічного завдання; проектування мережі на базі VPN;охорона праці та безпека надзвичайних ситуаціях.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) Електронні плакати

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці та безпека в надзвичайних ситуаціях	ст. викл. Критська Я.О.		

7. Дата видачі завдання 15.05.2019

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Ознайомлення з предметною галуззю	03.05 – 15.05	
2	Аналіз задачі та постановка проблеми	16.05 – 18.05	
3	Розгляд існуючих рішень щодо вирішення	19.05 – 25.05	
	задачі		
4	Вибір методу побудови мережі	26.05 – 03.06	
5	Розробка програмного коду і тестування	04.06 – 10.06	
6	Розробка розділу «Охорона праці та	04.06 – 08.06	
	безпека в надзвичайних ситуаціях»		
7	Оформлення пояснювальної записки	09.06 – 11.06	

Студент _____ _____
(підпис) (прізвище та ініціали)

Керівник _____ _____
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка до дипломного проекту бакалавра. Об’єкт розробки: корпоративна комп’ютерна мережа офісів аптек ПП “Вітал”.

Мета роботи: вибір технології, топології ,мережевого обладнання та методу побудови корпоративної комп’ютерної мережі.

В проекті виконано:

1) аналіз мережі офісів та структура досліджуваного об'єкта;

2) розробка технічних вимог до корпоративної комп’ютерної мережі (ККМ) офісів ПП “Вітал”;

3) опис побудови ККМ, огляд мережевого обладнання;

4) організація ККМ на основі імітаційного моделювання NetCracker Professional;

5) проектування ЛКМ кожного офісу;

6) розробка корпоративної мережі на базі VPN;

7) розробка заходів з техніки безпеки;

Отримано наступні результати.

Спроектована ККМ, яка забезпечує спільний доступ користувачів до баз даних усіх офісів та роботу з пакетами комунікаційних програм.

Практичне значення, галузь застосування роботи: Розробка корпоративної мережі на базі VPN для мережі офісів аптек ПП “Вітал”.

Робота містить 87 сторінок , 31 рисунок, 3 додатки, 18 джерел.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ЛКМ – локальна комп'ютерна мережа;

ПК – персональний комп'ютер;

ПЗ – програмне забезпечення;

БД – база даних;

СКМ – структуровані кабельні мережі;

VPN (Virtual Private Network) – віртуальна приватна мережа;

ETHERNET – топологія мережі;

LAN (Local Area Network) – локальна мережа;

MAN (Metropolitan area network) – кампусна мережа;

WAN (Wide Area Network) – широкомасштабна мережа;

EIA (Electronic Industries Allience) – альянс галузей електронної промисловості;

OSI (Open systems interconnection) – мережева модель;

UTP (Unshielded twisted pair) – неекранована кручена пара;

STP (Unshielded twisted pair) – екранована кручена пара;

ВСТУП

Будь-яка організація - це сукупність взаємодіючих структурних елементів (підрозділів), кожен з яких може мати свою особливість. Елементи пов'язані між собою функціонально, тобто вони виконують окремі види робіт у рамках єдиного бізнес проекту, а також за допомогою інформації, обмінюючись документами, , письмовими повідомленнями і усними розпорядженнями і так далі. Крім того, ці елементи взаємодіють із зовнішніми системами, і їх взаємодія також може бути інформативною, а також функціональною.

Зі зростанням і розвитком організації в її керівництві неминуче виникає потреба створити найбільш гнучку і ефективну систему управління існуючими підрозділами, забезпечити якісну і надійну комунікацію між центральним офісом і всіма підрозділами, забезпечити конфіденційність передачі інформації, зменшити витрати на телекомунікації, витрачати менше часу на збір доповідей і ефективно обробляти потоки інформації, що циркулюють між підрозділами.

Корпоративні комп'ютерні мережі є невід'ємною частиною сучасних компаній. За допомогою таких мереж можна оперативно і безпечно передавати і отримувати інформацію. Вони забезпечують зв'язок між комп'ютерами одного підприємства, розташованими в межах однієї будівлі або географічно розподіленими. Існує кілька способів побудови подібних мереж. До недавнього часу найбільшою популярністю користувалися системи Local Area Network (LAN), які об'єднують обмежену кількість ПК. Вони забезпечують максимальну швидкість обміну файлами і абсолютну безпеку інформації, так як її потоки не потрапляють в загальний доступ. Використання структур цього типу є безкоштовним. До мінусів LAN можна віднести високу вартість і неможливість підключення віддалених користувачів. Альтернативою стали віртуальні мережі - Virtual Private Network (VPN), які будуються поверх глобальних мереж WAN (Wide Area Network), що охоплюють велику кількість ПК і комп'ютерних систем по всій планеті. До їх безперечних достоїнств відносяться простота (а відповідно, і невисока вартість) побудови, можливість підключення безлічі

абонентів, що знаходяться в різних кінцях світу, і безпеку передачі даних. VPN активно витісняють LAN з ринку. Так, за результатами досліджень, проведених Forrester Research Inc. і Infonetics Research, витрати на використання та обслуговування VPN майже в три рази нижче, ніж логістичних структур, побудованих за технологією LAN.

Створити мережу, яка буде повністю відповідати потребам підприємства, можуть тільки професіонали, тому перше, що потрібно зробити потенційному замовнику, - вибрати надійного провайдера і підготувати технічне завдання. У більшості випадків провайдери поставляють своїм клієнтам все необхідне обладнання на термін дії договору надання послуг. Але за бажанням замовник може придбати техніку самостійно. У такому випадку йому знадобиться стандартне мережеве обладнання, а також спеціальний шлюз Virtual Private Network Gateway. Цей шлюз потрібен для формування тунелів, захисту даних, контролю трафіку, а в певних випадках - і централізованого управління. Найбільш відомими виробниками таких шлюзів є корпорації Assured Digital, Cisco, Intel, Avaya, Red Creek Communications, Net Screen Technologies, 3com, Nokia, Intrusion, Watch Guard Technologies, Sonic Wall, eSoft і ін. Вартість шлюзу для малих офісів в середньому становить 700 -2500 доларів.

Мережа в офісі - це просте і зручне рішення як для фірм з великою кількістю офісів і віддалених користувачів, так і для компаній, що бажають мати недорогу, легку в управлінні і гнучку систему. Ця технологія дозволяє додавати нові структурні елементи, а також істотно збільшувати розміри мереж без серйозного розширення інфраструктури. Робити це може сам замовник без залучення провайдера до вирішення цих завдань. Додавання нового абонента займе всього кілька хвилин. Управління такими системами не становить труднощів для користувача, так як більша частина функцій адміністратора в Virtual Private Network автоматизована. Фахівці провайдера інсталюють на сервері клієнтської фірми необхідне ПО, а також створюють базу суб'єктів і об'єктів VPN (для кожного суб'єкта генерується ключ шифрування). Потім ця база зберігається на знімному носії та передається замовнику. Користувачеві

необхідно буде тільки підключати ключ-карту до комп'ютера для ідентифікації та отримання доступу. Якщо в процесі роботи захищеної корпоративної мережі виникають будь-які неполадки, то замовнику слід звернутися до провайдера, і він вирішить ці проблеми в термін, обумовлений умовами контракту. Таким чином, VPN - це рішення, актуальне для середніх і великих компаній, що мають в своєму штаті фахівців, які працюють віддалено, а також відділення в інших містах і країнах. Крім того, подібні системи просто незамінні для організацій, у яких: часто змінюється коло осіб і структурних підрозділів, які потребують доступ до конфіденційних даних (відповідно, необхідно, щоб структура була досить гнучкою і легко налаштовувалася); є абоненти, яким потрібно надати доступ до даних різного рівня (співробітники, клієнти, постачальники); є необхідність у створенні декількох логічних мереж в рамках однієї фізичної структури (наприклад, якщо потрібно створити власну систему для кожного підрозділу підприємства).

Звичайно, КМ має свої проблеми, але головним доказом ефективності є незаперечний факт їх поширення. Все більше і більше з'являється великих мереж з сотнями робочих станцій і десятками серверів.

.

1 АНАЛІЗ ТЕХНІЧНОГО ЗАВДАННЯ

1.1 Огляд предметної області

VPN (віртуальна приватна мережа) - це локальна мережа, створена в інших мережах на основі публічних або довірчих каналів інших мереж (Інтернет). Безпека передачі пакетів через публічні мережі може бути досягнута за допомогою шифрування, що створює канали обміну інформацією закритого типу. VPN дозволяє об'єднати, наприклад, кілька географічно віддалених організацій в єдину мережу, використовуючи неконтрольовані канали для зв'язку між ними.

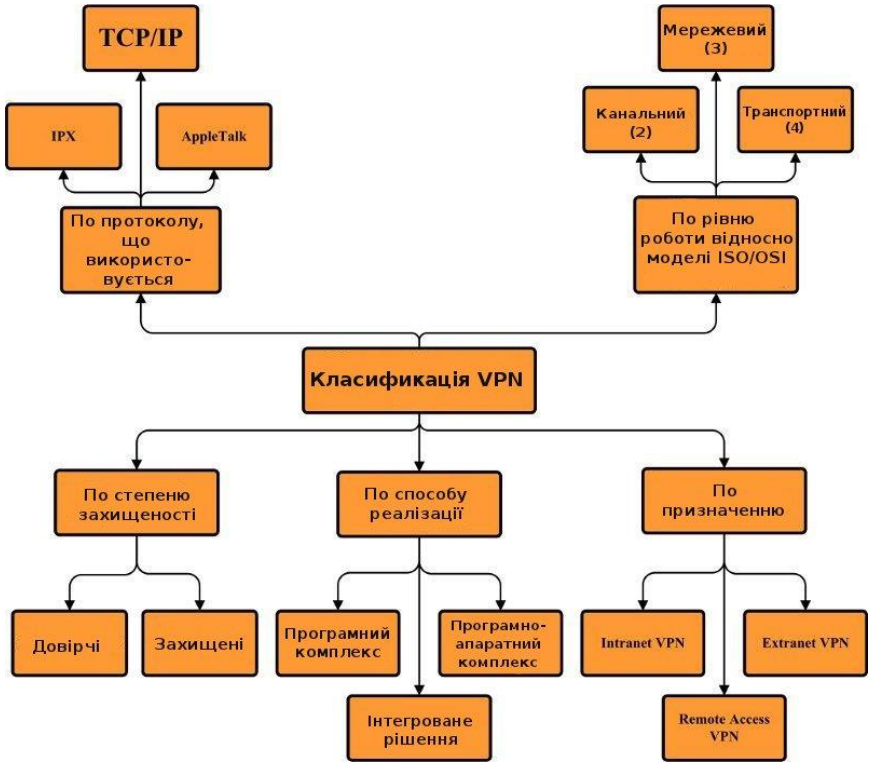


Рисунок 1.1 - Класифікація VPN за типом використовуваного середовища

VPN складається з двох частин: «внутрішньої» (контрольованої) мережі, яка може бути декількома, і «зовнішньої» мережі, через яку проходять інкапсульовані з'єднання (зазвичай використовується Інтернет).

Підключення до VPN віддаленого користувача здійснюється за допомогою сервера доступу, який з'єднаний як з внутрішньою, так і з зовнішньою (загальнодоступною) мережею. При підключенні віддаленого користувача (або при підключенні до іншої захищеної мережі) сервер доступу вимагає продовження процесу ідентифікації, а потім процесу аутентифікації. Після успішного проходження обох процесів віддалений користувач (віддалена мережа) має право працювати в мережі, тобто процес авторизації завершено.

VPN класифікуються за типом використовуваного середовища.

Захищені - найбільш часто використовувана віртуальна приватна мережа. З його допомогою можна створити надійну і безпечну підмережу, засновану на ненадійній мережі, зазвичай Інтернету. Прикладом захищених протоколів VPN є Ipsec, SSL і PPTP. Прикладом використання SSL є програмне забезпечення OpenVPN.

Довірчі - використовується в тих випадках, коли середовище, до якого передаються дані, може вважатися надійним і необхідно вирішувати тільки завдання створення віртуальної підмережі в межах більшої мережі. Питання безпеки стають нерелевантними. Прикладами подібних рішень VPN є: Multi-protocol label switching (MPLS) і L2tp (Layer 2 Tunneling Protocol).

Захист інформації при розумінні VPN включає в себе шифрування, аутентифікацію і контроль доступу. Кодування означає шифрування, що передається через інформацію VPN. Читати всі отримані дані може тільки власник ключа до шифру. Найбільш часто використовуваними в VPN рішеннями алгоритмами кодування в наш час є DES, Triple DES і різні реалізації AES. Аутентифікація включає в себе перевірку цілісності даних та ідентифікацію фізичних та юридичних осіб, що беруть участь у VPN. Перша гарантує, що дані потраплять до адресата саме в тому вигляді, в якому вони були відправлені. Найбільш популярними алгоритмами перевірки цілісності даних на сьогодні є MD5 і SHA1.

Як правило, VPN формуються на рівнях над мережею, оскільки використання криптографії на цих рівнях дозволяє використовувати незмінні транспортні протоколи (такі як TCP, UDP).

Технологія VPN нещодавно використовувалася не тільки для створення приватних мереж, а й для деяких постачальників на пострадянському просторі для забезпечення доступу до Інтернету.

Завдяки належному рівню реалізації та використанню спеціального програмного забезпечення, мережа VPN може забезпечити високий рівень шифрування переданої інформації. Завдяки правильному вибору всіх компонентів, технологія VPN забезпечує анонімність у мережі.

Зазвичай, коли створюється VPN, використовується зв'язок "точка-точка" з певним сервером або встановлюйте тунель Ethernet з певним сервером, який призначає тунель певній підмережі. Таким чином, сервер VPN виконує функції маршрутизації та фільтрації трафіку для доступу до локальної мережі через VPN.

Використовуючи цей підхід, все ще є можливість фільтрувати трафік на основі методу підключення (наприклад, використовувати різні фільтри для локальної мережі і для віддалених користувачів), але необхідність налаштування маршрутизації вимкнена, а віддалені машини включені безпосередньо до локальної мережі, навіть здатні використовувати широкосмугові посилки взагалі без будь-яких додаткових налаштувань.

VPN включають:

– IPSec (IP-безпека) - часто використовується через IPv4;

– (PPTP (протокол тунелювання між точками) - розроблений спільно кількома компаніями, включаючи Microsoft;

– P PPPoE (протокол точка-точка) через Ethernet (PPP);

– TP L2TP (протокол туннелювання 2-го рівня) - використовується в продуктах від Microsoft і Cisco;

– TP L2TPv3 (протокол 2 тунелювання версії 3);

– OpenVPN - це SSL VPN з відкритим вихідним кодом, який підтримує PPP, bridge, point-to-point,

Корпоративна мережа та методи побудови корпоративних мереж.

Корпоративна мережа - це мережа, головним призначенням якої є забезпечення функціонування конкретного підприємства, що володіє цією мережею. Користувачами корпоративної мережі є тільки співробітники даного підприємства. На відміну від мереж операторів зв'язку, корпоративні мережі, в загальному випадку, не роблять послуг іншим організаціям або користувачам.

Корпоративна мережа підприємства характеризується двома елементами. ЛОМ - локальна обчислювальна мережа, що забезпечує стабільний обмін необхідними даними і управління правами доступу користувачів. Для її створення необхідно апаратне забезпечення - структуровані кабельні мережі, далі СКМ, являє собою телекомунікаційну інфраструктуру - сукупність всіх комп'ютерних пристроїв компанії, між якими відбувається обмін даними в режимі реального часу.

Створення корпоративної мережі складається з вибору:

– робочої групи;

– середовища моделювання;

– програмних і апаратних рішень для її створення;

– налагодження і супровід готової архітектури.

Побудова архітектури і вибір технології корпоративної мережі складається з кількох етапів:

– вибір елементарних об'єктів, що входять в корпоративну мережу обміну даними. Як правило, це певні продукти, послуги компанії і інформація по ним;

– вибір функціональних, інформаційних і ресурсних моделей для майбутньої мережі. На цьому етапі визначається «внутрішня логіка» функціонування майбутньої мережі;

– далі, на основі вже обраних параметрів визначаються мови і методи моделювання, здатні вирішити поставлені завдання.

Наприклад, при формуванні корпоративної мережі невеликої виробничої компанії застосовуються найбільш доступні, невимогливі до апаратних потужностей мови моделювання. І навпаки, створення архітектури для великих компаній з широким профілем діяльності передбачає використання потужних інструментів.

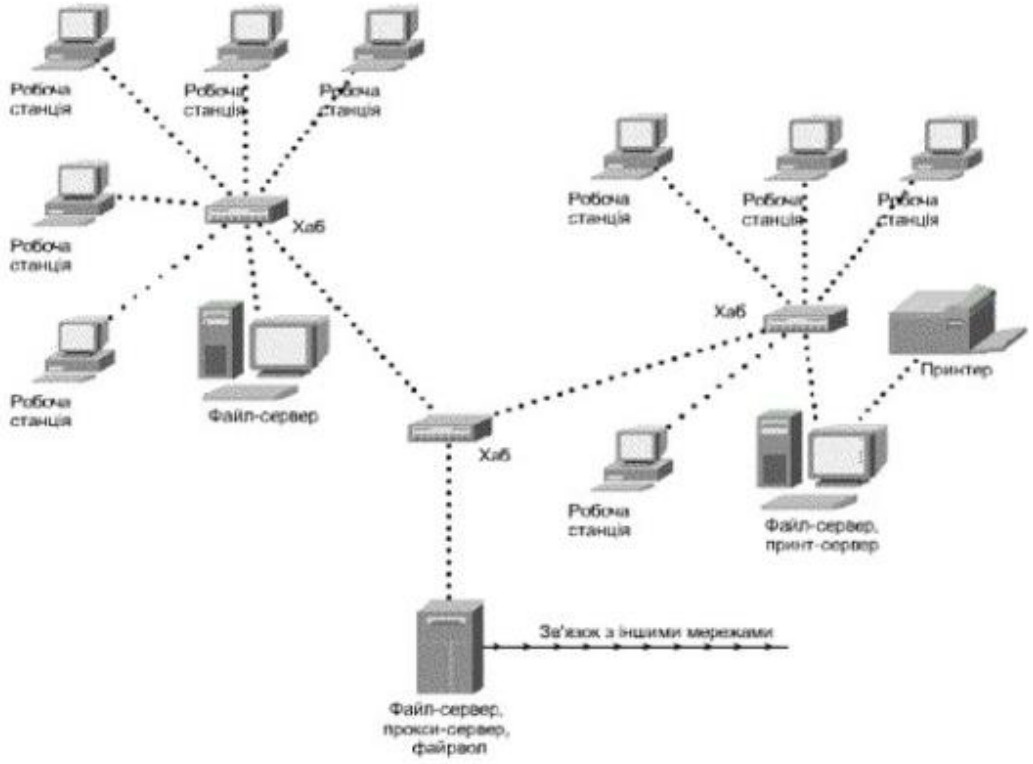


Рисунок 1.2 - Приклад корпоративної мережі

Найпоширеніші методи організації корпоративних мереж.

Перший варіант - компанія сама створює лінії зв'язку між структурами. Якщо офіси і філіали компанії розкидані по країні або місту, то буде потрібно вирішувати завдання пов'язані з прокладанням кабелю або будівництвом мережі радіозв'язку. У першому випадку вас чекають проблеми землевідведення, оренди кабельної каналізації, геодезичних вишукувань траси, копки траншей або закладки кабелю в існуючу каналізацію. І все це не рахуючи вартість самого кабелю і використовуваного обладнання підтримки: повторювачів, термінаторів і т.п. У другому - проблеми будівництва веж (і,

знову-таки, землевідведення) або оренди місць на дахах високих будівель, підбору та погодження частот і щорічна плата за використання частотного ресурсу, узгодження місць установки антен з самими різними організаціями - від санепіднагляду до ППО. Орієнтовна вартість такого проекту буде порядку декількох мільйонів гривень. Однак такий метод побудови дозволить досягти найвищої швидкості передачі даних по мережі з доступних.

Другий варіант - компанія орендує виділений канал зв'язку у провайдера. Рішення, засноване на оренді каналів, трохи відрізняється від рішення з виділеними лініями зв'язку. Основною відмінністю накладених мереж є те, що орендар отримує в своє розпорядження не певний канал, а ресурс мережі з гарантованою пропускною здатністю.

Орендуючи канал у провайдера, ми економимо гроші компанії, адже вартість орендованих ресурсів мережі помітно нижче вартості виділених ліній зв'язку. Крім того, ми отримуємо можливість створити мережу з інтеграцією послуг передачі даних.

Третій варіант - компанія купує виділену лінію зв'язку у провайдера. Корпоративні мережі зв'язку, побудовані на основі виділених ліній зв'язку, дозволяють організувати віддалений доступ до баз даних, побудувати корпоративну поштову систему і корпоративну телефонну мережу. Для них характерні висока якість послуг, проте, їх організація - справа недешева в основному за рахунок високої вартості виділених ліній зв'язку, хоча такий варіант в рази менш витратний, ніж варіант з прокладанням кабелю своїми силами.

Четвертий варіант - віртуальне з'єднання. Технологія віртуальних мереж передбачає побудову корпоративної мережі зв'язку поверх мережі Інтернет або будь-який інший мережі загального користування. При цьому для захисту переданих даних від несанкціонованого доступу здійснюється їх шифрування з використанням спеціальних протоколів.

1.2 Формулювання завдання роботи

Метою даного дипломного проекту є розробка корпоративної обчислювальної мережі для аптек ПП «Віталь».

В межах даного проекту буде об’єднано головний офіс ПП (вул..Менделєєва, 22а), офіс 1 (вул..Володимирська, 32) та офіс 2 (вул.. Менделєєва, 40).

Розташування серверів та робочих станцій наведено в таблиці 1.1.

Таблиця 1.1 - Розташування комп’ютерної техніки

Адреса магазину	Назва відділу	Кількість робочих станцій (серверів)	Кабінет
Головний офіс вул. Менделєєва, 22а	Приймальний кабінет	1	1
	Торгівельна зала	2	2
	Бухгалтерія	3	3
	Склад/ Серверна	3	4
Офіс 1 вул. Володимирська, 32	Торгівельна зала	2	1
	Склад	3	2
Офіс 2 вул.. Менделєєва, 40	Склад	2	1
	Торгівельна зала	2	2

Для вирішення поставленої мети в дипломному проекті вирішуються наступні завдання:

– вибір мережної архітектури для комп'ютерної мережі, топології, типу кабельної системи;

– вибір способу об’єднання сегментів корпоративної мережі;

– вибір способу управління мережею;

– конфігурація мережного устаткування - кількість серверів, комутаторів;

– управління мережними ресурсами і користувачами мережі;

– розгляд питань безпеки мережі;

– перевірка працездатності проекту мережі;

– розрахунок витрат на створення корпоративної мережі.

Необхідно розробити раціональну, гнучку структурну схему мережі, яка б була легкою в обслуговуванні та у пошуку несправностей, передбачити режими швидкого оновлення оперативної інформації на сервері, а так само пропрацювати питання забезпечення необхідного рівня захисту даних офісів торгівельного підприємства; передбачити можливість підключення робочих станцій корпоративної мережі до Internet.

1.2.1 Вимоги до функціональних характеристик

Необхідно забезпечити наступні вимоги:

– забезпечити електронний обмін інформацією між офісами корпоративної мережі;

– забезпечити конфіденційність передачі інформації;

– швидкість обміру інформацією не повинна опускатися нижче 2 Мбіт/с;

– забезпечити високу надійність системи.

1.2.2 Вимоги до програмного забезпечення

Організація VPN каналів між офісами буде виконана на основі програмного продукту OpenVPN.

У проекті мається на увазі, що OPENVPN встановлюватиметься на платформах Windows 10 та Windows Server 2008.

Висновок

У розділі було проведено аналіз технічного завдання (розглянуто предметну область та методи побудови корпоративних мереж.). Крім того було сформовано призначення системи та вимоги до її роботи.

2 АНАЛІЗ ТА ВИБІР ОРГАНІЗАЦІЇ РЕСУРСІВ МЕРЕЖІ

2.1 Структури комп’ютерної мережі

Існує дві моделі локальних обчислювальних мереж:

– однорангова локальна обчислювальна мережа;

– локальна обчислювальна мережа типу клієнт-сервер.

Дані моделі визначають взаємодію комп'ютерів в локальній обчислювальній мережі.

Однорангова мережа представлена на рисунку 2.1.

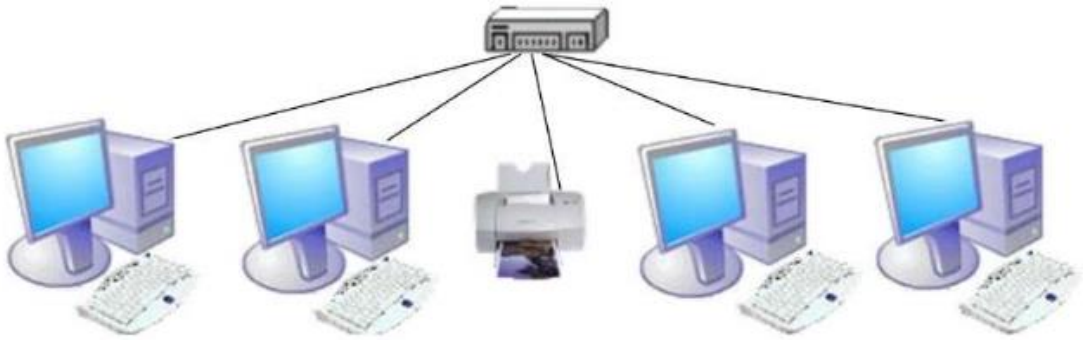


Рисунок 2.1 - Однорангова локальна мережа

У одноранговій локальній мережі всі комп'ютери є рівноправними, тобто в локальній мережі немає жодної ієрархії і немає, так само, якогось головного комп'ютера, який заправляє всіма процесами. У одноранговій локальної мережі кожен комп'ютер одночасно поєднує в собі функції, як клієнта, так і сервера.

Кожен користувач комп'ютера сам визначає, які дані будуть доступні для загального мережевого доступу. Однорангові локальні мережі називають робочими групами, в які входять до 12-ти комп'ютерів. Основні моменти, які характерні всім одноранговим локальним мережам:

– з'єднання всіх комп'ютерів дуже просте

– користувачі є так само і адміністраторами

– всі комп'ютери розташовані в одному приміщенні

Положення, які необхідно враховувати при створенні тимчасової локальної мережі:

– немає централізованої системи контролю. Дуже незручно управлятися зі справами, коли немає начальника, який буде контролювати весь процес;

– користувач має можливість керувати мережею. Тобто для загальнодоступних даних користувач сам повинен встановлювати різні захисні паролі, що б не сталося витоку інформації.

– кожен комп'ютер витрачає велику кількість ресурсів при виконанні робочих операцій. Більшість системних ресурсів спрямовані на обчислювальну потужність, при цьому для різних мережевих операцій виділена мала частина ресурсів комп'ютера. Відзначимо, що однорангові локальні мережі є дуже простими у створенні. Тобто досить з'єднати всі персональні комп'ютери проводами - і можна насолоджуватися готовою мережею.

На кожен комп'ютер в мережі доводиться велике обчислювальне навантаження, тобто при центральному комп'ютері все обчислення виконуються саме на ньому. А в нашому випадку кожен комп'ютер повинен мати достатню обчислювальну потужність, тобто витрати на покупку персональних комп'ютерів (ПК) в рази перевищують ці ж витрати в мережах на основі сервера.

Технологія «Клієнт - сервер» - це архітектура програмного комплексу, в якій відбувається розподіл прикладної програми за двома логічно різними компонентами (клієнт і сервер), які взаємодіють за схемою «запит-відповідь» і вирішаючих свої певні завдання

Комп'ютер (або програма), керуючий / або володіє будь-яким ресурсом, називають сервером цього ресурсу.

Комп'ютер (або програма), який запитує або користується будь-яким ресурсом, називають клієнтом цього ресурсу.

Клієнт і сервер можуть перебувати як на одному комп'ютері (ПК), так і на різних ПК в мережі. Також може виникати така ситуація, коли деякий

програмний блок буде одночасно виконувати функції сервера по відношенню до одного блоку і клієнта по відношенню до іншого.

Основний принцип технології «Клієнт-сервер» полягає в поділі функцій додатка як мінімум на три групи:

– модулі інтерфейсу з користувачем.Також цю групу називають логікою представлення. Через цю групу користувачі взаємодіють з додатком.

– модулі зберігання даних. Цю групу також називають бізнес-логікою. Бізнес-логіка визначає, для чого конкретно призначено додаток (наприклад, прикладні функції, характерні для даної предметної області). Поділ додатків по межах між програмами забезпечує природну основу для розподілу програми на декількох комп'ютерах.

– модулі обробки даних (функції управління ресурсами). Цю групу також називають логікою доступу до даних або алгоритмами доступу до даних. Алгоритми доступу до даних історично розглядалися як специфічний для конкретного додатка інтерфейс до механізму постійного зберігання даних на зразок файлової системи або СУБД. За допомогою модулів обробки даних організовується специфічний для додатка інтерфейс до СУБД. За допомогою інтерфейсу додаток управляє базою даних і запитами до неї.

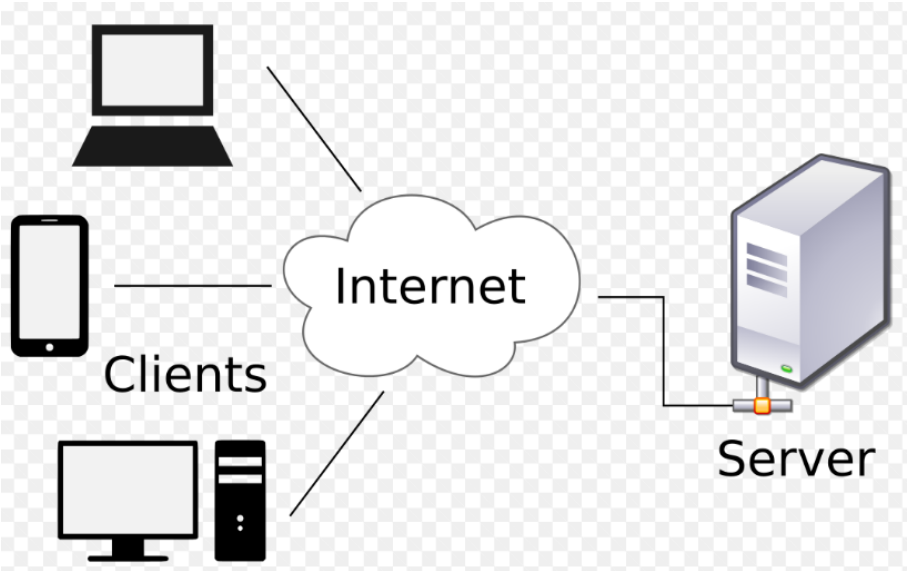


Рисунок 2.2 - Клієнт-серверна архітектура

Передумови появи клієнт-серверної технології:

– число користувачів більше 10 - 20 осіб;

– висока вартість великих OEM та засобів розробки для них;

– вирішення завдань на рівні підприємства і управління підприємством в цілому;

– можливість роботи з користувачами різних регіонів;

– критичне забезпечення цілісності інформації (банки тощо).

В основі клієнт-серверних технологій є дві ідеї:

– загальні для всіх користувачів дані на одному або декількох серверах;

– багато користувачів (клієнтів) на різних обчислювальних установках спільно (паралельно і одночасно) оброблюють загальні дані.

Тобто системи, засновані на цих технологіях, розподілені лише щодо користувачів, тому часто їх вважають видом багатокористувацьких систем.

2.2 Топології локальної комп’ютерної мережі

Топологія мережі - це спосіб опису конфігурації мережі, схема розташування і з'єднання мережних пристроїв. Топологія мережі дозволяє побачити всю її структуру, мережні пристрої, що входять в мережу, і їх зв'язок між собою.

Виділяють кілька видів топологій: фізичну, логічну, інформаційну та топологію управління обміном. До базових топологій належать: шина, зірка, кільце.

Мережі з шинною топологією

Шинна топологія (рисунок 2.3) - найпростіша форма топології, яка являє собою один основний кабель (коаксіальний), обмежений з обох сторін спеціальними роз'ємами - термінаторами, які запобігають появі відбиття сигналів. Недоліки та переваги наведені у таблиці 2.1.

Таблиця 2.1 - Переваги та недоліки топології шина

Переваги	Недоліки
1. Відмова кожної зі робочих станцій не впливає на роботу всієї мережі. 2. Простота і гнучкість з'єднань. 3. Недорогий кабель і роз'єми. 4. Необхідно невелика кількість кабелю. 5. Прокладка кабелю не викликає особливих складнощів.	1. Розрив кабелю, або інші неполадки в з'єднанні може припинити нормальну роботу всієї мережі. 2. Обмежена довжина кабелю і кількість робочих станцій. 3. Важко знайти дефекти з'єднань. 4. Невисока продуктивність. 5. При великому обсязі переданих даних головний кабель може не справлятися с навантаженням.

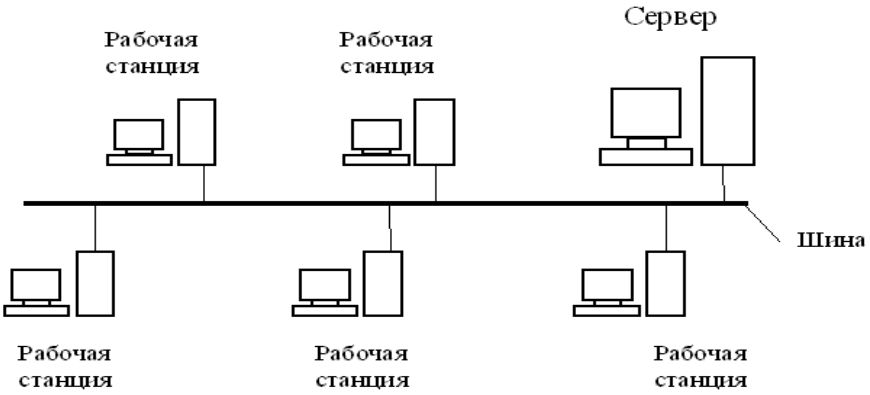


Рисунок 2.3 - Шинна топологія

Мережі з кільцевою топологією

У комп'ютерній мережі з топологією «кільце» (рисунок 2.4) комп'ютери підключаються до кабелю, замкнутого в коло. Тому у кабелі просто не може бути вільного кінця, на який треба поставити термінатор. Сигнали передаються по кільцю в одному напрямі і проходять через кожен комп'ютер. На відміну від пасивної топології «шина», тут кожен комп'ютер виступає в ролі повторювача, підсилюючи сигнали і передаючи їх наступному комп'ютеру. Тому, якщо вийде з ладу один комп'ютер, припиняє функціонувати вся мережа.

Рисунок 2.4 - Мережа з кільцевою топологією

Кільцева топологія дуже чутлива до обривів кабелю кільця. 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 комутаторів. Правда, збільшується сумарна довжина кільця.

Недоліки мережі з кільцевою топологією:

– відмова одного комп'ютера в мережі може вплинути на працездатність всієї мережі;

– додавання або видалення комп'ютера змушує розривати мережу, усувається завдяки використанню "подвійного" кільця. Для цього до складу локальної мережі включають додаткові лінії зв'язку, пристрої реконфігурації — спеціальні перемикальні пристрої, прості й надійні.

Мережі з топологією “зірка”

«Зірка» (рисунок 2.5) — це єдина топологія мережі з явно виділеним центром, до якого підключаються всі інші абоненти. Обмін інформацією йде винятково через центральний комп'ютер, на який лягає більше навантаження, тому нічим іншим, крім мережі, він, як правило, займатися не може. Зрозуміло, що мережне устаткування центрального абонента повинно бути істотно складнішим, чим устаткування периферійних абонентів. Про рівноправність всіх абонентів (як у шині) у цьому випадку говорити не доводиться. Звичайно центральний комп'ютер найпотужніший, саме на нього покладають всі функції

по керуванню обміном. Ніякі конфлікти в мережі з топологією зірка в принципі неможливі, тому що керування повністю централізоване. . Недоліки та переваги наведені у таблиці 2.

Таблиця 2.2 - Переваги та недоліки топології “зірка”.

Переваги	Недоліки
1. Підключення нових робочих станцій не викликає особливих труднощів. 2. Можливість моніторингу мережі та централізованого управління мережею 3. При використанні централізованого управління мережею локалізація дефектів з'єднань максимально спрощується. 4. Гарна розширюваність і модернізація.	1. Відмова концентратора призводить до відмови у доступі до мережі всіх робочих станцій, підключених до неї. 2. Досить висока вартість реалізації, тому що потрібна велика кількість кабелю.

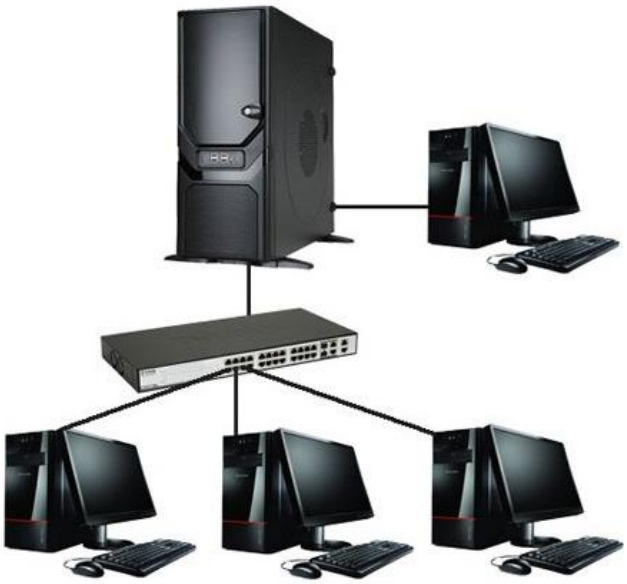


Рисунок 2.5 - Мережа з топологією “зірка”

2.3 Обґрунтування вибору топології мережі

Для організації ЛОМ в офісах ПП «Віталл» будемо застосовувати зіркоподібну топологію. Велика перевага топології «зірка» (як пасивної, так і активної) полягає в тому, що всі точки підключення знаходяться в одному місці. Це дозволяє з легкістю контролювати роботу мережі, виправляти

несправності мережі шляхом простого відключення від центра тих або інших абонентів (що неможливо, наприклад, у випадку «шини»), а також обмежувати доступ сторонніх осіб до життєво важливих для мережі точок підключення.

2.4 Мережеве обладнання для локальних мереж

2.4.1 Мережеві кабелі

Найпростіша вита пара — це два перевитих навколо один одного ізольовані мідні дроти.

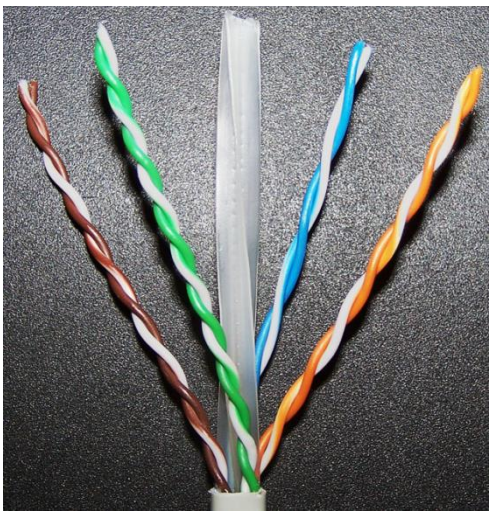


Рисунок 2.6 – Кабель типу «вита пара»

Існує два типи витої пари:

- неекранована (unshielded) вита пара (UTP)
- екранована (shielded) вита пара (STP).

Декілька витих пар проводів часто поміщають в одну захисну оболонку. Їх кількість в такому кабелі може бути різною. Завивка проводів дозволяє позбавитися електричних перешкод, що наводяться сусідньою парою і іншими зовнішніми джерелами, наприклад двигунами, реле і трансформаторами.

Неекранована вита пара (специфікація OBaseT) широко використовується в локальних мережах; максимальна довжина сегменту становить 100 м

(328 футів). Неекранована вита пара складається з двох ізольованих мідних дротів. Існує декілька специфікацій, які регулюють кількість витків на одиницю довжини, — залежно від призначення кабелю.

Кабель екранованої витої пари (STP) має мідне обплетення, яке забезпечує надійніший захист від перешкод. Крім того, пара проводів STP обмотані фольгою. В результаті екранована вита пара чудово захищає передавані дані від зовнішніх перешкод. Все це означає, що STP, в порівнянні з UTP, менше схильна до дії електричних перешкод і може передавати дані з вищою швидкістю і на великі відстані

Для інформаційної індустрії застосовуються різні види кабелів, але на сьогоднішній день найбільшого поширення набули оптоволоконні кабелі. Оптичні технології стали справжнім проривом в телекомунікаційних системах. А оптоволоконний кабель став саме тим засобом, який дозволяє передавати дані з неймовірно високою швидкістю. Будову оптоволоконного кабелю наведено на рисунку 2.2.

Рисунок 2.7 – Оптоволоконний кабель.

Складається такий кабель з зовнішньої оболонки, захисних оболонок, оптоволокон і серцевини. Він являє собою скорочення певним чином оптоволокна, які покриваються захисною оболонкою. Завдяки серцевині відбувається передача сигналів. Незважаючи на те, що зовні такий кабель дуже схожий на електричний, всередині замість мідного дроту розташоване скловолокно. Внутрішня оболонка замінена на пластиковову або скляну оболонку, яка не дає можливості світлу виходити за межі скловолокна.

Таким чином, головний елемент волоконно-оптичного кабелю - це прозоре скловолокно, яке проводить світло на величезні відстані. Як правило, у такого кабелю немає металевої сітки, так як не потрібно екранувати вплив зовнішніх електромагнітних завад. Однак іноді вона потрібна, щоб забезпечити захист кабелю від факторів навколишнього середовища. В цьому випадку цифровий оптичний кабель вважається броньованим і здатний витримувати значні фізичні навантаження.

Якщо порівняти оптичний кабель з мідним, то перший має масу переваг:

– відрізняється простотою монтажу;
– несприйнятливий до перешкод;
– має високу якість передачі інформації;
– простий у використанні;
– має менші розміри і вагу;
– володіє широкою смугою пропускання;
– довговічний;
– має низькі втрати даних;
– має високу швидкість передачі даних;
– несприйнятливий до погодних умов.

Не так давно найпоширенішим типом вважався коаксіальний кабель. Це пояснювалося двома причинами.

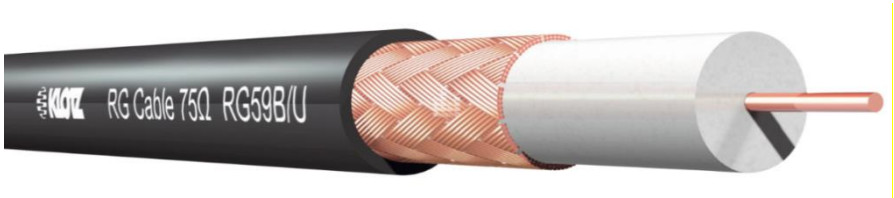


Рисунок 2.8 – Коаксіальній кабель

Коаксіальний кабель - цей різновид кручений пари, але з набагато більшою помехозащищенностью, найбільш підходящий провідник для ВЧ сигналу.

Коаксіальний кабель складається з центральної жили (провідника), екранованого шару (екрана) і двох ізолюючих шарів.

Внутрішній ізолятор служить для ізоляції центральної жили коаксіального кабелю від екрану, зовнішній - для захисту кабелю від механічних пошкоджень і електричної ізоляції.

Існує два типи коаксіальних кабелів: тонкий (thinnet) коаксіальний кабель та товстий (thicknet) коаксіальний кабель. Вибір того або іншого типу кабелю залежить від потреб конкретної мережі.

2.4.2 Мережевий комутатор

Мережевий комутатор, або як його ще називають, свитч (від англійського «switch»), створений з'єднувати ряд вузлів, розміщених в межах однієї або декількох зон (сегментів) комп'ютерної мережі. Його призначення полягає в передачі даних конкретному одержувачу, завдяки чому інші вузли (сегменти), що знаходяться на зв'язку з комутатором, звільняються від необхідності обробки даних, які для них не призначені. Це сприяє підвищенню безпеки і значного збільшення продуктивності мережі. В основі роботи комутаторів лежить технологія мережевого мосту, тому комутатори з повним правом можна назвати багатопортовими мостами.

Рисунок 2.10 – Мережний комутатор

2.4.3 Маршрутизатор

Маршрутизатор - це фізичний мережевий пристрій, який полегшує і встановлює з'єднання між локальною мережею та Інтернетом шляхом передачі інформації в мережі з пакетною комутацією і з них. Він виконує цю функцію за допомогою аналізу заголовка пакета даних, який містить IP-адресу призначення пакета. На основі пакета даних маршрутизатор визначає найбільш ефективний маршрут до адреси призначення.

Рисунок 2.11 – Маршрутизатор

Маршрутизатор підключений до модему і інших пристроїв. Маршрутизатор створює приватну мережу, отримуючи від модему дані з мережі Інтернет, який підключається через кабельне, або інше провідне з'єднання від постачальника інтернет-послуг. Маршрутизатор мають кілька портів, з яких можна встановити підключення до пристроїв для поширення підключення до Інтернету. За допомогою зв'язку між модемами і пристроями в локальній мережі маршрутизатор полегшує зв'язок з Інтернетом і всередині мережі. Маршрутизатор забезпечує підключення на мережевому рівні системи і, таким чином, функціонує на третьому рівні моделі OSI.

2.4.4 Мережевий міст

Network bridge (Мережевий міст) - це мережевий пристрій, призначений для об'єднання сегментів мережі передачі даних в єдину мережу. Він працює на

канальному (другому) рівні моделі OSI (моделі взаємодії відкритих систем). На відміну від концентратора, який працює на фізичному рівні, мережевий міст не просто транслює отримані з одного порту пристрою на інші, а аналізує заголовок і відправляє на будь-який один порт, або не передає ні куди. Однак на відміну від маршрутизатора Network bridge не має таблиці маршрутизації і є саме налаштованим пристроєм і працює по заздалегідь закладеним в ньому принципам. Network bridge використовується в декількох мережевих технологіях, протенайбільшого поширення знайшов в Ethernet

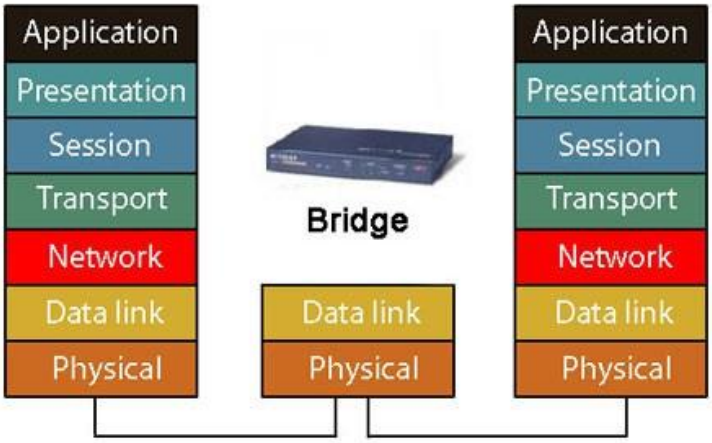


Рисунок 2.12 – Мережевий міст

Після включення в мережу Network bridge аналізує поле "адреса джерела» прийнятих пакетів. Цю інформацію він заносить в спеціальну таблицю. Відправляє він пакети відповідно до поля "адреса одержувача» після аналізу тієї ж таблиці. Якщо там немає відповідності порту і MAC-адреси, то він направляє цей пакет в усі вихідні порти. Якщо поле "адреса одержувача» містить MAC-адресу пристрою, який належить тій же мережі, звідки надійшов пакет, то він блокується. Таким чином, міст блокує пакети, призначені для одного сегмента мережі.

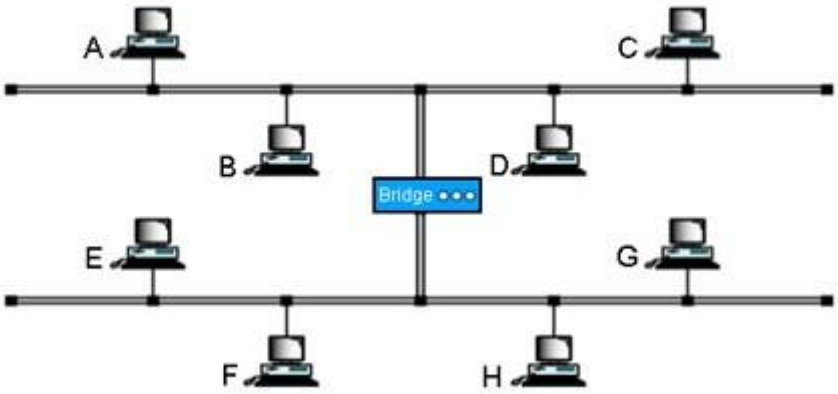


Рисунок 2.13 – Принцип роботи мережних мостів

Саме в цьому полягає головна перевага використання мостів - скорочення обсягу переданої інформації по всій мережі, за рахунок його локалізації на окремі фрагменти мережі.

Висновок

Рекомендовано використовувати топологію «зірка». За рахунок цього забезпечується захист від розриву кабелю, тобто якщо кабель робочої станції буде пошкоджений, це не призведе до виходу з ладу всього сегмента мережі, що забезпечує надійність всієї мережі. При збільшенні робочих станцій мережу не треба повністю міняти, треба тільки замінити або додати деякі компоненти. Технологія Fast Ethernet відповідає всім вимогам і підходить для корпоративної локальної комп'ютерної мережі.. Використовується недорогий кабель типу вита пара.

3 ПРОЕКТУВАННЯ І ДОСЛІДЖЕННЯ ЛОКАЛЬНОЇ МЕРЕЖІ НА ОСНОВІ ПРОГРАМНОГО ЗАСОБУ NETCRACKER PROFESSIONAL

3.1 Компоновка локальної комп'ютерної мережі

Робочі станції локальної обчислювальної мережі офісів ПП «Вітал» будуть об'єднані шляхом підключення до комутаторів по інтерфейсу Fast Ethernet 100BaseTX. У якості кабельної системи ЛОМ використовується кабель типу кручена пара категорії 5е (UTP Category 5e), що забезпечує пропускну здатність мережі у 100 Мбіт/сек. Фізична топологія кабельної системи представляє собою «зірку». Основним протоколом передачі даних у мережі є протокол TCP/IP.

Побудова локальної обчислювальної мережі мережі аптек буде виконана шляхом компоновки наступних підсистем:

1)Підсистема робочого місця.

2)Горизонтальна кабельна підсистема.

3)Центр комутації (телекомунікаційне приміщення).

3.2 Підсистема робочого місця

Абонентська підсистема робочого місця призначена для підключення устаткування користувачів до локальної обчислювальної мережі.

При побудові ЛОМ дуже важливим чинником є універсальність пропонованого рішення, можливість подальшої модернізації відповідно до вимог нових технологій інформаційних систем.

Для з'єднання комп'ютерного обладнання у локальної мережу знадобляться розетки RJ 45, патч-корди та конектори RJ 45.

Кожне робоче місце оснащується розетковим блоком RJ-45.

Їх кількість відповідатиме кількості робочих станцій та серверів в мережі.

Установка розеток може бути проведена:

– у внутрішній простір короба;

– на короб;

– поряд з коробом.

Для реалізації кожного з основних варіантів установки використовуються свої технічні засоби.

Загальною вимогою до інформаційної розетки, яке наведене в рекомендаціях BICSI, є їх розміщення на одній висоті з силовими розетками.

Як правило, для установки розетки у внутрішній простір застосовується багатосекційний короб. Центральна секція використовується тільки або переваг громадської для монтажу розеток , силові та інформаційні кабелі різного призначення прокладаються в бічних секціях.

Установка розетки з даного принципу технічно може бути виконана тільки для коробів досить великого поперечного перетину (звичайно 50х100 мм і більше).

Установка розетки на короб здійснюється за допомогою монтажної рамки. Цей спосіб установки розеток дозволяє в порівнянні з попереднім варіантом (установка розетки всередині короба) використовувати настінні кабельні канали трохи меншого поперечного перерізу. Однак виступаючі над поверхнею короба розетки менш захищені від механічних пошкоджень і володіють найгіршими з розглянутих варіантів установки естетичними характеристиками. Крім того, він часто можливий далеко не для всіх габаритів коробів одного типу.

Установка розетки поруч з коробом багато в чому об'єднує переваги двох попередніх варіантів, однак, застосовна тільки відносно коробів досить невеликих розмірів (мінікоробов або мініплінтусов).

Кріплення розетки поруч з коробом носить часто вживане на практиці.

Вони надто сильно виступають над поверхнею стіни, володіють хорошими естетичними показниками і дозволяють повністю використовувати внутрішній простір короба для прокладки кабелю. Їх недоліком є дещо більша

трудомісткість монтажу в порівнянні з методом установки у внутрішній простір короба (для кріплення потрібно просвердлити в стіні мінімум два, а частіше три додаткові отвори), а також необхідність застосування монтажної рамки.

Рисунок 3.1 – Однопортова розетка RJ-45

Горизонтальні короби в приміщеннях аптек будемо монтувати на висоті 1,0 м та 3,0 (2,5) м від підлоги.

Термінування кабелів в модулях RJ-45 проводиться згідно стандарту TIA/EIA T568B.

Рисунок 3.2 – Пристрій для термінування роз’ємів 8P8C (RG-45)

Підключення комп’ютерного устаткування до телекомунікаційних розеток здійснюється стандартними комутаційними кабелями з роз'ємами RJ-45.

В даному проекті для підключення комп’ютерного устаткування будуть використані патч-корди довжиною 1метр.

3.3 Горизонтальна кабельна підсистема

Проектований сегмент мережі об'єднуватиме 18 комп'ютерів, що розташовані в трьох офісах ПП «Вітал». Робочі станції, розташовані в окремих

офісах, будуть об’єднані між собою за допомогою комутаторів. Об’єднання сегментів корпоративної мережі буде виконано за допомогою програмного забезпечення Open VPN (через мережу Інтернет).

На рисунку 3.3 наведено схему розташування проектованих сегментів корпоративної мережі ПП «Вітал».

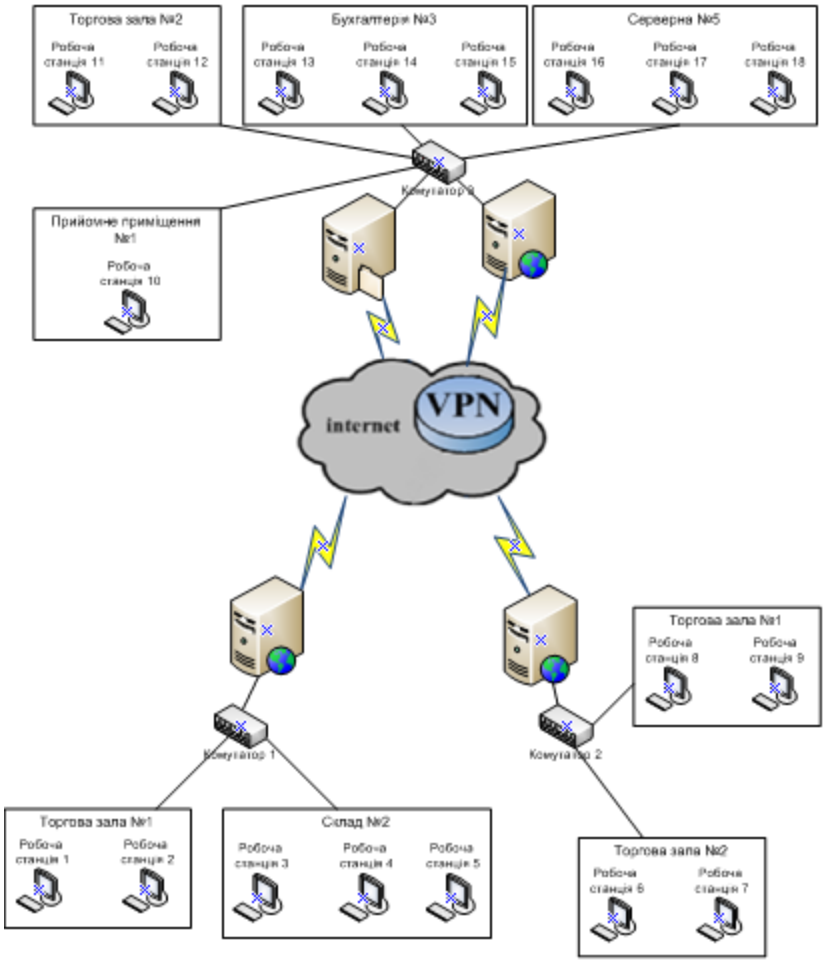


Рисунок 3.3 - Схема розташування сегментів корпоративної мережі ПП «Вітал»

У таблиці 3.1 приведена кількість зайнятих портів комутаторів та обрана кількість портів мережного устаткування.

Таблиця 3.1- Розміщення комутаційного обладнання

Назва приміщення	Назва обладнання	Кількість зайнятих портів	Кількість обраних портів
Серверна (5)	SW3	9	16
Склад (2)	SW1	5	8
Склад (1)	SW2	4	8

Комутатори вибрані з кількістю портів трохи більшим необхідного на даний момент, для того щоб в майбутньому можливо було включати в мережу нові робочі станції.

Для використання в проекті обрані комутатори TP-LINK TL-SF1008D, TP-LINK TL-SF1016DS. Ці комутатори володіють всіма необхідними нам функціями.

3.4 Центр комутації

Центр комутації розташований в головному офісі (вул.. Менделєєва, 22а) на першому поверсі (кабінет №5). Кабелі горизонтальної системи від робочих станцій, розташованих в інших приміщеннях, заведені в серверну кімнату.

У серверній кімнаті буде розташовуватись центральний комутатор на 16 портів і серверне устаткування.

3.5 Розрахунок кабелю, коробу та необхідних пристроїв

На підставі плану приміщення і схеми розташування устаткування проводиться розрахунок довжини кабельних сегментів та коробів для прокладки кабелю. Результати розрахунку занесені до таблиці 3.2, де наведена необхідна кількість патч-кордів, конекторів та мережних розеток.

Таблиця 3.2- Розрахунок кабельної системи

Назва приміщення	Кінцеве обладнання		Метраж кабелю,м				Кількість конекторів RJ-45	Кількість патч - кордів	Кількість мережних розеток
			ор (магіст	Перехід зі стелі	Горизонтально в кімнаті	Перехід до розетки			
1	2	3	4	5	6	7	8	9	10
Склад (2) Офіс 1 (вул.. Володимирсь-ка, 32)	SW1	1	0	0	5,0	0	1	1	1
		2	0	0	3,5	0	1	1	1
		3	0	0	1,0	0	1	1	1
		4	0	0	2,5	0	1	1	1
		5	0	0	5,5	0	1	1	1
Серверна (5) Головний офіс (вул..Менделеєва, 22а)	SW3	10	0	4,0	12,5	0	1	1	1
		11	0	0	8,5	0	1	1	1
		12	0	0	6,0	0	1	1	1
		13	0	0	7,0	0	1	1	1
		14	0	0	5,5	0	1	1	1
		15	0	0	4,0	0	1	1	1
		16	0	0	1,0	0	1	1	1
		17	0	0	2,5	0	1	1	1
		18	0	0	4,5	0	1	1	1
Склад (1) Офіс 2 (вул..Менделеєва, 44)	SW2	6	0	3,0	4,5	0	1	1	1
		7	0	0	7,5	0	1	1	1
		8	0	0	1,5	0	1	1	1
		9	0	0	3,0	0	1	1	1
Всього:			0	7	85,5	0	18	18	18

Таким чином, з урахуванням запасу у 5%, для організації сегменту корпоративної мережі аптек необхідно100 метри кабелю UTP Cat 5e.

Незалежно від різновидів конкретного конструктивного виконання кабельних трас «канального типу» всю їх сукупність можна класифікувати як:

– канали на основі труб;

– канали з прямокутним перерізом і знімними кришками, які встановлюють головним чином горизонтально з невеликою кількістю вертикальних ділянок в місцях переходу на різні рівні;

– канали з прямокутним перерізом без кришки;

– канали для прокладки кабельних джгутів.

В процесі проектування кабельних трас велике значення потребує оцінка ємності їх каналів, яка визначається як конструктивними особливостями каналів, так і типом і кількістю прокладених кабелів.

Максимальна теоретична кількість кабелів одного типу, яке може бути прокладено в конкретному кабельному каналі, досягається у випадку так званої гексагональної укладки. На практиці цього досягнути не можливо по деяким причинам. По-перше, кабель, прокладений в каналі тим чи іншим способом, не є ідеально прямим стержнем. По-друге, наявність стяжок, відводів і відхилень в певних межах знижує щільність упаковки пучка кабельних виробів. Вся сукупність вказаних факторів носить статистичний характер, і в процесі виконання практичних розрахунків її зручно враховувати за допомогою інтегрального параметра – коефіцієнта ki використання площі каналу конкретного виду. За визначенням коефіцієнт використання дорівнює відношенню сумарної площі Si перетину окремих кабелів, що знаходяться в каналі, до загальної площі Sкан перетину каналу конкретного типу:

$$k_i = \frac{\sum S_j}{S_{кан}},$$

Для каналів з круглим перерізом $k_i = 0{,}907$.

Для кабелю типу UTP 5e $S_i = 25{,}7$ мм^2.

Отримуємо формулу для розрахунку площі перерізу:

$$S_{кан} = \frac{25.7 * n}{0.907},$$

де n – кількість прокладених в каналі кабелів.

При виборі січення коробу корисно оцінити ємність коробу виходячи із заповнення його однорідним кабелем. Зазвичай розрахунки виконуються для

інформаційного кабелю діаметром 5,5 мм, силового кабелю NYM 3x1.5 діаметром 9 мм и силового кабелю NYM 3x2.5 діаметром 10 мм. У відповідності з методикою коефіцієнт заповнення приймається рівним 50%. У цьому випадку кількість кабелів (N) розраховується за формулою:

$$N=2*S/3.14*d^2,$$

де S – внутрішній переріз коробу, мм^2,

d - діаметр одиночного кабелю, мм.

Результати розрахунку і вибір конкретного конструктивного виконання коробів наведені в таблиці 3.3.

Таблиця 3.3 - Розрахунок і вибір конструктивного виконання кабельних каналів

Вид кабельного каналу	Довжина коробу, м	Максимальна кількість кабелів, прокла-дених в каналі	Розра-хункова площа перерізу в каналі, мм^2	Обраний кабельний канал
Горизонтальний канал в кімнаті	44	9	255,02	Короб з прямокутним перер ізом і знімною кришкою ро зміром 40x16
Вертикальний перехід в кімнаті	7	2	56,67	Короб з прямокутним перер ізом і знімною кришкою ро зміром 16x16

У таблиці 3.4 приведений розрахунок необхідного обладнання для організації локальної мережі.

Таблиця 3.4 – Необхідне обладнання для організації локальної мережі

№	Обладнання	Кількість, шт.
1	Комутатор TP-LINK TL-SF1008D <8 Ports, 100 Mbit>	2
2	Комутатор TP-LINK TL-SF1016DS<16 Ports, 100 Mbit, RJ45>	1
3	Розетка RJ-45 (однопортова)	18
4	Патч-корд литий UTP5e/ RJ45 (1,0м)	18
5	Кабель UTP 5e	100
6	Короб з кришкою 40x16	44
7	Короб з кришкою 16x16	8
8	Конектори RJ-45	18

3.6 Проектування і моделювання мереж зв'язку на основі програмного засобу NetCracker Professional

Побудову моделі спроектованої корпоративної мережі будемо виконувати за допомогою прикладної програми NetCrackerProfessional 4.1.

Програма NetCrackerProfessional призначена для моделювання локальних комп'ютерних мереж всіх типів, а також імітації процесів в цих мережах. При імітації процесів в створених проектах мереж програма дозволяє видавати звіти за результатами імітації.

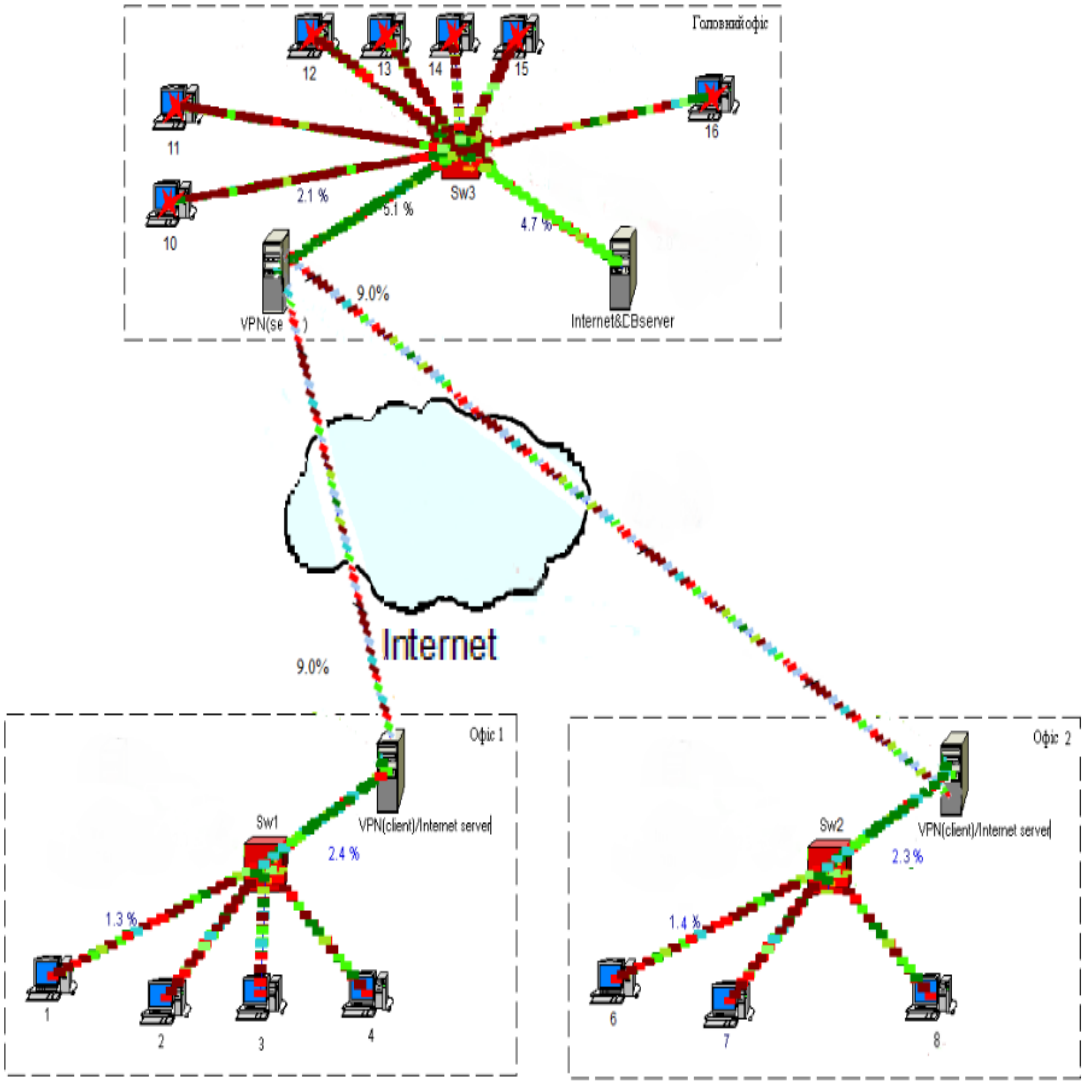


Рисунок 3.4 – Моделювання роботи мережі у програмі NetCracker Professional

При моделюванні спроектованої мережі встановлені наступні типи трафіків:

– усі комп’ютери в офісах обмінюються між собою звичайним офісним трафіком;

– робочі станції офісів мають доступ до файлового сервера та сервера баз даних головного офісу;

– комп’ютери бухгалтерії також мають доступ до сервера баз даних 1С у термінальному режимі;

– усі комп’ютери мають доступ до серверів Інтренет відповідного магазину.

Висновок

Моделювання проводилось при умові, що пропускна здатність VPN каналів складає близько 10 Мбіт/с.

Програмою NetCracker Professional 4.1 було змодельоване 48 годин роботи мережі у реальному часі. Моделювання дало наступні результати по завантаженню каналів зв’язку:

– завантаженість каналів що з’єднують комп’ютери з комутаторами у серверних становить близько 2,1%;

– завантаженість каналів, між центральними комутаторами та серверами не перевищує 6%;

– завантаженість VPN каналів становить від 9 % до 23,3%, але може бути зменшене при розширенні Інтернет каналу.

Виходячи з проведеного моделювання, можна зробити висновок, що мережа цілком працездатна.

4 ВИБІР ПРОГРАМНИХ ЗАСОБІВ, УСТАТКУВАННЯ ТА НАЛАШТУВАННЯ МЕРЕЖНИХ ПАРАМЕТРІВ

4.1 Вибір мережевого обладнання

При проектування сегментів локальної обчислювальної мережі офісів ПП «Віталь», будемо використовувати комутатори з кількістю портів 8 та 16:

- Комутатор TP-LINK TL-SF1016DS:
- EIA/TIA-568 100 Ом екранована вита пара (макс. 100 м);
- 100Base-Tx: неекранована вита пара категорій 5, 5e (макс.100 м);
- EIA/TIA-568 100 ОМ екранована вита пара (макс. 100 м);
- порти 16 x Fast Ethernet (10/100 Мбит/с);
- підтримка PoE - ні;
- можливість керування – некерований.

Рисунок 4.1 - Комутатор TP-LINK TL-SF1016DS

Комутатор TP-LINK TL-SF1008D

- протокол CSMA/CD;
- протоколи і стандарти IEEE 802.3 10Base-T, IEEE 802.3u 100Base-TX;
- порти 8 x Fast Ethernet (10/100 Мбит/с);
- підтримка PoE – ні;

– можливість керування – некерований.

Рисунок 4.2 - Комутатор TP-LINK TL-SF1008D

4.2 Вибір програмного забезпечення

Для забезпечення функціонування мережних сервісів в кожному офісі корпоративної мережі є по одному комп'ютеру-серверу, що виконують наступні функції:

– інтернет-шлюз – забезпечує доступ комп'ютерів до мережі Інтернет.

– сервер оновлень – виконує оновлення антивірусних баз та спеціалізованого програмного забезпечення на комп’ютерах локальної мережі центру зайнятості.

– сервер баз даних – зберігає єдину зберігає базу даних установи та забезпечує доступ до бази згідно з правилами розподілення ресурсів.

– файловий сервер – зберігає дані користувачів, а також містить різні інформаційні ресурси.

OpenVPN сервер – для організації VPN каналів між офісами.

Сервери будуть забезпечувати централізоване управління доступом до інформації. За допомогою таких широко відомих технологій, як Active Directory, PGP та інших, можна структурувати систему зберігання данних за рівнями доступу, в результаті ми отримаємо систему, де: кожен користувач має

доступ тільки до певної інформації; на кожному ресурсі можливо збереженні тільки тих даних, які визначені політикою безпеки; є можливість протоколювання будь-яких подій доступу до інформаційних ресурсів; вся збережена інформація чітко впорядкована. Файл-сервер. Всі робочі файли зберігаються на сервері. Доступ до них для різних користувачів і груп користувачів можна обмежити. Потрібний файл лежать на цілодобово працюючому сервері. Крім цього, на сервері можна зберігати резервні копії даних з усіх комп'ютерів мережі, що зменшить ризик втрати критичних даних. Єдина точка доступу в мережу Інтернет. Це дозволить більш ефективно захистити мережу від загроз ззовні, таких як: віруси і злом. На сервері буде встановлено відповідне програмне забезпечення, яке буде відсікати віруси і спроби проникнення мережу з Інтернет. Створення такого Інтернет-шлюзу дозволить також більш ефективно контролювати Інтернет-трафік і активність користувачів мережі. Централізоване оновлення антивірусних баз і управління системними оновленнями. Серверні технології дозволяють оновлювати антивірусні бази на робочих станціях автоматично і централізовано. По-перше кожному окремому комп'ютеру в мережі не потрібно завантажувати оновлення для себе окремо. Викачуються вони тільки один раз - на сервер, після чого розподіляються по локальних машин. Те саме можна сказати і до оновлень систем. Таким чином дуже сильно економиться трафік і час.

У якості операційної системи в даному проекті рекомендовано використовувати ОС Windows 10 та Windows Server 2008.

Windows 10 — операційна система від компанії Microsoft створена для персональних комп'ютерів, планшетів , ноутбуків, лептопів-трансформерів і смартфонів.

Організація VPN каналів між офісами буде виконана на основі програмного продукту OpenVPN. OpenVPN - технологія дозволяє на базі відкритого вихідного коду вибудовувати мережу VPN між клієнтом і сервером, сайтом та сайтом, поверх самого інтернету. Створений Джеймсом Йонаном 10 квітня 2002 року OpenVPN досі широко застосовується користувачами з метою

шифрування трафіку і безпечного використання всесвітньої павутини. Більш того, популярність технологи зростає з року в рік.

Рисунок 4.3 - Програмний продукт OpenVPN

4.3 Вибір методу побудови корпоративної мережі

У якості методу побудови мережі було обрано метод VPN (англ. Virtual Private Network - віртуальна приватна мережа) - це безпечне, зашифроване підключення між двома мережами або між окремим користувачем і мережею. Мережі VPN дозволяють користуватися Інтернетом, зберігаючи конфіденційність. Особливість побудови такої мережі - можливість доступу до Internet з будь-якої точки світу за допомогою зареєстрованого логіна і пароля. Використовується IT-компаніями, дизайнерськими бюро та іншими підприємствами, які наймають співробітників для віддаленої роботи.

Технологія VPN працює як плащ-невидимка - маскує користувача і зберігає анонімність. Користувач прихований в зашифрованих даних і надійно захований за іншою IP-адресою.

Технологія VPN шифрує всі дії в інтернеті. Все, що відправляється і отримується користувачем. Якщо вхід в мережу інтернет був виконаний через VPN, то відобразиться не справжнє джерело підключення, а один з численних VPN-маршрутизаторів.

Переваги:

– надання конфіденційності.

– virtual private network легко масштабується і є оптимальним варіантом для підприємств, що володіють безліччю філій, а також для фірм, чиї

співробітники часто бувають у відрядженнях або працюють з дому. Підключення нового офісу або нового віддаленого співробітника здійснюється без додаткових витрат на комунікації. Крім того, первісна організація віртуальної системи вимагає мінімум грошових витрат. Надалі фінансові вкладення будуть зводитися до оплати послуг провайдера Інтернету.

Недоліки:

– можливе уповільнення роботи. При підключенні через VPN потік даних проходить більше етапів, ніж зазвичай, що може викликати помітне уповільнення роботи. Оскільки це скарга № 1 щодо VPN, розробники взяли це до відома. Багато з них настільки досягли успіху в оптимізації швидкості і продуктивності, що їх користувачі VPN можуть без найменших проблем грати в ігри і дивитися трансляції. З плином часу уповільнення роботи все більше непомітно;

– труднощі, пов'язані з QoS. QoS означає «якість обслуговування» і описує продуктивність служби або мережі. Для мереж VPN поки немає будь-якого стандарту, який можна було б заміряти і повідомити показники. А оскільки немає показників для аналізу, потрібно покладатися на професійні огляди та «сарафанне радіо», щоб дізнатися, які служби найнадійніщі.

– блокування VPN

Деякі компанії розуміють, що мережі VPN дають їх користувачам карт-бланш. Щоб протистояти цьому, вони починають блокувати доступ для відомих IP-адрес VPN. Проте, служби VPN так легко не здолати - вони просто використовують нові IP-адреси.

– відсутність повної конфіденційності

Хоча мережа VPN справляється з шифруванням і збереженням вашої конфіденційності, що знаходяться у вашому браузері файли cookie все одно можуть вас впізнати. Ви можете їх вимкнути, якщо хочете.

Принцип роботи VPN.

При використанні віртуальної приватної мережі ніхто не побачить реальну IP-адресу, тому що замість нього тепер буде розпізнаватися адреса VPN.

Крім того, саме підключення до Інтернету буде зашифровано, так що ніхто не побачить дані, які користувач завантажує або відправляє. Шифрування - це спосіб перетворення тексту, що перетворюється в нечитаний набір кодів. Існує три основних види шифрування: хешування, симетричне і асиметричне шифрування. У кожного виду свої переваги і недоліки, але всі вони шифрують ваші дані так, що в чужих руках вони будуть марними.

Додатковий рівень захисту, який є у більшості служб VPN - їх власна система DNS. DNS - система доменних імен - це телефонна книга інтернету, в якій текстові URL-адреси ототожнені з відповідними IP-адресами. Система DNS дозволяє замість довгої послідовності цифр вводити назву сайту, наприклад vk.com. Кіберзлочинці можуть спостерігати за запитами DNS, щоб відстежувати ваші дії в інтернеті, але система DNS в службах VPN розроблена так, щоб за допомогою додаткового шифрування перешкодити їм.

Залежно від особливостей роботи підприємства і її конкретних завдань, Virtual Private Network може бути побудована за однією з наступних моделей:

– Remote Access. У цьому випадку створюється захищений канал між офісом і віддаленим користувачем, що підключаються до ресурсів підприємства з домашнього ПК через Інтернет. Подібні системи прості в побудові, але менш безпечні, ніж їх аналоги, вони використовуються підприємствами з великою кількістю віддалених співробітників.

– Intranet. Такий варіант дозволяє об'єднати кілька офісів організації. Передача даних здійснюється по відкритих каналах. Intranet може використовуватися для звичайних філій компаній і для мобільних офісів. Але слід мати на увазі, що такий спосіб передбачає установку серверів у всіх офісах.

– Extranet. Доступ до інформації підприємства надається клієнтам і іншим зовнішнім користувачам. При цьому їх можливості по використанню системи помітно обмежені. Не призначені для абонентів файли надійно захищаються засобами шифрування. Це відповідне рішення для фірм, яким необхідно забезпечити своїм клієнтам доступ до певної інформації.

– Client / Server. Цей варіант дозволяє обмінюватися даними між декількома вузлами всередині одного сегмента. Він користується найбільшою популярністю у організацій, яким необхідно в рамках однієї фізичної мережі створити кілька логічних (наприклад, окремі структури можуть бути створені для фінансового відділу, кадрової служби та ін.). Для захисту трафіку під час поділу використовується шифрування.

Різні види мереж VPN

Існує два основних види мереж VPN. Шлюз захищеного віддаленого доступу до VPN дозволяє користувачам підключитися до іншої мережі (до інтернету або внутрішньої системі своєї компанії) по приватному зашифрованому тунелю.

Другий вид - VPN типу «мережа-мережа», який ще називають VPN між маршрутизаторами. Цей вид мережі VPN в основному використовується в корпоративному середовищі, особливо якщо у підприємства є штаб-квартири з різним розташуванням. VPN типу «мережа-мережа» використовується для створення закритої внутрішньої мережі, де всі офіси можуть підключатися один до одного. Ця технологія відома як інтранет.

Існує ще кілька протоколів VPN, тобто способів забезпечення безпеки. Найстаріший з них - PPTP (протокол тунелювання «точка-точка»), який як і раніше застосовується, але вважається одним з самих ненадійних протоколів. Решта - IPSec, L2TP, SSL, TLS, SSH і OpenVPN. Багато хто віддає перевагу протоколу OpenVPN, оскільки це програмне забезпечення з відкритим вихідним кодом. Якщо в ній буде виявлена уразливість, хтось відразу ж про це повідомить, після чого її швидко виправлять.

4.4 Організація розподілення ресурсів мережі

Кожен комп'ютер, що підключається до локальної мережі офісів ПП «Віталл» й повинен мати свою індивідуальну IP-адресу. Ця адреса може бути виділена DHCP-сервером або вибрана із статичного діапазону IP-адрес.

IP-адреси для комп’ютерів мережі слід обирати з діапазонів, зарезервованих для локальних мереж:

- 10.0.0.0 - 10.255.255.255 (одна мережа класу A).
- 172.16.0.0 - 172.31.255.255 (шістнадцять мереж класу B).
- 192.168.0.0 - 192.168.255.255 (256 мереж класу C).

Оскільки корпоративна мережа офісів ПП «Віталл» поєднує в собі 3 офіси, то для кожного офісу повинен бути виділений власний адресний простір. Тобто повинно бути створено 3 підмережі:

1 Офіс 1 (вул..Володимирська, 32);

2 Офіс 2 (вул. Менделєєва, 40);

3 Головний офіс (вул..Менделєєва, 22а).

Обираємо за початкову мережу для розрахунків мережу з адресою 192.168.1.0 і маскою підмережі 255.255.255.0 (/24). Дана мережа дозволяє адресувати 254 вузли максимум. Запишемо маску підмережі в двійковому вигляді:

11111111.11111111.11111111.00000000

Щоб виділити в даній мережі підмережі, потрібно в останньому октеті частину старших біт використовувати для нумерації підмереж. Число 3 уміщається в 2 біта (22 > 3). Тому двум старшим бітам останнього октету привласнимо 1 - це означатиме, що ці біти є частиною номера мережі. У результаті отримаємо наступну маску підмережі:

11111111.11111111.11111111.11000000

Комбінація IP-адреси і маски підмережі в двійковому вигляді виглядатиме так::

11000000.10101000.00000001.00000000

11111111.11111111.11111111.11000000

Визначимо адреси підмереж, а також адреси вузлів в підмережах

Таблиця 4.1 – Розподілення адресного простору мережі

Підмережа №1		
Адреса підмережі	11000000.10101000.00000001.00000000 192.168.1.0	
Маска підмережі	11111111.11111111.11111111.11000000 255.255.255.192 /26	
Широкомовна адреса	11000000.10101000.00000001.00111111 192.168.1.63	
Адреси вузлів		
Вузол 1	192.168.1.1	
Вузол 2	192.168.1.2	
Вузол 3	192.168.1.3	
Вузол 4	192.168.1.4	
Вузол 5	192.168.1.5	
Підмережа №2		
Адреса підмережі	11000000.10101000.00000001.01000000 192.168.1.64	
Маска підмережі	11111111.11111111.11111111.11000000 255.255.255.192 /26	
Широкомовна адреса	11000000.10101000.00000001.01111111 192.168.1.127	
Адреси вузлів		
Вузол 6	192.168.1.65	
Вузол 7	192.168.1.66	
Вузол 8	192.168.1.67	
Вузол 9	192.168.1.68	
Підмережа №3		
Адреса підмережі	11000000.10101000.00000001.10000000 192.168.1.128	
Маска підмережі	11111111.11111111.11111111.11000000 255.255.255.192 /26	
Широкомовна адреса	11000000.10101000.00000001.10111111	192.168.1.191

Продовження таблиці 4.1

Адреси вузлів	
Вузол 10	192.168.1.129
Вузол 11	192.168.1.130
Вузол 12	192.168.1.131
Вузол 13	192.168.1.132
Вузол 14	192.168.1.133
Вузол 15	192.168.1.134
Вузол 16	192.168.1.135
Вузол 17	192.168.1.136
Вузол 18	192.168.1.137

4.5 Організація VPN каналів між офісами.

Організація VPN каналів між офісами буде виконана на основі програмного продукту OpenVPN.

У проекті мається на увазі, що OPENVPN встановлюватиметься на платформах Windows 10 та Windows 7.

4.6 Структура корпоративної мережі

В даному проекті корпоративна мережа має наступну структуру:

1. Мережа офісу по вулиці Володимирська, 32 (Офіс 1);
2. Мережа офісу по вулиці Менделєєва, 40 (Офіс 2);
3. Мережа головного офісу за адресою вул..Менделєєва, 22а (далі - офіс).

Необхідно з'єднати офіси так, щоб кінцевий комп'ютер користувача (PC1) офісу 2 (3) мав доступ до загальних ресурсів головного офісу.

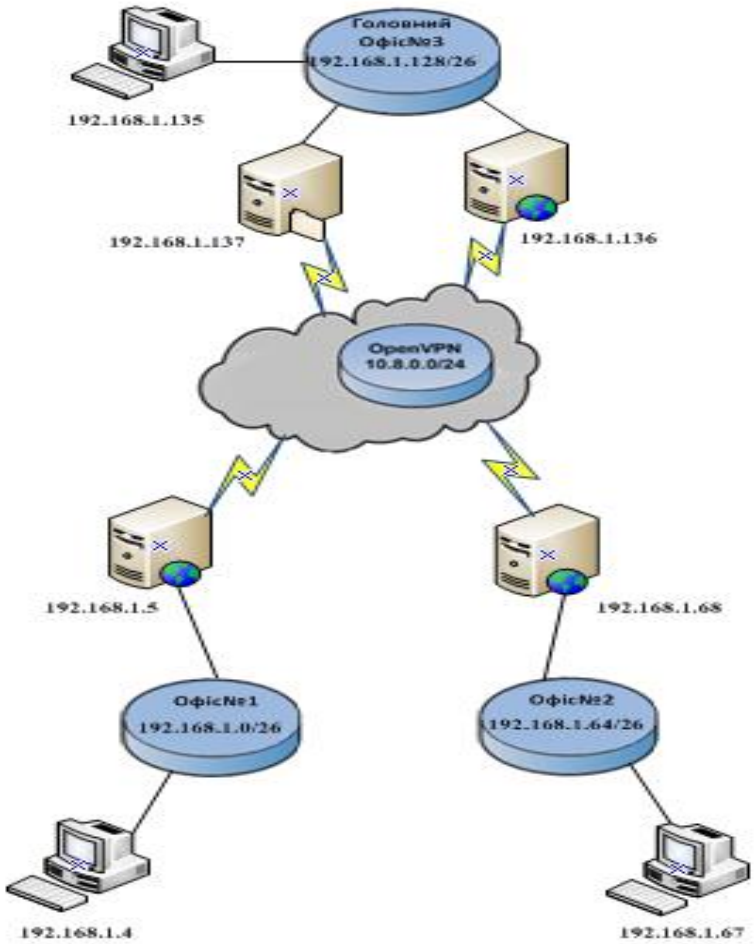


Рисунок 4.4 – Структура корпоративної мережі аптек

Мережа центрального офісу має в своєму складі:

Інтернет-шлюз з двома мережними інтерфейсами:

– 111.111.111.111 - видається провайдером, дивиться в Інтернет.

– 192.168.1.136 - призначається системним адміністратором, дивиться в локальну мережу.

OpenVPN сервер на якому встановлено програмне забезпечення OpenVPN з одним віртуальним і одним фізичним інтерфейсом;

– 10.8.0.1 - адреса віртуального інтерфейсу (інтерфейс встановлюється в процесі установки програми OpenVPN). Адреса для цього інтерфейсу призначається програмою.

– 192.168.1.137 - фізичний інтерфейс, параметри задаються системним адміністратором, дивиться в локальну мережу головного офісу.

PC1 - комп'ютер користувача, з мережним інтерфейсом 192.168.1.135, дивиться аналогічно в локальну мережу.

Мережа першого офісу має в своєму складі:

Інтернет-шлюз/ OpenVPN клієнт з такими мережними інтерфейсами:

– 111.111.111.112 - видається провайдером, дивиться в Інтернет.

– 192.168.1.5 - призначається системним адміністратором, дивиться в локальну мережу офісу.

– 10.8.0.2 - адреса віртуального мережного інтерфейсу (інтерфейс встановлюється в процесі установки програми OpenVPN). Адреса для цього інтерфейсу так само призначається програмою OpenVPN.

PC2 - комп'ютер користувача, з мережним інтерфейсом 192.168.1.4, дивиться аналогічно в локальну мережу.

Мережа другого офісу має в своєму складі:

Інтернет-шлюз/ OpenVPN клієнт з такими мережними інтерфейсами:

– 111.111.111.113 - видається провайдером, дивиться в Інтернет.

– 192.168.1.68 - призначається системним адміністратором, дивиться в локальну мережу офісу.

– 10.8.0.3 - адреса віртуального мережного інтерфейсу (інтерфейс встановлюється в процесі установки програми OpenVPN). Адреса для цього інтерфейсу так само призначається програмою OpenVPN.

PC3 - комп'ютер користувача, з мережним інтерфейсом 192.168.1.67, дивиться аналогічно в локальну мережу.

4.7 Налаштування OpenVPN сервера

VPN-сервер надає VPN-послуги, які являють собою комбінацію апаратних і програмних технологій. Як правило, це стандартний сервер, який налаштований за допомогою ПО на надання VPN-послуг, але тільки обладнаний додатковими логічними і фізичними портами. Більшість серверів

для аутентифікації нових клієнтів використовують більше одного методу комунікації і протоколу шифрування (як, наприклад, PPP).

В процесі установки в систему інсталюється віртуальний мережний адаптер Tap-win32 Adapter V9 і, відповідно, драйвер до нього. Цьому інтерфейсу програма OpenVPN якраз і призначатиме IP адресу і маску віртуальної мережі OpenVPN. У нашому випадку йому призначена адреса 10.8.0.1 з маскою 255.255.255.0 на сервері OpenVPN головного офісу і 10.8.0.2 та 10.8.0.3 з аналогічною маскою на клієнтах OpenVPN в офісах.

За стандартом програма встановлюється в C:\ProgramFiles\OpenVpn. У цій директорії слід відразу ж створити додатково папку KEYS (тут необхідно зберігати ключі аутентифікації) та папку CCD (тут будуть знаходиться конфігураційні файли налаштувань сервера для клієнта).

У директорії C:\ProgramFiles\OpenVpn\sample-config представлені стандартні конфігураційні файли. Конфігураційні файли, які необхідно створити самостійно, повинні розміщуватися в директорії C:\ProgramFiles\OpenVpn\config.

Налаштування OpenVPN починається з генерації ключів. Ключі, що генеруються, діляться на:

– головний сертифікат і ключ для підписки кожного сертифікату сервера і клієнта, CertificateAuthority (CA).

– публічний і приватний ключі для сервера і кожного (це важливо) клієнта окремо.

Послідовність створення ключів наступна (назви файлів сертифікатів і ключів вказані в дужках):

– генеруємо основний сертифікат і CA (ca.key) CA (ca.crt) ключ;

– генеруємо сертифікат (server.crt) і ключ (server.key) сервера;

– генеруємо сертифікат (ClientVPN1.crt) і ключ (ClientVPN1.key) для клієнта;

– генеруємо сертифікат (ClientVPN2.crt) і ключ ClientVPN2.key) для клієнта;

– генерація параметрів Diffiehellman (dh2048.pem);
– генерація ключа tls-auth (ta.key) для аутентифікації пакетів.

4.7.1 Генерація основного сертифікату та ключа

Ключ VPN-шифрування - це випадкова строка бітів, що використовується для шифрування і розширювання даних. Кожный ключ шифрування унікальний. Довжина ключа шифрування вимірюється у бітах - як правило, чим довше ключ, тим вище рівень шифрування.

У командному рядку необхідно виконати наступну команду:

```
cd C:/Program Files/Openvpn/easy-rsa
```

Таким чином здійсниться перехід до директорії easy-rsa.

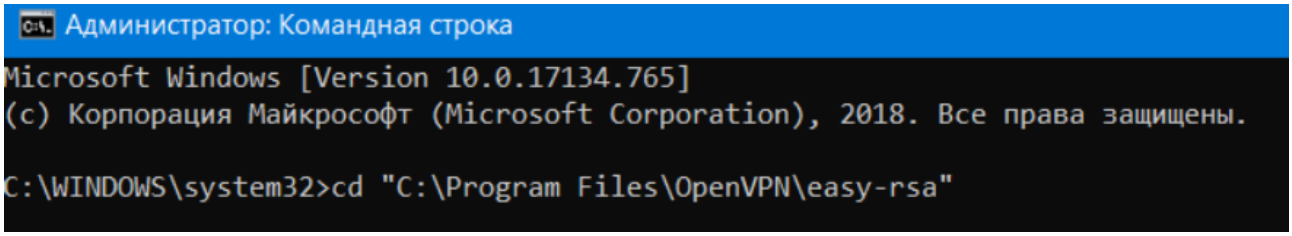


Рисунок 4.5 – Перехід до директорії easy-rsa

Під час виконання всіх пунктів генерації ключів необхідно знаходитися саме в цій директорії.

Далі виконується команда: init-config.

Не закриваючи командний рядок, необхідно зайти в C:\ Program Files/Openvpn \easy-rsa та відрегувати файл vars.bat, заповнивши наступні параметри:

```
Key_country=ua
Key_province=lg
Key_city=rubigne
Key_org = PP Vital
Key_email= danylenkov84@gmail.com
```

Наступним кроком необхідно створити CA сертифікат та CA ключ. В командному рядку вписуються команди:

```
vars
clean-all
build-ca
```

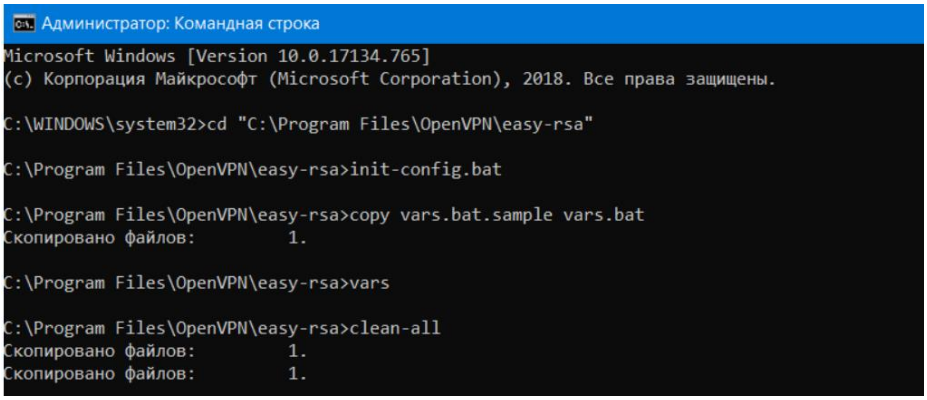


Рисунок 4.6 – Генерація CA сертифікату

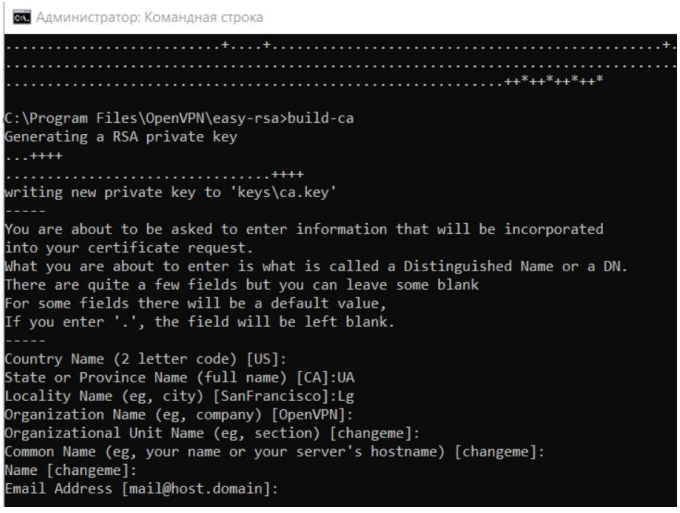


Рисунок 4.7 – Генерація CA ключа

Остання команда саме і виконує генерацію CA сертифікату і CA ключа. В процесі створення ключа система ставитиме питання, на які необхідно відповідати просто натисненням Enter'a (тоді значення братимуться з файлу vars.bat) або ж вводити свої.

4.7.2 Генерація сертифікату та ключа сервера

Не виходячи з директорії EASY-RSA, в командному рядку необхідно продовжити вводити команди. Сертифікат сервера і ключа генерується командою:

```
build-key-server ServerVPN
```

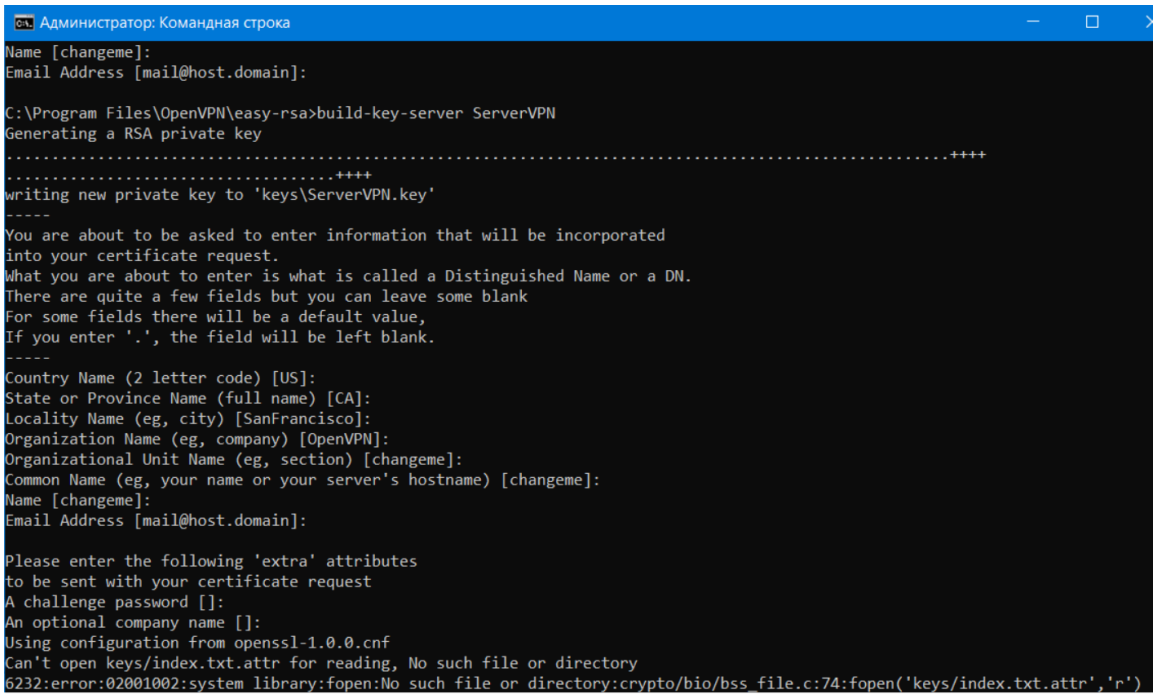


Рисунок 4.8 – Генерація ключа сервера

На питання відповідати потрібно так само. На питання:

Common Name *: server

Необхідно ввести: server. На питання: «Sign the certificate? [y/n]» та «1 out of 1 certificate requests certified, commit? [y/n]» потрібно дати позитивну відповідь: Y.

4.7.3 Генерація сертифікату та ключа для клієнтів

Очевидно, що клієнтів може бути багато, в нашому прикладі їх два - ClientVPN1 та ClientVPN2. Залежно від кількості клієнтів наступна команда в командному рядку виконується кілька разів, причому назви ключів, що генеруються, так само змінюються:

```
build-key ClientVPN1
```

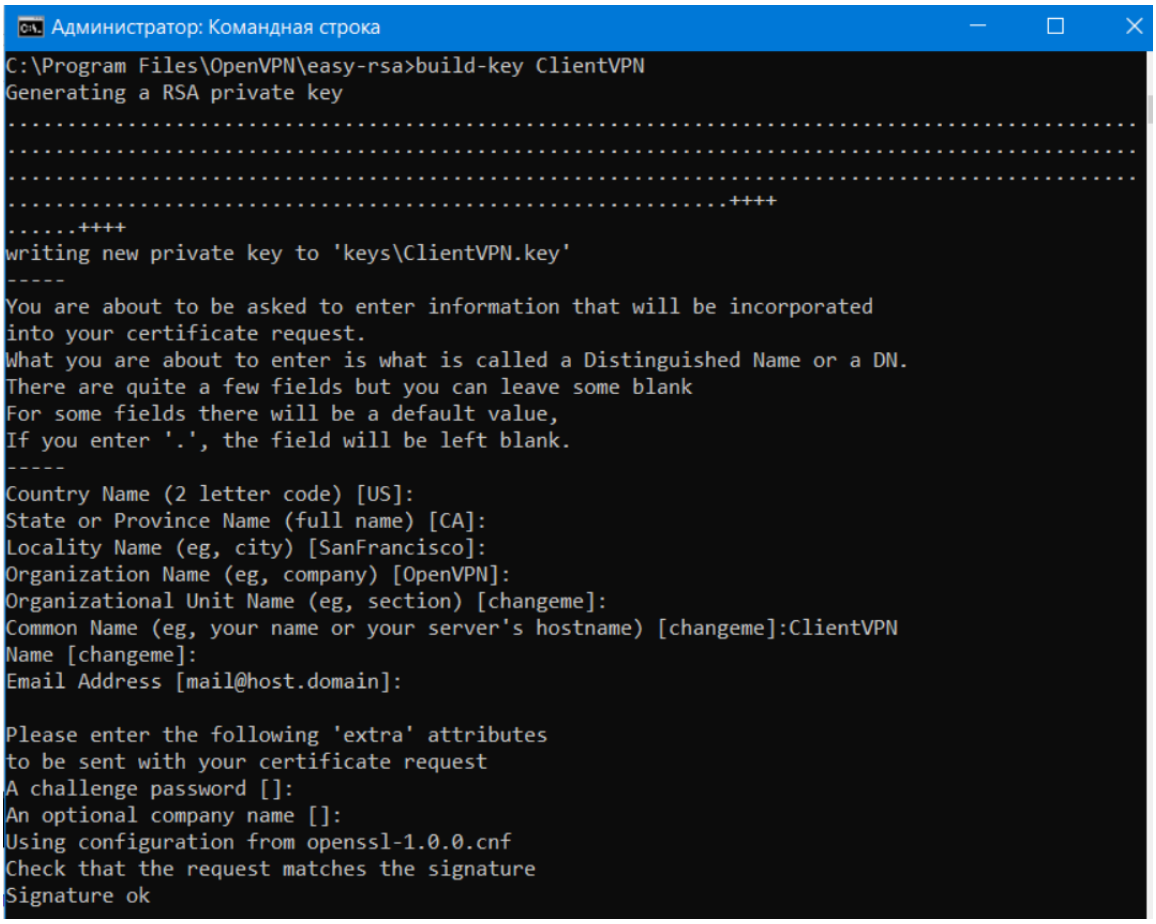


Рисунок 4.9 – Генерація ключа клієнта

Якщо потрібний ще сертифікати і ключі для другого клієнта, то необхідно ввести:

```
build-key ClientVPN2
```

В процесі відповіді на питання кожен клієнт на питання CommonName повинен отримати унікальне ім'я, наприклад: ClientVPN1, ClientVPN2 і так далі.

4.7.4 Створення конфігураційного файлу сервера

На сервері повинні знаходитися в створеній директорії keys тільки наступні файли:

ca.crt;

ca.key;

dh2048.pem;

server.crt;

server.key;

ta.key.

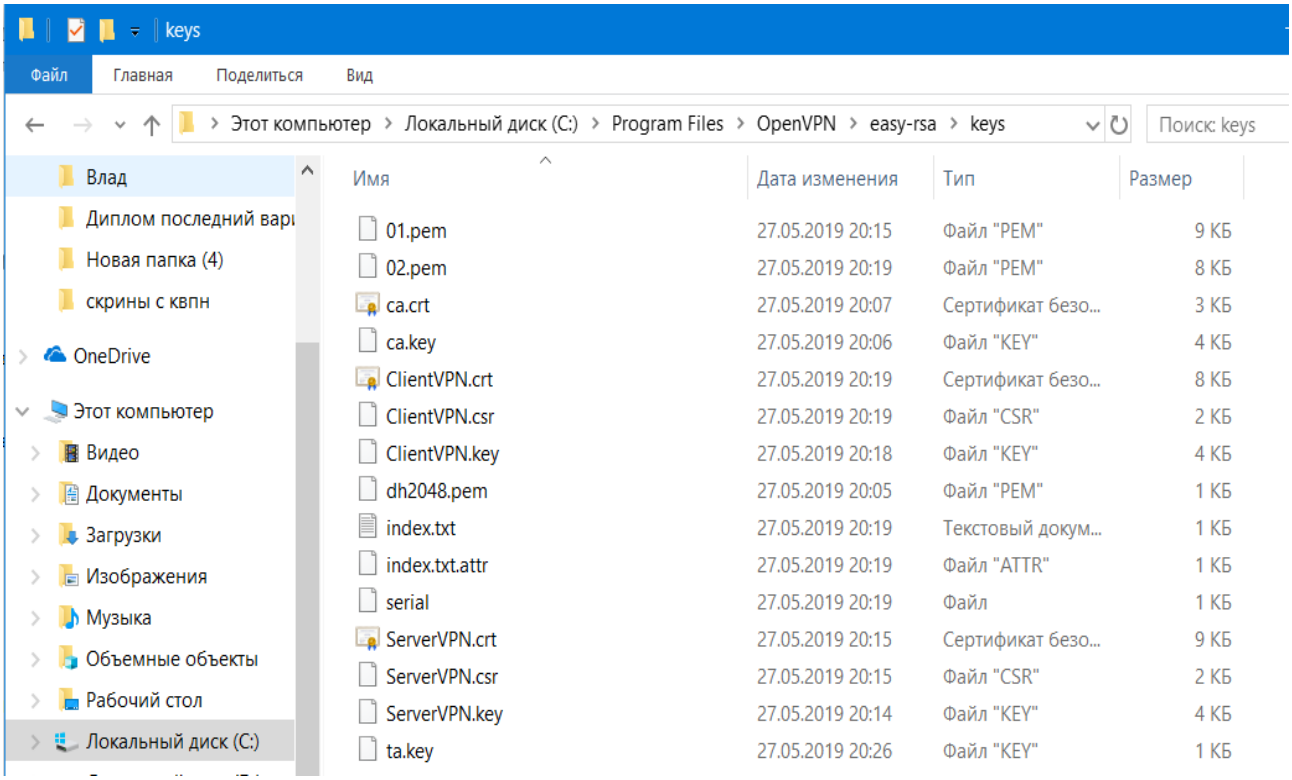


Рисунок 4.10 – Перелік файлів для сервера

Всі файли з розширенням .key є секретними. Передавати їх варто тільки по захищених каналах, краще на фізичних носіях.

У директорії config необхідно створити файл з наступною назвою і розширенням «server.ovpn» та відкоригувати наступним чином:

Протокол для передачі даних - в даному випадку udp:

```
proto udp
```

Стандартний порт для OPENVPN:

port 1194

Режим роботи програми L3-туннель. У даному режимі OPENVPN - роутер:

```
dev tun
```

Режим клієнт-сервер:

```
tls-server
```

Ця топологія доступна з версії 2.1 і полягає в тому що кожному клієнтові видається по 1 адресі, без віртуальних портів маршрутизатора:

```
topology subnet
```

Маршрути додаються через .exe:

```
route-method exe
```

Затримка при додаванні маршруту, можна зменшити до 5:

```
route-delay 10
```

Дана опція задає організацію мережі. Таким з'являється віртуальна мережа 10.8.0.0 /24. Перша адреса з цієї мережі, тобто 10.8.0.1 видається серверу, подальші (10.8.0.2, 10.8.0.3 і так далі) клієнтам. DHCP сервер отримує адреса 10.8.0.254:

```
server 10.8.0.0 255.255.255.0
```

Шлюз в OpenVPN мережі:

```
route-gateway 10.8.0.1
```

Директорія, в якій повинні розташуватись файл з назвою клієнта, тобто CA:

```
client-config-dir "C:\ProgramFiles\OpenVPN\ccd"
```

Далі йдуть шляхи до файлів сертифікатів і ключів сервера.

```
ca  "C:\program Files\OpenVPN\keys\ca.crt"
cert "C:\program Files\OpenVPN\keys\server.crt"
key  "C:\program Files\OpenVPN\keys\server.key"
dh "C:\program Files\OpenVPN\keys\dh2048.pem"
tls-auth "C:\program Files\OpenVPN\keys\ta.key"
```

Далі серверу OpenVPN необхідно задати маршрут на всю мережу:

```
route 10.8.0.0 255.255.255.0
```

Метод стиснення:

cipher BF-CBC

Стиснення трафіку:

```
comp-lzo
```

OpenVPN передає системі реєстрації подій програми не критичні помилки мережі. На практиці це зменшить вміст статус-вікна, сервера OpenVPN, що з'являється при запуску:

verb 1

Сервер пінгує протилежну сторону з інтервалом в 5 секунд і якщо сторона не відповідає за 60 секунд, то сервер запустить перепідключення:

```
keepalive 5 60
```

Далі необхідно перейти в директорію ccd і створити файл, в якому лежатимуть команди, що посилаються клієнтові від сервера. Назвати його треба так само як було названо самого клієнта: ClientVPN1 та ClientVPN2. Файл не матиме розширення.

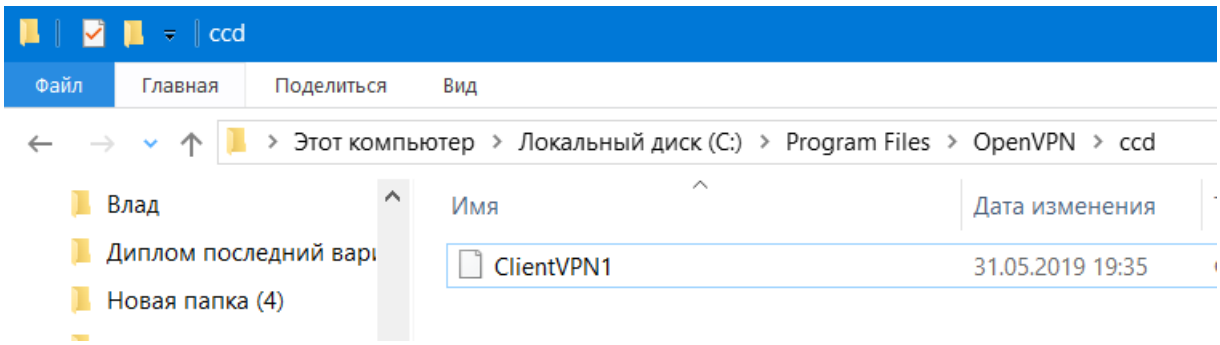


Рисунок 4.11 – Конфігураційний файл клієнта

Всі параметри, задані нижче, будуть автоматично передані клієнтові.

IP-адреса та маска для клієнта ClientVPN1:

```
ifconfig-push 10.8.0.2 255.255.255.0
```

Маршрут на всю мережу:

```
push "route 10.8.0.0 255.255.255.0"
```

Шлюз для клієнта:

```
push "route-gateway 10.8.0.1"
```

Ця команда говорить серверу OpenVPN про те, що за даним клієнтом, а саме за першим офісом(ClientVPN1) знаходиться мережа 192.168.1.0:

```
iroute 192.168.1.0 255.255.255.192
```

Аналогічно створюється файл для другого клієнта OpenVPN.

4.8 Налаштування OpenVPN клієнта

Для зміни параметрів клієнта необхідно в директорії config на комп’ютерах-клієнтах OpenVPN (5 та 9) створити конфігураційний файл ClientVPN1.ovpn та ClientVPN2.ovpn відповідно.

Ряд опцій у цьому файлі повторює аналогічні на сервері:

```
dev tun
proto udp
port 1194
```

Вказуєму зовнішню адресу Інтернет-шлюзу:

```
remote 111.111.111.111
```

Клієнт буде в працювати в режимі tls-клиєнта:

```
tls-client
```

Ця опція захищає від підміни сервера третьою особою:

```
remote-cert-tls server
```

Наступні опції аналогічні серверу:

```
route-method exe
route-delay 10
```

Задаємо маршрут до мережі 192.168.1.0:

```
route 192.168.1.0 255.255.255.192
```

Наступна команда вирішує прийом конфігурації клієнта з сервера:

```
pull
```

Шляхи до ключів:

```
ca "C:\program Files\OpenVPN\keys\ca.crt"
cert "C:\program Files\OpenVPN\keys\ ClientVPN1.crt"
key "C:\program Files\OpenVPN\keys\ ClientVPN1.key"
tls-auth "C:\program Files\OpenVPN\keys\ta.key"
```

Решта опцій також аналогічна серверу:

```
cipher BF-CBC
comp-lzo
verb 1
keepalive 5 60
```

4.9 Налаштування брандмауера і маршрутизація

Якщо мережа використовує мережевий екран або антивірус, на екрані повинні бути дозволені пакети ICMP. Це дозволить необмежену кількість пінг-

хостів у мережах інших офісів корпоративної мережі.Варто також додати віртуальний інтерфейс програми OpenVPN до списку надійних мереж.

На Інтернет-шлюзі головного офісу повинні бути виконані наступні дії:

– Налаштовано перенаправлення порту 1194 протоколу UDP з інтерфейсу 111.111.111.111 на інтерфейс сервера OpenVPN 192.168.1.137.

На Інтернет-шлюзі першого офісу треба зробити аналогічні дії:

– Налаштування перенаправлення порту 1194 протоколи UDP з інтерфейсу 111.111.111.112 на інтерфейс клієнта OpenVPN 192.168.1.5.

Перевірити, чи відкритий порт 12345 протоколу UDP у файєрволі.

На Інтернет-шлюзі другого офісу виконуються дії:

– Налаштування перенаправлення порту 1194 протоколи UDP з інтерфейсу 111.111.111.113 на інтерфейс клієнта OpenVPN 192.168.1.64.

Перевірка, чи відкритий порт 1194 протоколу UDP у файєрволі.

Далі необхідно забезпечити правильний маршрут пакетів від клієнта OpenVPN до видаленої мережі 192.168.1.0.

Потрібно встановити постійний маршрут до цієї мережі на самому клієнті OpenVPN:

```
route  -p add 192.168.1.0 mask 255.255.255.192 10.8.0.1
```

Потім необхідно забезпечити маршрут пакетів з сервера OpenVPN до видаленої мережі 192.168.1.64 та 192.168.1.128. Виконується це аналогічно варіанту вище:

```
route -p add 192.168.1.64 mask 255.255.255.192 10.8.0.2
route -p add 192.168.1.128 mask 255.255.255.192 10.8.0.3
```

Аналогічно, сервер OpenVPN і клієнти OpenVPN повинні включати службу маршрутизації та віддаленого доступу в послуги, забезпечуючи таким чином маршрутизацію до внутрішньої мережі (переадресація).

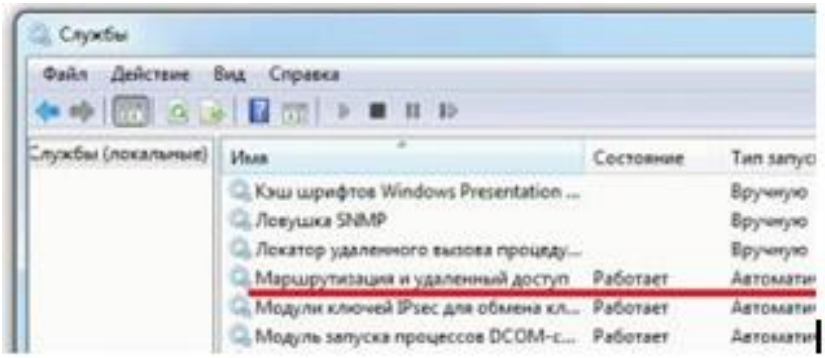


Рисунок 4.12 – Запуск служби «Маршрутизація і видалений доступу»

Останнім кроком буде маршрутизація командного рядка в мережу 10.8.0.0 на всіх комп'ютерах користувачів.

Для комп’ютерів головного офісу:

```
route -p add 192.168.1.0 mask 255.255.255.192 192.168.1.5
route -p add 192.168.1.64 mask 255.255.255.192 192.168.1.68
```

Для комп’ютерів першого офісу:

```
route -p add 192.168.1.64 mask 255.255.255.192 192.168.1.68
route -p add 192.168.1.128 mask 255.255.255.192 192.168.1.137
```

Для комп’ютерів другого офісу:

```
route -p add 192.168.1.0 mask 255.255.255.192 192.168.1.5
route -p add 192.168.1.128 mask 255.255.255.192 192.168.1.137
```

Як результат, відкриті ресурси в локальних мережах будуть доступні по їх внутрішніх адресах.

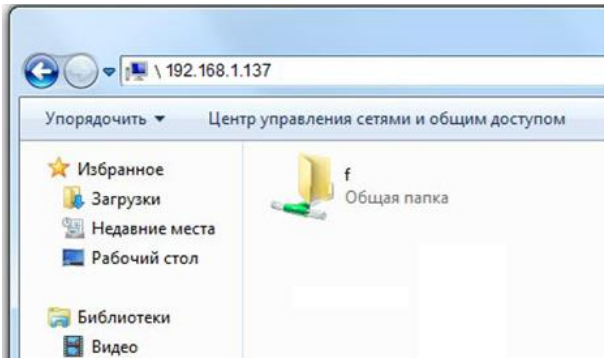


Рисунок 4.13 – Приклад доступу до ресурсів інших мереж.

Висновок

У даному розділі була спроектована мережа на основі програмного продукту OpenVPN. Мережа повністю налаштована та функціонує без нарікань..

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

В даному розділі проведено аналіз потенційних небезпечних та шкідливих виробничих факторів, причин пожеж. Розглянуті заходи, які дозволяють забезпечити гігієну праці і виробничу санітарію. На підставі аналізу розроблені заходи з техніки безпеки та рекомендації з пожежної профілактики.

Завданням даного проекту бакалавра було створення корпоративної комп'ютерної мережі для факультету Інформаційних Технологій та Електроніки СНУ ім. В. Даля, і як результат була спроектована корпоративна комп'ютерна мережа, яке забезпечує спільний доступ до баз даних та роботу з пакетами комунікаційних програм. Так як в процесі проектування виконувалось у домашніх умовах, то аналіз потенційно небезпечних і шкідливих виробничих чинників виконується для персонального комп'ютера на якому буде розроблена комп'ютерна мережа.

5.1 Загальні питання з охорони праці

Згідно з законом "Про охорону праці" [14] охорона праці це – система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності.

При роботі з обчислювальною технікою змінюються фізичні і хімічні фактори навколишнього середовища: виникає статична електрика, електромагнітне випромінювання, змінюється температура і вологість, рівень вміст кисню і озону в повітрі. Забезпечення цих умов покладається на власника або уповноважений ним орган (далі роботодавець). Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального

захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам нормативних актів про охорону праці.

5.2 Аналіз стану та умов праці

Робота над створенням локальної комп’ютерної мережі проходить в побутовому приміщенні. Для даної роботи достатньо однієї людини, для якої надано робоче місце зі стаціонарним комп’ютером.

5.2.1 Вимоги до приміщення

Геометричні розміри приміщення зазначені в табл. 5.1.

Таблиця 5.1 – Розміри приміщення

Найменування	**Значення**
Довжина, м	5
Ширина, м	4
Висота, м	3
Площа, $м^2$	20
Об’єм, $м^3$	60

Згідно з ДСН 3.3.6.042-99 “Санітарні норми мікроклімату виробничих приміщень” [15] розмір площі для одного робочого місця оператора персонального комп’ютера має бути не менше 6 кв. м, а об’єм — не менше 20 куб. м. Отже, дане приміщення цілком відповідає зазначеним нормам.

Також для дотримання визначеного рівня мікроклімату в будівлі встановлено систему опалення та кондиціонування.

Для забезпечення потрібного рівного освітленості кімната має вікно та систему загального рівномірного освітлення, що встановлена на стелі. Для дотримання вимог пожежної безпеки встановлено порошковий вогнегасник та систему автоматичної пожежної сигналізації.

5.2.2 Вимоги до організації робочого місця

При порівнянні відповідності характеристик робочого місця нормативним основні вимоги до організації робочого місця за ДСанПіН 3.3.2.007-98 «Правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» [16] і відповідними фактичними значеннями для робочого місця, констатуємо повну відповідність в таблиці 5.2.

Таблиця 5.2 - Характеристики робочого місця

Найменування параметра	**Фактичне значення**	**Нормативне значення**
Висота робочої поверхні, мм	700	680 ÷800
Висота простору для ніг, мм	680	не менше 600
Ширина простору для ніг, мм	550	не менше 500
Глибина простору для ніг, мм	700	не менше 650
Висота поверхні сидіння, мм	500	400 ÷500
Ширина сидіння, мм	400	не менше 400
Глибина сидіння, мм	400	не менше 400
Висота поверхні спинки, мм	600	не менше 300
Ширина опорної поверхні спинки, мм	400	не менше 380
Радіус кривини спинки в горизонтальній площині, мм	400	400
Відстань від очей до екрану дисплея, мм	800	700 ÷800

Приміщення кабінету знаходиться у вчасній одноповерховій будівлі і має об’єм 54 м3, площу — 18 м2.

Температура в приміщенні протягом року коливається у межах 18–24°С, відносна вологість — близько 50%. Система вентилювання приміщення — природна неорганізована, а опалення — централізоване.

Розміщення вікон забезпечує природне освітлення з коефіцієнтом природного освітлення не менше 1,5%, а загальне штучне освітлення, яке здійснюється за допомогою однієї люмінесцентної лампи, забезпечує рівень освітленості не менше 200 Лк

За ступенем пожежної безпеки приміщення належить до категорії В

5.2.3 Навантаження та напруженість процесу праці

Під час виконання робіт використовують ПК та периферійні пристрої (лазерні та струменеві), що призводить до навантаження на окремі системи організму. Такі перекоси у напруженні різних систем організму, що трапляються під час роботи з ПК, зокрема, значна напруженість зорового аналізатора і довготривале малорухоме положення перед екраном, не тільки не зменшують загального напруження, а навпаки, призводять до його посилення і появи стресових реакцій.

Найбільшому ризику виникнення різноманітних порушень піддаються: органи зору, м'язово-скелетна система, нервово-психічна діяльність, репродуктивна функція у жінок.

Тобто наявні психофізіологічні небезпечні та шкідливі фактори:

а) фізичного перевантаження:

– статичного;
– динамічного;
– нервово-психічного перевантаження:
– розумового перенапруження;
– монотонності праці;
– перенапруження аналізаторів;
– емоційних перевантажень.

Роботу за дипломним проектом визнано, таку, що займає 50% часу робочого дня та за восьмигодинної робочої зміни рекомендовано встановити додаткові регламентовані перерви тривалістю 15 хв через кожну годину роботи.

5.3 Виробнича санітарія

На підставі аналізу небезпечних та шкідливих факторів при виробництві (експлуатації),пожежної безпеки можуть бути надалі вирішені питання

необхідності забезпечення працюючих достатньою кількістю освітлення, вентиляції повітря, організації заземлення, тощо.

5.3.1 Загальні заходи безпеки

Відповідно до санітарно-гігієнічних нормативів та правил експлуатації обладнання приклад деяких заходів безпеки:

1. Заходи безпеки під час експлуатації персонального комп'ютера та периферійних пристроїв передбачають:

– правильне організування місця праці та дотримання оптимальних режимів праці та відпочинку під час роботи з ПК;

– експлуатацію сертифікованого обладнання;

– дотримання заходів електробезпеки;

– забезпечення оптимальних параметрів мікроклімату;

– забезпечення раціонального освітлення місця праці (освітленість робочого місця не перевищувала 2/3 нормальної освітленості приміщення);

– облаштовуючи приміщення для роботи з ПК, потрібно передбачити припливно-витяжну вентиляцію або кондиціювання повітря;

– зниження рівня шуму та вібрації:

2. Заходи безпеки під час експлуатації інших електричних приладів передбачають дотримання таких правил:

– постійно стежити за справним станом електромережі, розподільних щитків, вимикачів, штепсельних розеток, лампових патронів, а також мережевих кабелів живлення, за допомогою яких електроприлади під'єднають до електромережі;

– постійно стежити за справністю ізоляції електромережі та мережевих кабелів, не допускаючи їхньої експлуатації з пошкодженою ізоляцією;

– не тягнути за мережевий кабель, щоб витягти вилку з розетки;

– не закривати меблями, різноманітним інвентарем вимикачі, штепсельні розетки;

– не підключа4ти одночасно декілька потужних електропристроїв до однієї розетки, що може викликати надмірне нагрівання провідників, руйнування їхньої ізоляції, розплавлення і загоряння полімерних матеріалів;

– не залишати включені електроприлади без нагляду;

– не допускати потрапляння всередину електроприладів крізь вентиляційні отвори рідин або металевих предметів, а також не закривати їх та підтримувати в належній чистоті, щоб уникнути перегрівання та займання приладу;

– не ставити на електроприлади матеріали, які можуть під дією теплоти, що виділяється, загорітися (канцелярські товари, сувенірну продукцію тощо).

5.3.2 Електробезпека

Основним небезпечним фактором при роботі з ЕОМ є небезпека ураження людини електричним струмом, яка посилюється тим, що органи чуття людини не можуть на відстані виявити наявність електричної напруги на обладнанні.

Проходячи через тіло людини, електричний струм чинить на нього складний вплив, що є сукупністю термічної (нагрів тканин і біологічних середовищ), електролітичної (розкладання крові і плазми) і біологічної (роздратування і збудження нервових волокон та інших органів тканин організму) дій.

Тяжкість ураження людини електричним струмом залежить від цілого ряду чинників:

1) значення сили струму;

2) електричного опору тіла людини і тривалості протікання через нього струму;

3) типу і частоти струму;

4) індивідуальних властивостей людини і навколишнього середовища.

Приміщення для ЕОМ відноситься до приміщень без підвищеної небезпеки, тобто в приміщення, в яких відсутні умови, що створюють підвищену або особливу небезпеку. Небезпека ураження електричним струмом існує всюди, де використовуються електроустановки, тому приміщення без підвищеної небезпеки не можна назвати безпечними.

Електробезпека забезпечується:

1) відповідною конструкцією електроустановок;

2) застосуванням технічних способів і засобів захисту;

3) організаційними і технічними заходами.

Конструкція електроустановок відповідає умовам їх експлуатації та забезпечує захист персоналу від дотику до струмоведучих частин.

Основними технічними способами і засобами захисту від ураження електричним струмом, що використовуються окремо або в поєднанні один з одним, є:

1) захисне заземлення;

2) занулення;

3) вирівнювання потенціалів;

4) мале напруга;

5) електричне поділ мереж;

6) захисне відключення;

7) ізоляція струмоведучих частин;

8) компенсація струмів замикання на землю;

9) захисні пристрої;

10) попереджувальна сигналізація, блокування, знаки безпеки;

11) ізолюючі захисні та запобіжні пристосування.

5.3.3 Мікроклімат

Мікроклімат робочих приміщень – це клімат внутрішнього середовища цих приміщень, що визначається діючої на організм людини з'єднанням температури, вологості, швидкості переміщення повітря. В даному приміщенні проводяться роботи, що виконуються сидячи і не потребують динамічного фізичного напруження, то для нього відповідає категорія робіт Іа. Отже оптимальні значення для температури, відносної вологості й рухливості повітря для зазначеного робочого місця відповідають ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень» [15] і наведені в таблиці 5.3.

Таблиця 5.3 – Норми мікроклімату робочої зони об’єкту

Період рок	Температура, ^{o}C	Відносна вологість,%	Швидкість вітру, м/с, не більше
Холодний	21 - 23	60 – 40	0.1
Теплий	22 - 24	60 - 40	0.2

5.3.4 Освітлення

Світло є природною умовою існування людини. Воно впливає на стан вищих психічних функцій і фізіологічні процеси в організмі. Хороше освітлення діє тонізуюче, створює гарний настрій, покращує протікання основних процесів вищої нервової діяльності.

Збільшення освітленості сприяє поліпшенню працездатності навіть в тих випадках, коли процес праці практично не залежить від зорового сприйняття. При поганому освітленні людина швидко втомлюється, працює менш продуктивна, виникає потенційна небезпека помилкових дій і нещасних випадків.

У проекті, що розробляється, передбачається використовувати суміщене освітлення. У світлий час доби використовуватиметься природне освітлення

приміщення через віконні отвори, в решту часу використовуватиметься штучне освітлення.

Штучне освітлення в робочому приміщенні передбачається здійснювати з використанням люмінесцентних джерел світла у світильниках загального освітлення, оскільки люмінесцентні лампи мають високу потужність (80 Вт), тривалий термін служби (до 10000 годин), спектральний складом випромінюваного світла, близький до сонячного. При експлуатації ПК виконується зорова робота IV в розряду точності (середня точність). При цьому нормована освітленість на робочому місці (Ен) рівна 200 лк. Джерелом природного освітлення є сонячне світло. У приміщенні, де розташовані ЕОМ передбачається природне бічне освітлення, рівень якого відповідає ДБН В.2.5-28:2018 Природне і штучне освітлення [17]

Регулярно повинен проводитися контроль освітленості, який підтверджує, що рівень освітленості задовольняє [17]

Розрахунок освітлення.

Для виробничих та адміністративних приміщень світловий коефіцієнт приймається не менше -1/8, в побутових – 1/10:

$$S_b = \left(\frac{1}{5} \div \frac{1}{10}\right) \cdot S_n \qquad (5.1)$$

де Sb – площа віконних прорізів, м2;

Sn – площа підлоги, м2.

Sn = a × b = 3 × 6 = 20 м2 ,

S = 1/8 × 20 = 2.5м2 .

Приймаємо 1 вікно площею S = 2.5м2. Світильники загального освітлення розташовуються над робочими поверхнями в рівномірно-прямокутному порядку. Для організації освітлення в темний час доби передбачається обладнати приміщення, довжина якого складає 4м, ширина 4м, світильниками ЛПО2П, оснащеними лампами типа ЛБ (дві по 80Вт) з світловим потоком

5400лм кожна. Розрахунок штучного освітлення виробляється по коефіцієнтах використання світлового потоку, яким визначається потік, необхідний для створення заданої освітленості при загальному рівномірному освітленні.

Розрахунок кількості світильників n визначається по формулі (4.10):

$$n = \frac{E \times S \times Z \times K}{F \times U \times M} \qquad (5.2)$$

Де Е нормована освітленість робочої поверхні, визначається нормами – 300лк;

S – освітлювана площа, м2; S = 20 м2;

Z – поправочний коефіцієнт світильника (Z = 1.15 для ламп розжарювання та ДРЛ;

Z = 1,1 для люмінесцентних ламп) приймаємо рівним 1.1;

K – коефіцієнт запасу, що враховує зниження освітленості в процесі експлуатації – 1.5;

U – коефіцієнт використання, залежний від типу світильника, показника індексу приміщення і т.п. – 0.575;

M – число люмінесцентних ламп в світильнику – 2;

F – світловий потік лампи – 5400лм (для ЛБ-80). Підставивши числові значення у формулу (4.10), отримуємо:

$$n = \frac{300 \times 20 \times 1.1 \times 1.5}{5400 \times 0.575 \times 2} \approx 1{,}6$$

Приймаємо освітлювальну установку, яка складається з 2-х світильників, які складаються з двох люмінесцентних ламп загальною потужністю 160Вт, напругою 220В.

5.3.5 Рекомендації щодо пожежної безпеки

Пожежна безпека при застосуванні ПК забезпечується:

– системою запобігання пожежі,

– системою протипожежного захисту,

– організаційно-технічними заходами.

Згідно ДСТУ Б В.1.1-36:2016 [18] таке приміщення, площею 25 м2, відноситься до категорії "В" (пожежонебезпечної) та для протипожежного захисту в ньому проектом передбачено устаткування автоматичною пожежною сигналізацією із застосуванням датчиків-сповіщувачів РІД-1 (сповіщувач димовий ізоляційний) в кількості 1 шт., і застосуванням первинних засобів пожежогасіння. Відповідно до норм первинних засобів пожежогасінні пропонується використовувати:

– ручний вуглекислий вогнегасник ОУ-5 в кількості 1 шт;

– повсть 1 1 м2, кошму 2×1,5 м2 або азбестове полотно 2×2 м2 в кількості 1 шт.

Виникнення пожежі можливе, якщо на об'єкті є горючі речовини, окислювач і джерела запалювання. Вірогідність пожежної небезпеки приймається значною, якщо ймовірна взаємодія цих трьох чинників. Горючими компонентами є: будівельні матеріали для акустичної і естетичної обробки приміщень, перегородки, підлоги, двері, ізоляція силових, сигнальних кабелів і т.д.

Горючими матеріалами в приміщенні, де розташовані ПК, є:

– поліамід – матеріал корпусу мікросхем, горюча речовина, температура самозаймання 420 ˚С,

– полівінілхлорид – ізоляційний матеріал, горюча речовина, температура запалювання 335˚С, температура самозаймання 530 ˚С,

– склотекстоліт ДЦ – матеріал друкарських плат, важкогорючий матеріал, показник горючості 1.74, не схильний до температурного самозаймання,

– пластикат кабельний №.489 – матеріал ізоляції кабелів, горючий матеріал, показник горючості більше 2.1,

– деревина – будівельний і обробний матеріал, з якого виготовлені меблі, горючий матеріал, показник горючості більше 2.1, температура запалювання 255 ℃, температура самозаймання 399 ˚С.

Для відводу теплоти від ПК діє система кондиціонування. Тому кисень, як окиснювач процесів горіння, є в будь-якій точці приміщень ВЦ.

Простори усередині приміщень в межах, яких можуть утворюватися або знаходиться пожежонебезпечні речовини і матеріали відповідно до [18] відносяться до пожежонебезпечної зони класу П-IIа. Це обумовлено тим, що в приміщенні знаходяться тверді горючі та важко займисті речовини та матеріали. Приміщенню, у якому розташоване робоче місце, присвоюється II ступень вогнестійкості.

Потенційними джерелами запалювання можуть бути:

– іскри і дуги короткого замикання;

– електрична іскра при замиканні і розмиканні ланцюгів;

– перегріви від тривалого перевантаження,

– відкритий вогонь і продукти горіння,

– наявність речовин, нагрітих вище за температуру самозаймання,

– розрядна статична електрика.

Причинами можливого загоряння і пожежі можуть бути:

– несправність електроустановки;

– конструктивні недоліки устаткування;

– коротке замикання в електричних мережах;

– запалювання горючих матеріалів, що знаходяться в безпосередній близькості від електроустановки.

Продуктами згорання, що виділяються на пожежі, є: окис вуглецю; сірчистий газ; окис азоту; синильна кислота; акромін; фосген; хлор і ін. При горінні пластмас, окрім звичних продуктів згорання, виділяються різні продукти термічного розкладання: хлорангідриді кислоти, формальдегіди,

хлористий водень, фосген, синильна кислота, аміак, фенол, ацетон, стирол. (ГОСТ 12.1.044-89) [19].

Для захисту персоналу від дії небезпечних і шкідливих чинників пожежі проектом передбачається застосування промислового протигаза, що фільтрує, з коробкою марки «В» із сірою відміткою забарвлення – захист від неорганічних газів (хлор, фтор, бром, сірководень, сірковуглець, хлорциан, галогени), а цей фільтр не захистить від СО (тобто від чадного газу).

Висновки до розділу 5

В результаті проведеної роботи було зроблено аналіз умов праці, шкідливих та небезпечних чинників, з якими стикається робітник. Було визначено параметри і певні характеристики приміщення для роботи над запропонованим проектом написаному в кваліфікаційній роботі, описано, які заходи потрібно зробити для того, щоб дане приміщення відповідало необхідним нормам і було комфортним і безпечним для робітника.

Приведені рекомендації щодо організації робочого місця, а також важливу інформацію щодо пожежної та електробезпеки. Були наведені розміри приміщення та наведено значення температури, вологості й рухливості повітря, необхідна кількість і потужність ламп та інші параметри, значення яких впливає на умови праці робітника, а також – наведені інструкції з охорони праці, техніки безпеки при роботі на комп’ютері.

ВИСНОВКИ

У даній роботі була спроектована високошвидкісна корпоративна комп'ютерна мережа стандарту Fast Ethernet для мережі офісів аптек ПП «Вітал».

Була обрана вита пара у якості кабельної системи як найбільш економічний вид кабелю.

При проектуванні локальної мережі використовувалася топологія типу «зірка». Велика перевага «зірки» (як активної, так і пасивної) полягає в тому, що всі точки підключення зібрані в одному місці. Це дозволяє легко контролювати роботу мережі, локалізувати несправності мережі шляхом простого відключення від центра тих або інших абонентів (що неможливо, наприклад, у випадку «шини»), а також обмежувати доступ сторонніх осіб до життєво важливих для мережі точок підключення.

Мережа була спроектована на основі програмного продукту OpenVPN. Перевага цього методу полягає в тому, що він забезпечує надійний захист інформації та швідку передачу даних.

Пропускна здатність мережі 100 Мбіт / с. Зіткнень даних не виникає.

Розроблена корпоративна мережа виконує наступні функції:

– створення єдиного інформаційного простору, який здатний охопити і застосовувати для всіх користувачів інформацію створену в різний час і під різними типами зберігання і обробки даних, контроль виконання робіт і обробки даних по ним;

– передає інформацію через VPN канали між офісами, це забезпечує захист усіх даних.

– забезпечує достовірність інформації та надійності її зберігання шляхом створення стійкої до збоїв і втрати інформації;

– забезпечує доступ користувачів до мережі Інтернет.

– задає можливість доступу до баз даних, файлового сервера і інтернету з периферійних робочих місць, що потребують інформації

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1) VPN (Virtual Private Network — віртуальна приватна мережа). URL: https://ru.wikipedia.org/wiki/VPN .
2) Корпоративна мережа URL: https://uk.wikipedia.org/wiki/Корпоративна_мережа .
3) Програма OPENVPN . URL: https://openvpn.net/ .
4) Технологія VPN URL: https://sites.google.com/site/zahistlokalnoiemerezi/zahist/virtualna-privatna-mereza .
5) Однорангова локальна мережа URL: https://ru.wikipedia.org/wiki/Одноранговая_сеть.
6) Локальна обчислювальна мережа типу клієнт-сервер. URL: https://ru.wikipedia.org/wiki/ Клиент_—_сервер .
7) Топології обчислювальних мереж URL: http://komseti.narod.ru/index.files/4.htm.
8) Мережеві кабелі URL:https://ru.wikipedia.org/wiki/Категория:Сетевые_кабели .
9) Маршрутизатор URL: https://ru.wikipedia.org/wiki/ Маршрутизатор.
10) Мережевий комутатор URL: https://ru.wikipedia.org/wiki/Сетевой_коммутатор .
11) Мережевий міст URL: https://ru.wikipedia.org/wiki/ Сетевой_мост.
12) NetCracker Professional URL: https://docplayer.ru/80742024Modelirovanie-kompyuternyh-setey-v-srede-netcracker-professional-4-1.html .
13) Методичні вказівки створення VPN серверу URL:https://www.youtube.com/watch?v=ZTnkEdggzPg .
14) Закон України «Про охорону праці». [Електронний ресурс] // Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/2694-12 (дата звернення 10.06.2019)

15) Санітарні норми мікроклімату виробничих приміщень ДСН 3.3.6.042-99.//Законодавство України. URL: [Електронний ресурс] https://zakon.rada.gov.ua/rada/show/va042282-99 (дата звернення 10.06.2019)
16) Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПІН 3.3.2.007-98. // Законодавство України. URL: [Електронний ресурс]https://zakon.rada.gov.ua/rada/show/v0007282-98 (дата звернення 10.06.2019)
17) Природне і штучне освітлення ДБН В.2.5-28:2018. [Електронний ресурс] https://dbn.co.ua/load/normativy/dbn/dbn_v_2_5_28/1-1-0-1188 (дата звернення 10.06.2019)
18) Визначення категорій приміщень, будинків, установок за вибухопожежною та пожежною небезпекою ДСТУ Б В.1.1-36:2016 2018. . // Державні будівельні норми. URL: [Електронний ресурс] https://dbn.co.ua/load/normativy/dstu/dstu_b_v_1_1_36/5-1-0-1759 (дата звернення 10.06.2019)
19) ГОСТ 12.1.044-892016 2018. . // Кодекс. URL: [Електронний ресурс] http://docs.cntd.ru/document/gost-12-1-044-89 (10.06.2019).

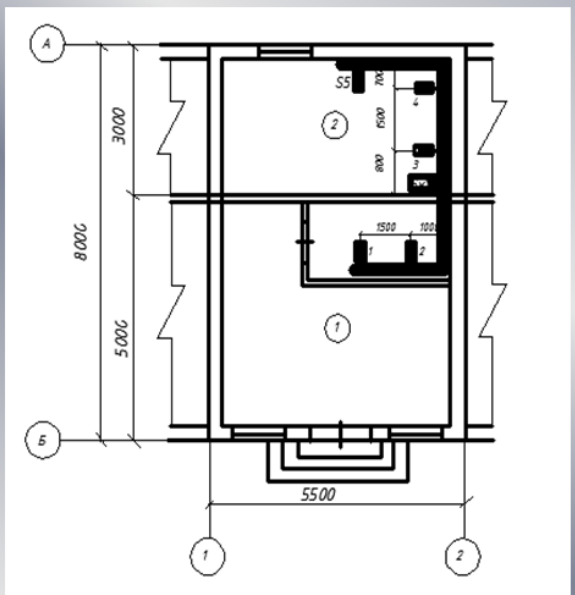
ДОДАТОК А ПРЕЗЕНТАЦІЯ

Мережа офісів аптек ПП "Вітал". Розробка корпоративної мережі на базі VPN.

Дипломант: Даниленко В.О.

Керівник: Барбарук Л.В.

СХЕМА ПРОКЛАДКИ КАБЕЛЬНИХ ТРАС (Офіс №1, офіс №2)



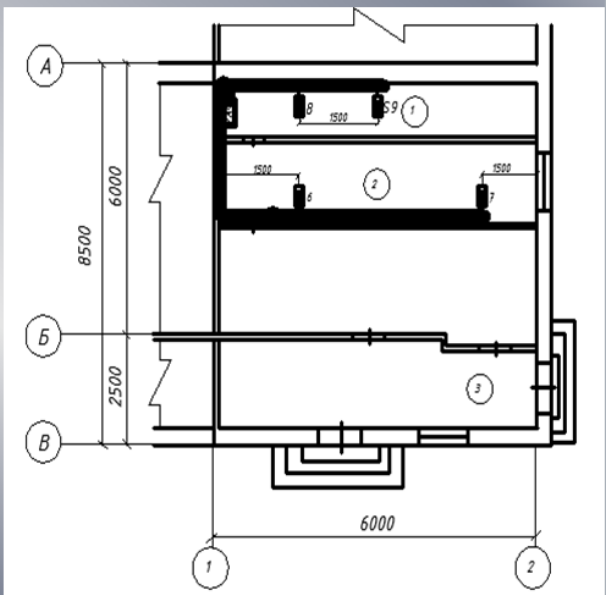
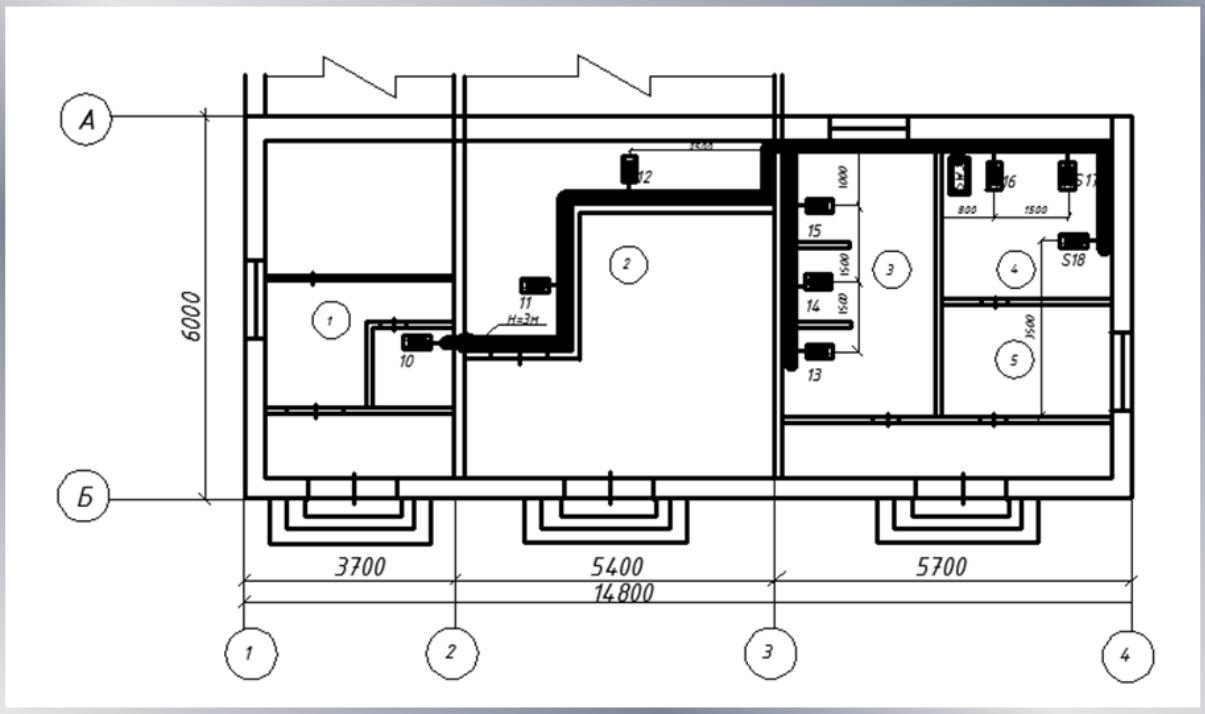
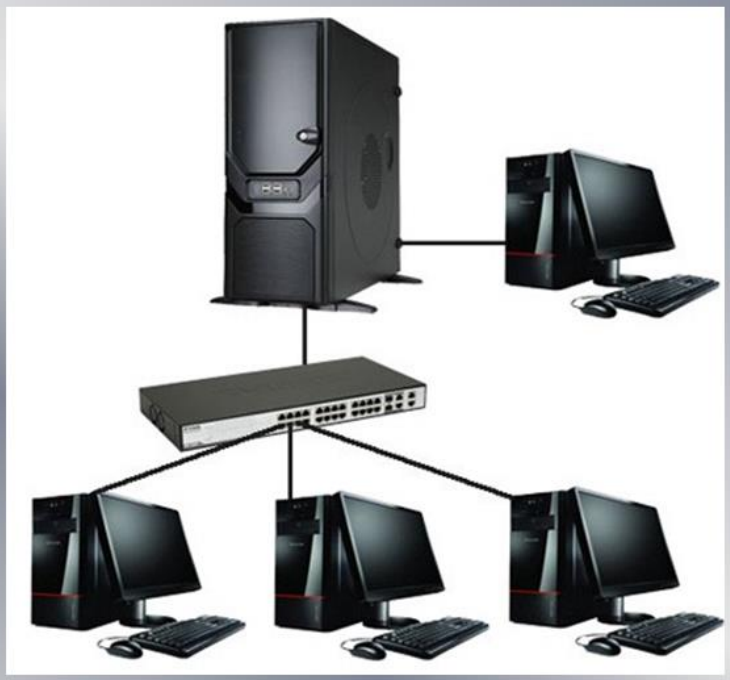


СХЕМА ПРОКЛАДКИ КАБЕЛЬНИХ ТРАС (Офіс №3)



ТОПОЛОГІЯ КОРПОРАТИВНОЇ МЕРЕЖІ

Топологія типу "Зірка"



Кабельне середовище мережі

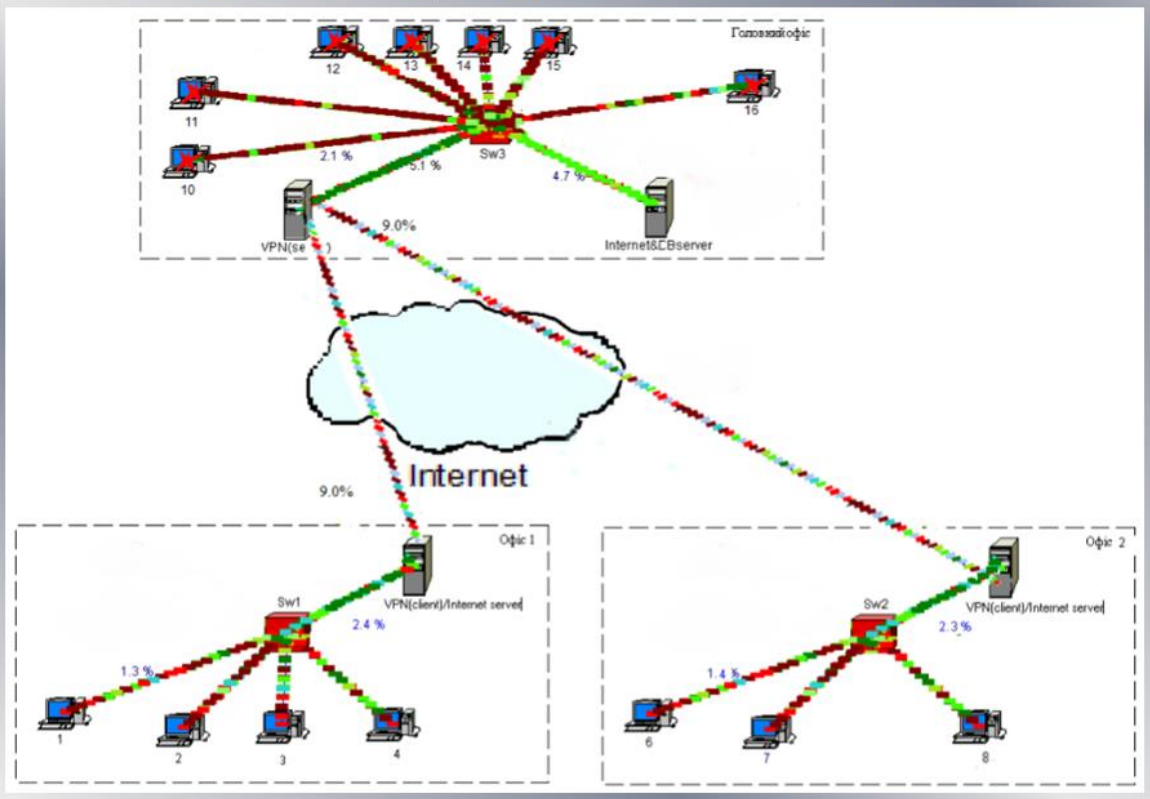
Кабель типу "вита пара" категорії 5е

Тип кабеля	UTP	
	Кат. 5	Кат. 6
Масса, кг/км	30-33	34-37
Внешний диаметр, мм	4.9	5.2
Рабочий диапазон температур, С	-20 - +60, +70	
Радиус изгиба, мм	30-35	

Необхідне обладнання для організації корпоративної мережі

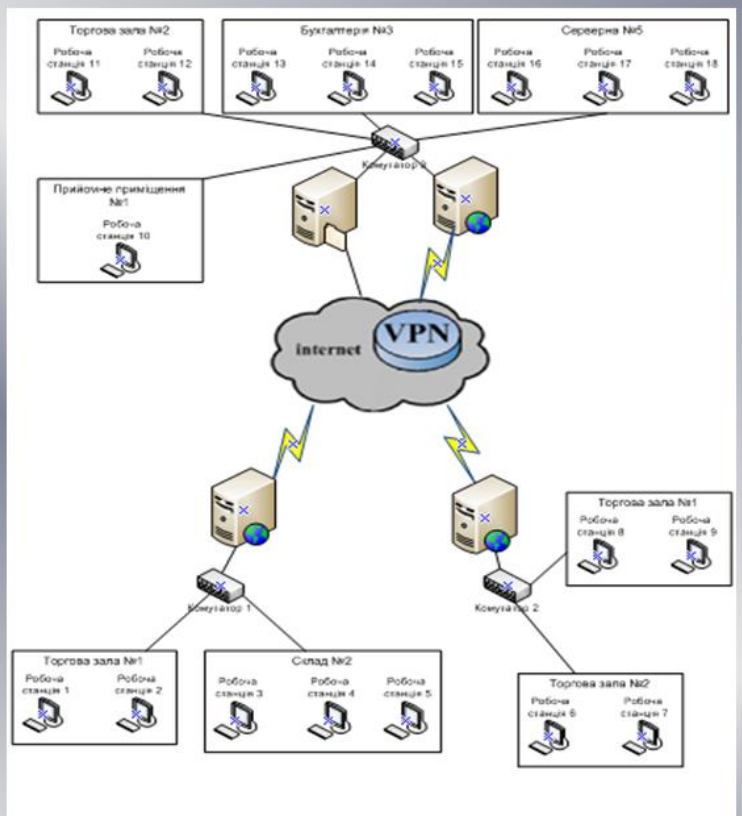
№	Обладнання	Кількість, шт.
1	Комутатор TP-LINK TL-SF1008D <8 Ports, 100 Mbit>	2
2	Комутатор TP-LINK TL-SF1016DS<16 Ports, 100 Mbit, RJ45>	1
3	Розетка RJ-45 (однопортова)	18
4	Патч-корд литий UTP5e/ RJ45 (1,0м)	18
5	Кабель UTP 5e	100
6	Короб з кришкою 40х16	44
7	Короб з кришкою 16х16	8
8	Конектори RJ-45	18

Модель корпоративної мережі



ГОРИЗОНТАЛЬНА КАБЕЛЬНА ПІДСИСТЕМА

Схема розташування сегментів мережі



Генерація основного сертифікату та ключа

```
Администратор: Командная строка
Microsoft Windows [Version 10.0.17134.765]
(c) Корпорация Майкрософт (Microsoft Corporation), 2018. Все права защищены.

C:\WINDOWS\system32>cd "C:\Program Files\OpenVPN\easy-rsa"

C:\Program Files\OpenVPN\easy-rsa>init-config.bat

C:\Program Files\OpenVPN\easy-rsa>copy vars.bat.sample vars.bat
Скопировано файлов:         1.

C:\Program Files\OpenVPN\easy-rsa>vars

C:\Program Files\OpenVPN\easy-rsa>clean-all
Скопировано файлов:         1.
Скопировано файлов:         1.
```

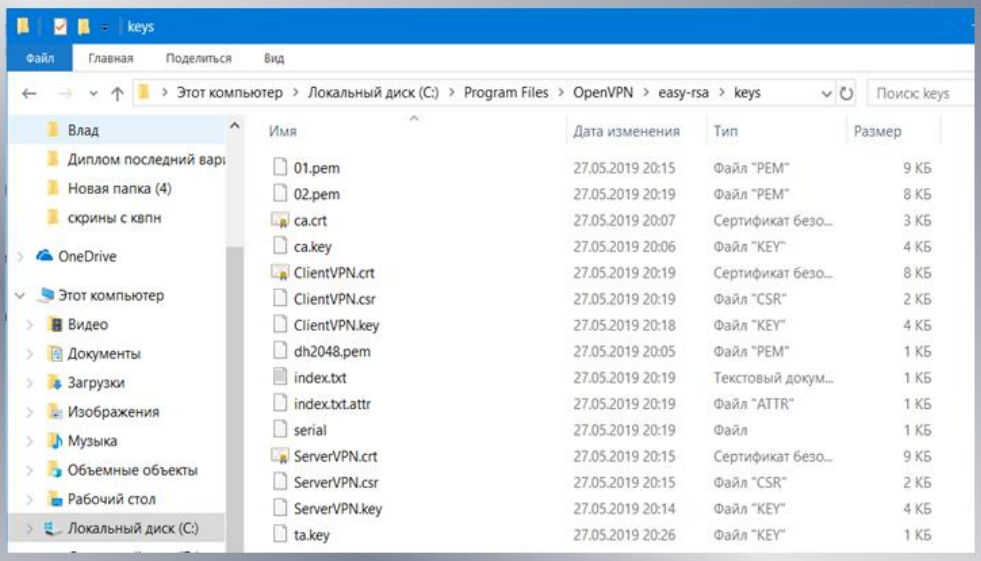
```
Администратор: Командная строка
.....+....+.....+.
.....
.....++*++*++*++*

C:\Program Files\OpenVPN\easy-rsa>build-ca
Generating a RSA private key
...++++
.....++++
writing new private key to 'keys\ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:
State or Province Name (full name) [CA]:UA
Locality Name (eg, city) [SanFrancisco]:Lg
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [changeme]:
Name [changeme]:
Email Address [mail@host.domain]:
```

Генерація сертифікатів та ключів для сервера та клієнта

```
Администратор: Командная строка
Name [changeme]:
Email Address [mail@host.domain]:

C:\Program Files\OpenVPN\easy-rsa>build-key-server ServerVPN
Generating a RSA private key
.....++++
.....++++
writing new private key to 'keys\ServerVPN.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:
State or Province Name (full name) [CA]:
Locality Name (eg, city) [SanFrancisco]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [changeme]:
Name [changeme]:
Email Address [mail@host.domain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from openssl-1.0.0.cnf
Can't open keys/index.txt.attr for reading, No such file or directory
6232:error:02001002:system library:fopen:No such file or directory:crypto/bio/bss_file.c:74:fo
```

```
Администратор: Командная строка
C:\Program Files\OpenVPN\easy-rsa>build-key ClientVPN
Generating a RSA private key
.....
.....
.....
.....++++
......++++
writing new private key to 'keys\ClientVPN.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:
State or Province Name (full name) [CA]:
Locality Name (eg, city) [SanFrancisco]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [changeme]:ClientVPN
Name [changeme]:
Email Address [mail@host.domain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
```

Конфігураційні файли



Налаштування брандмауера та маршрутизація

Для комп'ютерів головного офісу:

```
route -p add 192.168.1.0 mask 255.255.255.192 192.168.1.5
route -p add 192.168.1.64 mask 255.255.255.192 192.168.1.68
```

Для комп'ютерів першого офісу:

```
route -p add 192.168.1.64 mask 255.255.255.192 192.168.1.68
route -p add 192.168.1.128 mask 255.255.255.192 192.168.1.137
```

Для комп'ютерів другого офісу:

```
route -p add 192.168.1.0 mask 255.255.255.192 192.168.1.5
route -p add 192.168.1.128 mask 255.255.255.192 192.168.1.137
```