НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»
ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ФАХОВИЙ КОЛЕДЖ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

ПОЯСНЮВАЛЬНА ЗАПИСКА
до дипломної роботи
фахового молодшого бакалавра

на тему: **Проєкт локальної мережі для потреб приватного підприємства**

Виконав студент IV курсу, групи ТК-41
спеціальності 172 Телекомунікації та радіотехніка
ОПП «Телекомунікації та комп'ютерні технології»
Наконечний Юліан Володимирович

Керівник	_____ (підпис)	Людмила КРЕМПА
Нормоконтроль	_____ (підпис)	Володимир ПЛІШ
Рецензент	_____ (підпис)	Микола ЧИЖЕНЬКОВ
Голова ЕК	_____ (підпис)	Андрій ВАХ
Члени ЕК	_____ (підпис)	Ігор ТИБЕЛЬ
	_____ (підпис)	Володимир ПЛІШ

Дипломна робота захищена в ЕК «___» _____ 2025 р.

з оцінкою «_____»

Львів 2025

РЕФЕРАТ

Пояснювальна записка до дипломної роботи: 51 с., 12 рис., 14 табл. 10 джерел, 1 додаток.

Предметом дослідження є підприємство на прикладі компанії «*Lanet Network»*

Об'єкт дослідження – локальні комп'ютерні мережі.

Мета кваліфікаційної роботи – проектування локальної обчислювальної мережі, показати особливості локальної комп'ютерної мережі: структуру, класифікацію, призначення, топологію, технічну підтримку.

Методидослідження–аналітичнийтапрактичний.

Показані теоретичні і практичні сторони побудови локальної комп'ютерної мережі підприємства на прикладі компанії «*Lanet Network»*

Були проаналізовані літературні джерела на предмет класифікації локальних комп'ютерних мереж, запропоноване мережеве обладнання за відібраними характеристиками та надані рекомендації з налаштування для кожного з елементів локальної комп'ютерної мережі підприємства «*Lanet Network»*

Здійснено ознайомлення з інструментами для забезпечення захисту інформації та комерційної таємниці локальної мережі, а саме: брандмауери, проксі – сервери, VPN та протоколи. Проведена кількісна і якісна оцінка мережного обладнання, задля швидкого обміну даними між окремими підрозділами чи співробітниками та значної економії коштів.

ЛОКАЛЬНА МЕРЕЖА ЗВ'ЯЗКУ, LANET NETWORK, TP-LINK, МЕРЕЖА, МАРШРУТИЗАТОР, КОМУТАТОР, КОНЦЕНТРАТОР, ETHERNET, НАЛАШТУВАННЯ, СТРУКТУРОВАНА КАБЕЛЬНА СИСТЕМА, ТОПОЛОГІЯ МЕРЕЖІ, ПРОТОКОЛ, ЗАХИСТ ІНФОРМАЦІЇ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ВК – Вузол комунікації

ЛМ – Локальна мережа

СКС – Структурована кабельна система

ARP – Address Resolution Protocol BGP

BGP – Border Gateway Protocol

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

FTP – File Transfer Protocol

IEEE – Institute of Electrical and Electronics Engineers

IPSec – IP Security

IT – Information Technology

LAN – Local Area Network

MAC – Media Access Control

OSI – Open Systems Interconnection model

OSPF – Open Shortest Path First

PGP – Pretty Good Privacy

PPPoE – Point-to-point protocol over Ethernet

PPTP – Point-to-Point Tunneling Protocol

RIP – Routing Information Protocol

SSL – Secure Sockets Layer

TCP/IP – Transmission Control Protocol / Internet Protocol

TLS – Transport Layer Security

UI/UX – User Interface / User Experience

UTP – Unshielded Twisted Pair

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

WAN – Wide Area Network

WI-FI – Wireless Fidelity

ВСТУП

Поява та розвиток мереж дало новий, надійний і високоефективний метод взаємодії для людей. Так само, як і інші ресурси у сфері інформаційних технологій, мережі спочатку застосовувалися для наукових цілей, потім отримавши поширення у всіх галузях людської діяльності.

Темою кваліфікаційної роботи став процес проектування локальної обчислювальної мережі. Обрана тема актуальна, оскільки локальна мережа об'єднує деяку кількість комп'ютерів і дає можливість користувачам разом застосовувати ресурси комп'ютерів, а також приєднаних до мережі периферійних пристроїв (принтерів, плотерів, дисків, модемів).

Актуальність теми також визначається тим, що комп'ютерні мережі міцно зайшли в наше життя. Вони застосовуються буквально у всіх сферах життя: від вивчення до управління виробництвом, від розрахунків на біржі до домашньоїWI-FI мережі. З одного боку, вони є окремим випадком розподілених комп'ютерних систем, а з іншого - можуть розглядатися як засіб передачі інформації на гігантські відстані, для цього в них застосовуються способи кодування і мультиплексування даних, які отримали розвиток у різних телекомунікаційних системах.

Тому, в даній роботі розглядається проектування локальної мережі підприємства «*LanetNetwork»*

1 ВИБІР СТРУКТУРИ ТА ТОПОЛОГІЇ ОРГАНІЗАЦІЇ

1.1 Опис локальної мережі

Локальна мережа (ЛКМ) — це система обміну даними, що функціонує в межах однієї організації та перебуває під її повним контролем. Вона являє собою цілісну інформаційну інфраструктуру, яка забезпечує спільне використання ресурсів (програмного забезпечення, даних, периферійних пристроїв) і сприяє оптимізації бізнес-процесів.

Локальні мережі поділяються на:

- офісні (установчі) — використовуються у фірмах, освітніх закладах, установах управління;
- виробничі — для моніторингу та керування технологічними процесами на підприємствах.

У більшості випадків локальні мережі поєднують між собою персональні комп'ютери та робочі станції. Кожен вузол такої мережі оснащений власним процесором, що дозволяє самостійно виконувати обчислення, одночасно маючи доступ до спільних ресурсів. Це забезпечує ефективне використання принтерів, файлів, баз даних та іншого обладнання, а також дає змогу користувачам обмінюватися повідомленнями, листуватися через електронну пошту та спілкуватися в чатах.

В якості бази для проектування локальної мережі в дипломній роботі розглядається компанія «LanetNetwork» — українська сервісна компанія, яка надає технологічні рішення для міжнародного IT-сектора. Вона створює R\&D центри, формує спеціалізовані команди під проєкти клієнтів, а також надає офшорну та оншорну технічну підтримку.

Компанія спеціалізується на створенні сучасних програмних продуктів у таких напрямах:

- 3D-моделювання;
- штучний інтелект (AI);
- розробка мобільних додатків (App Development);

- електронна комерція (E-commerce);
- UI/UX-дизайн;
- аналіз даних (Data Analysis);
- машинне навчання (Machine Learning);
- наука про дані (Data Science).

Один із офісів «LanetNetwork» розташований у центральній частині Києва. Він займає три поверхи в адміністративній будівлі та включає 30 робочих місць. Проєктована локальна мережа охоплює весь офіс, забезпечуючи ефективну взаємодію працівників і високу продуктивність інформаційного середовища.

1.2 Структура локальних комп'ютерних мереж

Для побудови локальної комп’ютерної мережі (ЛКМ) необхідно забезпечити наявність кількох ключових компонентів: мережевих адаптерів (мережевих карт), фізичного середовища передавання (наприклад, кабелів) і відповідного програмного забезпечення. У рамках даної дипломної роботи структура ЛКМ розглядається з урахуванням таких основних ознак:

Топологія мережі — це геометричне розташування пристроїв та спосіб їх з’єднання. Найбільш поширені варіанти: «зірка», «шина», «кільце», а також ієрархічні структури. Вибір топології впливає на продуктивність, надійність і простоту обслуговування мережі.

Протоколи — це набір правил і стандартів, які регламентують обмін даними в мережі. Найпопулярнішим є Ethernet із застосуванням стека протоколів TCP/IP, що підтримує як клієнт-серверну, так і однорангову архітектури.

Фізичне середовище передачі (носій) — це тип кабелю або іншого з’єднувального середовища. До найпоширеніших належать вита пара (UTP), коаксіальний кабель та оптоволоконне з’єднання.

Мережеві інтерфейси реалізуються за допомогою мережевих карт, що встановлюються на материнські плати комп’ютерів. Їхні функції включають:

- забезпечення фізичного з’єднання з мережею;
- контроль за коректністю передавання та прийому даних;

– буферизацію трафіку;
– виявлення і попередження помилок та колізій;
– збирання даних для подальшої обробки системним програмним забезпеченням.

Доступ до ресурсів мережі здійснюється за мережевими іменами, які можуть бути прив’язані до певних фізичних або логічних адрес. При обміні даними часто використовується комутація каналів, за якої передача повідомлень відбувається через спеціалізовані вузли комунікації (ВК). Такі вузли можуть надавати пріоритетний доступ для певних категорій користувачів або трафіку.

Переваги побудови ЛКМ:
– невисока вартість підключення нових користувачів;
– легкість в адмініструванні та масштабуванні;
– можливість підключення/відключення пристроїв без зупинки всієї мережі.

Недоліки:
– залежність швидкості передавання від кількості активних користувачів і навантаження на мережу;
– надійність мережі прямо залежить від працездатності ВК;
– великі відстані між вузлами можуть знижувати ефективність використання фізичного середовища.

Для підвищення надійності вузли комутації будуються за модульним принципом із розділенням на основні та резервні блоки. Система автоматичної діагностики контролює стан обладнання і в разі збоїв перемикає навантаження на резервні модулі, забезпечуючи безперервну роботу мережі.

1.1 Класифікація локальних комп'ютерних мереж

Локальні комп'ютерні мережі можливо класифікувати за ознаками, які приведені в таблиці 1.1.

Таблиця1.1 – Класифікація локальних мереж

По ролі персонального комп’ютера у мережі	Мережі із сервером
	Одноранговi (рівноправні) мережі

По структур і(топології)мережі	Одно вузлові («зірка»)
	Магістральні («шина»)
	Кільцеві («кільце»)
	Комбіновані
За способом доступу користувачів до ресурсів та абонентів мережі	мережі з підключенням користувача за вказанимиадресамиабонентівзапринципом комутації каналів (зірка)
	мережі з централізованим (програмним) керуваннямпідключеннякористувачівдо мережі («кільце» та «шина»)
	мережі із випадковою дисципліною обслуговуваннякористувачів(«шина»)
За видом комунікаційного середовища передачі	Мережі із використанням існуючих установчих телефонних мереж
	Мережі на спеціально прокладених кабельних лініях зв'язку
	Комбіновані мережі, що поєднують кабельні лінії та радіоканали
З дисципліни обслуговування користувачів (спосіб доступу користувачів до мережі)	Пріоритетні, що задаються ЦУС, коли користувачі отримують доступ до мережі відповідно до пріоритетів
	Непріоритетні, коли всі користувачі мають рівні права доступу до мережі
З розміщення даних у компонентах мережі	З центральним банком даних
	З розподіленим банком даних
	З комбінованою системою розміщення даних

1.2 Топологія локальних мереж

Топологія комп’ютерної мережі (також відома як компонування, конфігурація або структура) — це спосіб фізичного розташування пристроїв у мережі та порядок їх з’єднання лініями зв’язку. Вона визначає, як саме вузли мережі взаємодіють між собою та передають дані.

Існують такі базові топології мережі:

Топологія «шина» (bus) — це тип мережевої архітектури, при якій усі комп’ютери та пристрої підключаються паралельно до одного спільного каналу передачі даних, тобто до єдиної лінії зв’язку. Така лінія виконує роль спільної магістралі, через яку передаються всі сигнали в мережі (рис. 1.1).

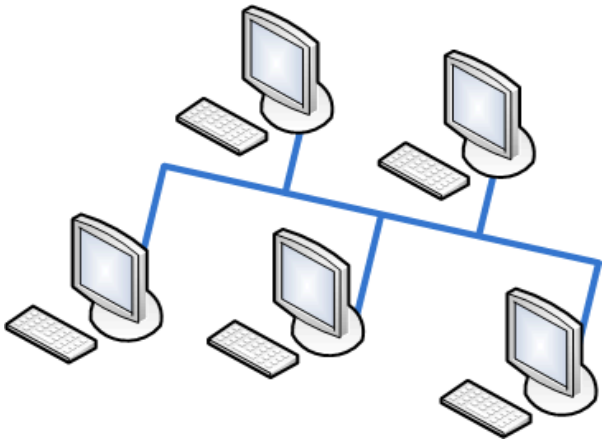

Рисунок1.1 – Мережна топологія шина

Зірка (star) – буває двох основних видів:

– активна зірка (справжня зірка) (рис. 1.2);

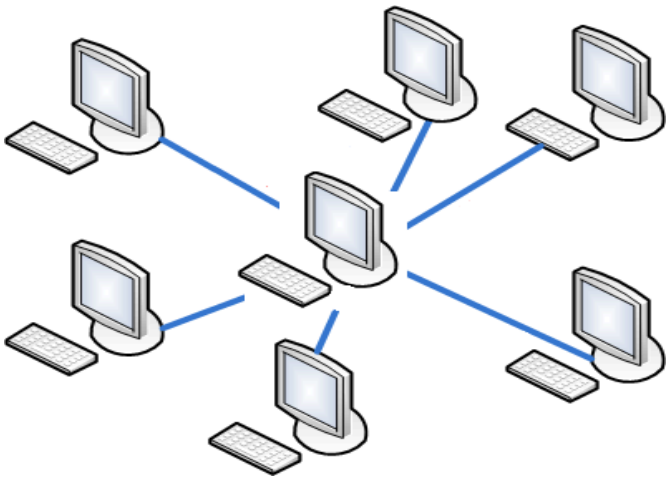

Рисунок 1.2 – Активна зірка

– пасивна зірка, яка зовні схожа на активну зірку (рис. 1.3).

У мережі з такою топологією центральним елементом є не комп’ютер, а спеціалізований мережевий пристрій — комутатор (switch), який відіграє ключову роль у передаванні даних між усіма підключеними вузлами (рис. 1.3). Саме через комутатор відбувається з’єднання всіх комп’ютерів, принтерів, серверів та інших пристроїв у єдину мережеву інфраструктуру.

Комутатор приймає пакети даних від одного пристрою і адресно надсилає їх

безпосередньо до отримувача, що значно підвищує ефективність роботи мережі. Завдяки цьому виключаються зайві перешкоди та зменшується кількість колізій, що є типовими для менш розумних пристроїв, таких як концентратори.

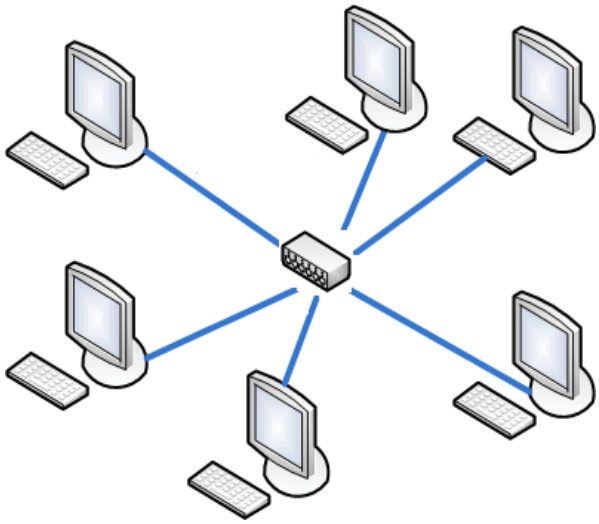

Рисунок1.3 – Пасивна зірка

Кільце (ring) - комп'ютери послідовно об'єднані в кільце (рис.1.4).

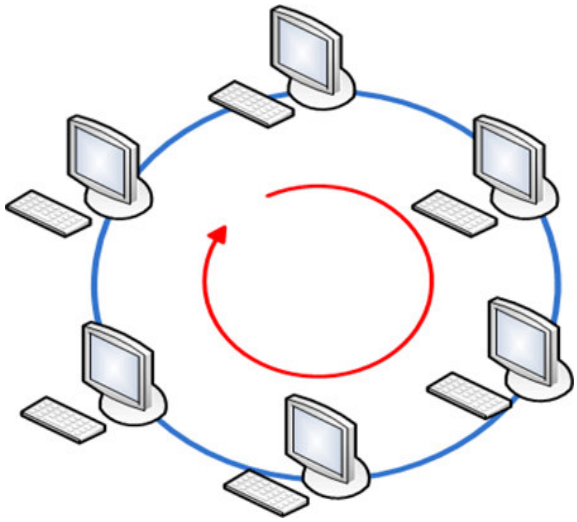

Рисунок 1.4 – Мережна топологія кільце

Термін «топологія», або «топологія мережі», визначає фізичне розташування кабелів, комп'ютерів та інших мережевих компонентів. Топологія мережі визначає її характеристики. Зокрема, вибір топології впливає на:

– складне обхідних мережевих пристроїв;

– характеристики мережевих пристроїв;

– можливості розширення мережі;

– спосіб управління мережею.

У нашому випадку топологія мережі – це «зірка». Концепція топології мережі «зірка» походить від мейнфрейма, де хост отримує та обробляє всі дані з периферійних пристроїв як активний вузол обробки. Цей принцип використовується в системах передачі даних. Вся інформація між двома периферійними робочими станціями проходить через центральний вузол обчислювальної мережі.

Топологія «зірка» є найшвидшою з усіх топології обчислювальних мереж, оскільки передача даних між робочими станціями проходить через центральний вузол (з хорошою продуктивністю) на окремих лініях, які використовуються тільки цими робочими станціями. Частота запитів на передачу інформації від однієї станції до іншої низька порівняно з такою, що досягається в інших топологіях.

Мережа цієї топології просто модифікується. У такій мережі збій одного комп'ютера не впливає на інші комп'ютери мережі. Тільки комп’ютер, який вийшов з ладу, не зможе передавати або отримувати дані по мережі. Ця топологія мережі була обрана з наступних причин :

– досить велика кількість обслуговуваних робочих місць;

– розумна вартість мережі;

– така мережа забезпечує просте рішення в реалізації та експлуатації мережі;

– простота модифікації мережі при необхідності.

Ієрархічна топологія

Ієрархічна деревоподібна топологія – це тип мережевої структури, побудований на принципі вкладених топологій «зірка». У такій схемі один центральний комутатор (або кілька комутаторів) виконує роль кореня, до якого підключаються комутатори нижчих рівнів. До кожного з них, у свою чергу,

під'єднуються кінцеві пристрої – комп’ютери, принтери, сервери тощо.

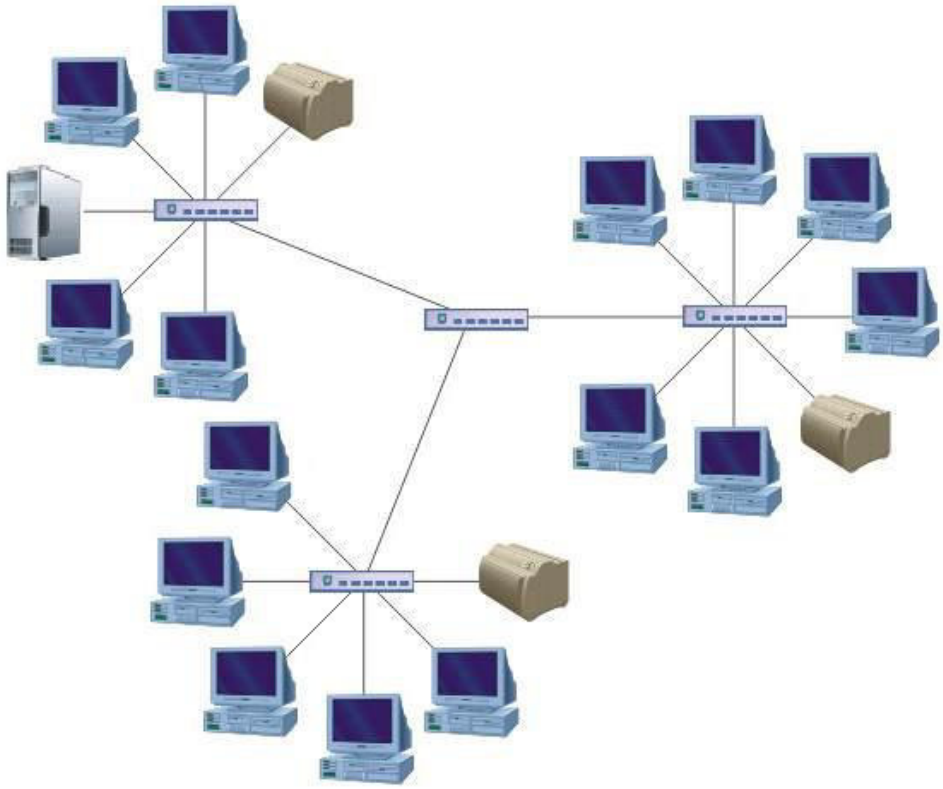

Рисунок 1.5 - Ієрархічна топологія

Цей підхід дозволяє ефективно організувати велику мережу з чіткою структурою, що легко масштабується. Ієрархічна топологія зменшує навантаження на центральний вузол, спрощує адміністрування та дозволяє ізолювати локальні збої — при виході з ладу одного вузла інші сегменти залишаються працездатними. Саме тому така топологія часто використовується в сучасних офісних, корпоративних та навчальних мережах.

2 СТРУКТУРОВАНА КАБЕЛЬНА СИСТЕМА

Структурована кабельна система (СКС) - це універсальна кабельна система корпусу, групи корпусів, розрахована на тривале використання без перебудови.

У СКС основні підсистеми:

– підсистема робочих груп.

Підсистема робочого простору призначена для підключення кінцевих користувачів (комп'ютерів, терміналів, принтерів, телефонів і т.д.) до інформаційної розетки. Включає комутаційні кабелі, адаптери, а пристрої, що дозволяють підключати кінцеве обладнання до мережі через інформаційну розетку. Робота СКС гарантує роботу саме підсистеми робочого простору.

– горизонтальна підсистема.

Горизонтальна підсистема покриває простір між інформаційною розеткою в робочому просторі та горизонтальним кросом у телекомунікаційній шафі. Вона складається з горизонтальних кабелів, інформаційних розеток та частини горизонтального кросу, що обслуговує горизонтальний кабель. Рекомендується обслуговувати кожен поверх будівлі власною персональною горизонтальною підсистемою.

Усі горизонтальні кабелі, незалежно від типу середовища передачі, не повинні перевищувати 90 м ділянці від інформаційної розетки робочому просторі до горизонтального кроса. На кожне робоче місце необхідно прокласти щонайменше 2 горизонтальні кабелі.

Схема одного з поверхів будівлі компанії (рис. 2.1). Приблизна кількість витої пари – 240 метрів на поверх. Використовується вита пара 5 категорії (UTP 5e) і технологія FastEthernet (з урахуванням можливості розвитку). Було використано 2 комутатори на 5 робочих груп, щоб заощадити обладнання. Для робочих груп застосовується топологію «зірка» з комутатором у центрі. Дана схемарозробленазурахуваннямвластивихїйособливостейконструкції.Кабелі Будуть проходити вздовж стіни в спеціально відведених каналах. Кабель тягнеться на верхні поверхи біля сходового отвору.

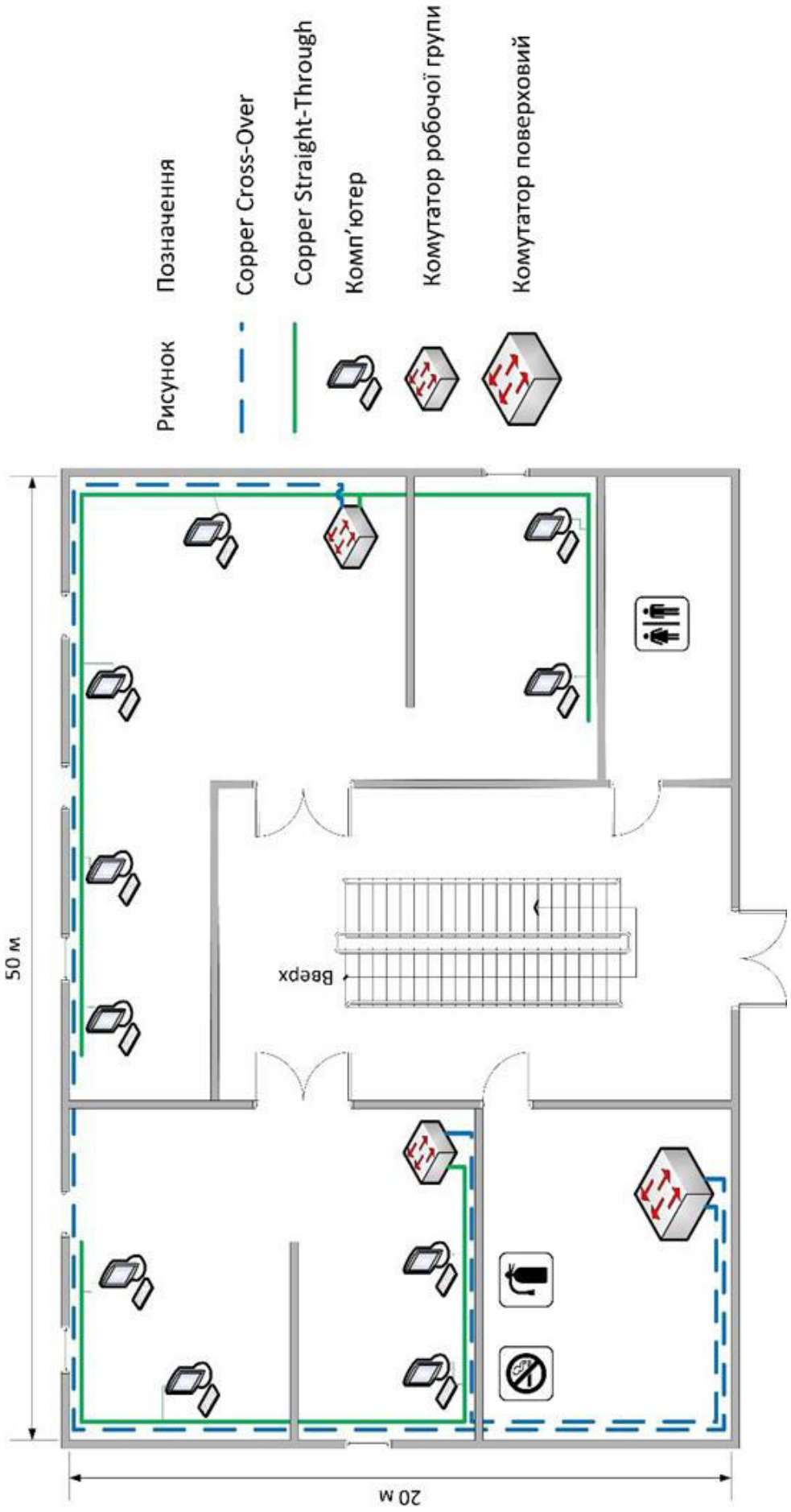

Рисунок 2.1 – Організація поверхів–вертикальна підсистема

Це невід’ємна частина СКС, яка забезпечує розподіл магістральних кабельних ліній по всій будівлі. Її призначення, як правило, полягає в з’єднанні горизонтальних підсистем між собою та з обладнанням та підсистемами адміністрування (з’єднання поверхових розподільних пунктів). Вертикальна підсистема базується на багатопарних неекранованих мідних та оптичнихкабелях. Вертикальна підсистема також включає супутнє обладнання, що використовується для прокладки кабелю через будівлю.

Схема будівлі офісу компанії «*LanetNetwork*»(рис.2.2). Орієнтовна кількість витої пари в 3-поверховому корпусі — 730 метрів. Використовується вита пара 5е-ої категорії (UTP 5e). Комутатори з'єднані між собою за допомогою 100BASE-TX, використовується технологія FastEthernet (з у рахуванням перспективи розвитку).

Топологія «зірка» використовується для з'єднання горизонтальних підсистем один з одним. Для побудови вертикальної підсистеми використовується комутатор 3 рівня OSI.

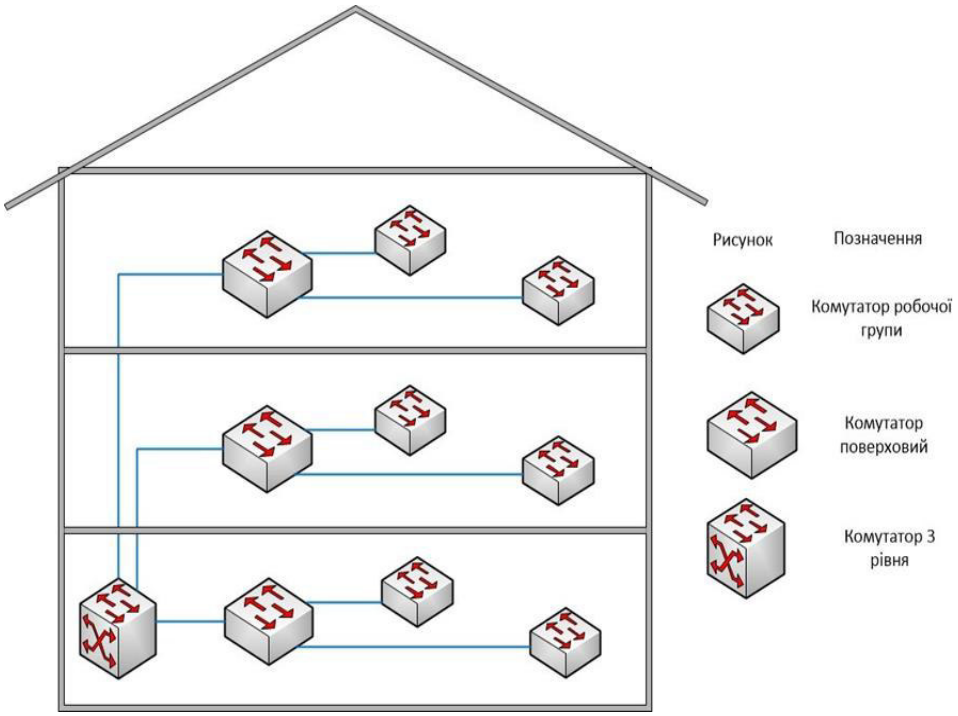

Рисунок 2.2 – Організація мережі будівлі

3 ВИБІР МЕРЕЖНОГО ОБЛАДНАННЯ

3.1 Критерії до вибору мережного обладнання

Вибір мережного обладнання,такого як комутатори і маршрутизатори в організації ЛМЗ, залежить від наступних умов:

– необхідна швидкість передачі даних;

– канальна технологія,що використовується в робочих,горизонтальних, вертикальних та базових підсистемах;

– простота і зручність регулювання;

– співвідношення ціни та якості.

3.2 Опис необхідного обладнання

Для побудови локальної мережі офісу ІТ підприємства я обрав мережне обладнання фірми TP-Link.

Компанія заснована у 1996 році в місті Шеньчжень. Засновниками (засновниками) є два брати ЧжаоЦзяньцзюнь та ЧжаоЦзясін. Назва TP-Link є скороченням від "TwistedPair" – кручена пара, "link" – з'єднання. Згодом TP почали трактувати як Trust and Performance .

2005року вийшла на світовий ринок. У 2007 році було відкрито представництва компанії в Сінгапурі та Індії. У 2008 році відкрито офіси в США та Німеччині. У 2011 році відкрито офіси в Польщі та в Україні .

ПродуктиTP-Linkвключаютьвисокошвидкіснікабельнімодеми,бездротові маршрутизатори, мобільні телефони, ADSL, розширювачі діапазону, маршрутизатори, комутатори, IP-камери та інші пристрої. TP-Link також виготовила маршрутизатор OnHub для Google. У 2016 році компанія запустила новий бренд Neffos для смартфонів. TP-Link виробляє пристрої розумного дому в рамках своїх ліній продуктів KasaSmart і Tapo. TP-Link є однією з небагатьох великих компаній з бездротових мереж, яка виробляє свою продукцію власноруч, на відміну від аутсорсингу виробників оригінального дизайну (ODM). У компанії стверджують, що такий контроль над компонентами та ланцюгом поставок є ключовою конкурентною відмінністю.

Маршрутизатор

Маршрутизатор TP-LINK Archer C5400X (рис.3.1).

Рисунок 3.1 – Зовнішній вигляд маршрутизатора

TP-LINK Archer C5400X оснащений 1.8 ГГц 64-бітним чотирьохядерним процесором, 3 співпроцесорами та 1 ГБоперативної пам'яті, забезпечує максимум потужності всім додаткам, онлайн-сервісам, а також виключає можливість затримки під час роботи.

Основні характеристики обладнання перелічені в табл. 3.1.

Таблиця3.1– Характеристики маршрутизатора TP-LINKArcher C5400X

Характеристики бездротової мережі	
СтандартWi-Fi5	IEEE802.11ac/n/a5ГГц IEEE802.11n/b/g2,4ГГц
ШвидкістьWi-FiAC5400	5ГГц:2167Мбіт/с (802.11ac) 5ГГц:2167Мбіт/с (802.11ac) 2,4ГГц:1000Мбіт/с (802.11n)
Тип антени	Зовнішня/Незнімна
Кількість антен	8
Захист інформації	WPA,WEP,EAP
Характеристики провідної мережі	

Вхідний інтерфейс (WAN)	10/100/1000BASE-TEthernet(MDI/MDIX)
Процесор	Чотирьохядерний 64-розрядний процесор 1,8 ГГц
КількістьWAN портів	1 шт.
КількістьLANпортів	8 шт.
Дод. порти і роз'єми	2 порта USB3.0
Підтримувані файлові системи	NTFS, exFAT, HFS+, FAT32
Підтримувані функції	Apple Time Machine FTP-сервер Мультимедійний сервер СерверSamba
Безпека	
Шифрування Wi-Fi	WEP WPA WPA2 WPA/WPA2-Enterprise(802.1x)
Мережева безпека	Міжмережевий екран SPI Управління доступом Прив'язка IP- та MAC-адрес Шлюз прикладного рівня
Антивірус HomeCare	Виявлення шкідливих сайтів Запобігання вторгненням у порт Ізоляція заражених пристроїв Повідомлення та логи
VPN-сервер	OpenVPN PPTP
Програмні характеристики	
Протоколи	IPv4 IPv6
Батьківський контроль HomeCare	Профілі, що настроюються Фільтрування контенту Блокування програм Фільтрування URL-адрес Обмеження часу, що проводиться у мережі Робота з розкладом (час сну) Детальна статистика
Типи WAN	Динамічний IP Статичний IP PPPoE, PPTP, L2TP

Хмарний сервіс	Автооновлення прошивки TP-LinkID , DDNS
Прокидання NAT	Перекидання портів Port Triggering DMZ, UPnP
IPTV	IGMP Proxy IGMP Snooping Міст ТегуванняVLAN
DHCP	Резервування адрес Список клієнтів DHCP, Сервер
DDNS	TP-Link NO-IP, DynDNS
Фізичні характеристики	
Ширина	288 мм
Висота	288 мм
Глибина	184 мм
Додаткові характеристики	
Комплектпоставки	Wi-FipoутерArcherC5400X Адаптер живлення Кабель Ethernet RJ45 Посібник із швидкого налаштування

Міжповерховий мережевий комутатор (switch)

Мережевий комутаторTP-LinkTL-SG1016D(рис.3.2).

Рисунок 3.2 – Зовнішній вигляд комутатора

16–портовий гігабітний комутатор TP-Link TL-SG1016D є доступним і високопродуктивним пристроєм, призначеним для вдосконалення мережі до гігабітних швидкостей. Всі 16 портів підтримують функцію авто-MDI/MDIX. Застосування інноваційної енергозберігаючої технології дозволяє зберігати до

25% споживаної електроенергії, а 80% пакувального матеріалу може бути повторно перероблено, завдяки чому пристрій є екологічним рішенням для мережі.

Основні характеристики обладнання перелічені в табл. 3.2.

Таблиця3.2 – Характеристики мережного комутатора TP-LinkTL-SG1016D

Характеристики	
Інтерфейси	16 портів 10/100/1000 Мбіт/с з автоузгодженням, з роз'ємами RJ45 (авто-MDI/MDIX)
Стандартита протоколи	IEEE802.3i, IEEE802.3u, IEEE802.3ab, IEEE802.3x
Середовище передачі даних	10Base-T: неекранована кручена пара категорій 3, 4, 5 (макс. 100 м)
	100Base-Tx: неекранована кручена пара категорій 5, 5e (макс. 100 м)
	1000Base-T: неекранована кручена пара категорій 5, 5e (макс. 100 м)
Джерело живлення	100-240 V AC,50/60 Hz
Енергоспоживання	Максимум: 9,26 Вт (220 В/50 Гц)
Розміри (ШхДхВ)	294 x 180 x 44 мм
Швидкість передачі пакетів	238 млн.пакетіву сек.
Таблиця MAC-адрес	8000 записів
Кадри Jumbo	10 Кбайт
Метод передачі	Store-and-Forward (Зберігання та передача)
Сертифікація	FCC,CE,RoHS
Комплектпоставки	16-портовийгігабітний. Настільний/монтований у стійку комутатор. Кабель живлення Інструкціякористувача Комплектдеталейдлямонтажуу стійку Гумовініжки
Комутаційна здатність	32 Гбіт/с

Мережевий комутатор поверху

Мережний комутаторTP-LINKTL-SG1024(рис.3.3).

Рисунок 3.3 – Зовнішній вигляд комутатора

24-портовий гігабітний комутатор TL-SG1024 підтримує останні енергозберігаючі технології, за допомогою яких можливо збільшити пропускну спроможність мережі зі значно меншими енерговитратами. Пристрійавтоматично вибирає режим живлення залежно від статусу з'єднання та довжини кабелю для того, щоб зберегти електроенергію і тим самим обмежити кількість викидів вуглецю, що здійснюються під час її вироблення.

Завдяки використанню неблокуючої архітектури комутатор TL-SG1024 може передавати та фільтрувати пакети на максимально можливій длямережевого середовища швидкості для забезпечення максимальної пропускної здатності. Таблиця MAC-адрес на 8000 записів забезпечує хорошу масштабованість навіть великих мереж. Комутатор також підтримує контроль потоку IEEE802.3хдляповнодуплексного режиму та контроль зворотного потоку для напівдуплексного режиму, щоб уникнути перевантажень та забезпечення надійної передачі даних.

Основні характеристики обладнання перелічені в табл. 3.3.

Таблиця3.3 – Характеристики мережевого комутатора TP-LINKT1700G-28TQ

Апаратні характеристики	
Стандартиі протоколи	IEEE802.3i, IEEE802.3u, IEEE802.3ab, IEEE 802.3x
Інтерфейс	24 портів 10/100/1000Мбіт/с з автоузгодженням, з роз'ємами RJ45 (авто-MDI/MDIX)

Середовищепередачіданих	10BASE-T:UTP (неекранована кручена пара) кабель категорії 3, 4, 5 (макс. 100 м)
	100BASE-TX/1000Base-T:UTP (неекранована кручена пара) кабель категорії 5, 5е або вище (макс. 100 м)
Джерело живлення	100~240 перем.струму,50/60Гц
Енергоспоживання	Максимум:14,6Вт(220В/50Гц)
Розміри(Ш×Д×В)	440*180*44 мм
Максимальне енергоспоживання	13.08Вт(220В/50Гц)
Продуктивність	
Комутаційна здатність	48 Гбіт/с
Швидкість передачі пакетів	35,7мільйонів пакетівз а секунду
Таблиця MAC-адрес	8000 записів
Кадри jumbo	10 Кбайт
QoS	802.1p/DSCPQoS*
Метод передачі	Store-and-Forward (Зберігання та передача)

Некерований комутатор сегменту

Комутатор некерований TP-LINKTL-SG1218MP (рис.3.4)

Рисунок 3.4– Зовнішній вигляд комутатора

TP-Link TL-SG1218MP – 18-портовий гігабітний комутатор із 16 портами PoE+. Універсальний продуктивний PoE-комутатор із Plug and Play. TL-SG1218MP повністю сумісний з пристроями PoE (IP-камерами, IP-телефонами, точками доступу тощо) та з пристроями без PoE (комп'ютерами, принтерами та

IPTV).

Основні характеристики обладнання перелічені в табл. 3.4.

Таблиця3.4 – Характеристики комутатора некерованого TP-LINKTL-SG1218MP

Апаратне забезпечення	
Інтерфейси	16 гігабітних портів RJ45PoE+ 2 гігабітні комбо RJ45/SFP-слоти
Стандартита протоколи	IEEE802.3, IEEE802.3u, IEEE802.3ab, IEEE 802.3x, IEEE 802.3af, IEEE 802.3at, IEEE 802.1q, IEEE 802.1p
Середовище передачі даних	10BASE-T: неекранована кручена пара
	Категорій 3, 4, 5(макс. 100м)
	EIA/TIA-568100 Ом екранована кручена пара (макс. 100 м)
	100BASE-TX: неекранована кручена пара категорій 5, 5e (макс. 100 м)
	EIA/TIA-568100 Ом екранована кручена пара (макс. 100 м)
	1000BASE-T: неекранована кручена пара категорій 5, 5e, 6 або вище (макс. 100 м)
	EIA/TIA-568100 Ом екранована кручена пара (макс. 100 м)
	1000BASE-XMMF, SMF
Джерело живлення	100–240В змінногоструму, 50/60Гц
ПортиPoE+(RJ45)	Стандарти: 802.3at/802.3af Порти PoE: 1–16 Бюджет PoE:250Вт
Розміри(Ш×Д×В)	440×180×44 мм
Максимальне енергоспоживання	21,4 Вт (220В/50 Гц, без підключених пристроїв живлення) 286,64 Вт (220В / 50Гц, з підключеними пристроями живлення 250 Вт)
Продуктивність	
Комутаційна матриця	36 Гбіт /с
Швидкість передачі пакетів	26,78 млн. пакетів засекунду
Таблиця MAC-адрес	8K записів

Додатковіфункції	Сумісність із пристроями стандартуIEEE 802.3at/af. Пріоритизація (QoS) 802.1p/DHCP. Автовизначення та запам'ятовування, а також автовидалення старих MAC-адрес. Керування потоком IEEE802.3x для режиму повного дуплексу та зворотний тиск (Backpressure) для режиму напівдуплексу.

Мережевий кабель

Кабель FTP cat.5e CCAVK cable, 305м (рис. 3.5).

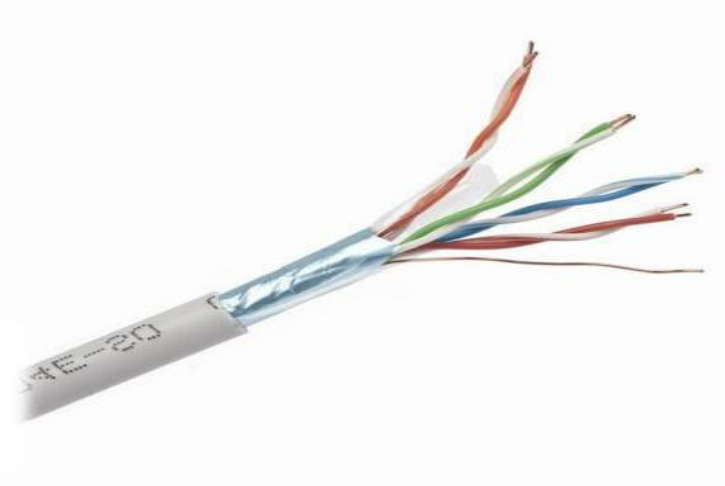

Рисунок3.5 – Зовнішній вигляд кабелю

4-парний FTP-кабель категорії 5e призначений для використання в локальних мережах передачі даних: PBX, V.11, X.21, ISDN, Ethernet (10Base-T), ATM-25/52/155 Мбіт/с, 100VG -AnyLAN, FastEthernet (100BASE-TX), TokenRing 16/100 Мбіт/с, GigabitEthernet (1000BASE-T), Firewire 100 Мбіт/с.

Кабель призначений для стаціонарної прокладки в телефонних каналах, в трубах, в колекторах, уздовж зовнішніх і внутрішніх стін будівель. Особливістю даного типу кабелю є використання алюмінієвих жил, покритих міддю, що значно знижує вартість кабелю.

Кабельскладаєтьсяз4парпровідників,скрученихразом.Алюмінієві(CCA) провідники, покриті міддю, провід 24 AWG. Ізоляція провідника - поліетилен високої щільності. Пари провідників розташовані в загальному щиті з алюмінієвої

фольги,під яким прокладається додатковий заземлювач. Зовнішня оболонка кабелю виготовлена з поліетилену сірого кольору, стабілізованого до ультрафіолету.

Основні характеристики кабелю перелічені в табл. 3.5

Таблиця3.5 – Характеристики кабелю для передачі даних по мережі

Виробник	EMT(Китай)
Умовний тип дроту	Мережний
Марка	FTP
Ступінь горючості	Не визначено
Матеріал жили	Алюміній
Конструкція жили	Монолітний
Форма	Круглий
Кількістьжил	8
Перетин	0,5мм²
Екранування	Екранований
Чим екранується кабель	Алюмінієва фольга
Матеріал зовнішньої оболонки	PVC
Категорія	cat5e
Колір	Сірий

3.3 Безпека локальної мережі

Під терміном безпека ми можемо розуміти не стан, а постійний процес, у якому прагнемо досягти і підтримувати задовільну безпеку мережі. Безпека локальних мереж – це дуже велика проблема, яка охоплює цілу низку відносно окремих областей. До них відносяться шифрування даних, брандмауери та загальна політика безпеки організацій.

В даний час все більше і більше дослідників аналізують різні аспекти вразливості у популярних протоколах, сподіваючись знайти рішення до того, як відбудеться масова атака. Правильно, що у комп'ютерних мережах є високіризики безпеки. Атаки залежать від використовуваних технологій. Основні цілі атак:

– перехоплення даних;

– обмін даними;

– доступ до мережі;

– переповнення мережі.

У бізнес-середовищі основною метою зловмисника може бути отримання недоступної інформації, яка може бути використана не за призначенням. У домашньому середовищі зловмисник має намір з'ясувати, що користувачі шукають в Інтернеті, отримати паролі або електронні листи. Види загроз мережевих атак постійно розвиваються.

Сніфінг – це процес перехоплення повідомлень у мережі. У локальній мережі зловмисники використовують спеціальні реалізовані налаштування мережевої карти в нерозбірливому режимі, що забезпечить отримання всіх повідомлень. Це спрощує захоплення, збереження чи інше використання будь-яких мережевих з'єднань. Зловмисники використовують спеціальні інструменти, звані сніфером, для перехоплення пакетів даних, що містять конфіденційну інформацію, таку як паролі, інформацію про банківські рахунки тощо. Деякі мережеві сніфери працюють тільки з пакетами TCP/IP, але складніші інструменти можуть працювати з багатьма іншими мережевими протоколами на нижчих рівнях, включаючи кадри Ethernet. Сніфер пакетів також використовується адміністраторами мережі для діагностики проблем, пов'язаних з мережею, наприклад, для ідентифікації пристрою, який не відповів на запит мережі. У провідній мережі дані, що збираються, залежать від мережевої структури. Сніфер пакетів може бачити трафік у всій мережі або лише в одному сегменті. Це залежить від того, як налаштовані та розміщені мережеві комутатори. У бездротовій мережі сніфер пакетів зазвичай може захоплювати лише один канал в даний момент часу. Якщо пакет вже захоплений, сніфер пакетів повинен проаналізувати та подати його у формі, доступній для читання зловмиснику. Людина, яка аналізує дані, може переглядати деталі зв'язку між двома або більше вузлами мережі.

Є багато способів захистити мережу та дані від зловмисників. Якщо

мережевий адміністратор хоче знати, чи використовує хтось у мережі сніфер, він може використовувати інструмент Antisniff. Цей інструмент може визначити,чи не переведено мережний інтерфейс у нерозбірливий режим. Інший спосіб захистити мережевий трафік від прослуховування – використовувати шифрування, таке як SSL або Transport Layer Security (TLS) .

Що стосується локальної мережі, загроза безпеки на будь-якому комп'ютері, заснована на конкретній атаці в локальній мережі, завжди походить від зламаного комп'ютера. Найпоширеніша атака – це спуфінг ARP, це також називається отруєнням ARP, маршрутизацією отруєння ARP або отруєнням кеша ARP. Він відноситься до атак Man-In-The-Middle (MITM). Як випливає з назви, в атаці MITM зловмисник намагається потрапити між двома пристроями, що взаємодіють, в мережі. Таким чином, зловмисник може захоплювати, аналізувати та змінювати всі повідомлення з обох пристроїв.

Ще одна можлива атака – це MAC-лавинне розсилання, яке дозволяє захоплювати конфіденційні дані з мережі або після перевантаження комутатора закривати з'єднання. Зловмисник може перехопити повідомлення та виконати атаку MITM. Атака з перехопленням портів також небезпечна, як і лавинна адресація MAC. Він використовує недоліки протоколу ARP, щоб ввести комутатор в оману. Атака з заміною DHCP також відноситься до групи атак MITM. Принцип атаки полягає у зловживанні протоколом процесу розподілу мережевого протоколу DHCP. Спочатку зловмисник повинен налаштувати фіктивний DHCP-сервер (шахрайський DHCP-сервер). Цей тип сервера не під контролем мережевихадміністраторів. Наприклад, підробний пристрій може бути бездротовим маршрутизатором із функціями DHCP, за допомогою якого зловмисник може підключитися до мережі. Сервери Rouge DHCP зазвичай використовуються зловмисниками для мережевих атак, таких як MITM, сніффінг та розвідувальні атаки. Зловмисник також може настроїти підроблений DNS-сервер для перенаправлення трафіку жертви на підроблені веб-сайти та запустити фітинговий скрипт. Ще одна можлива атака – підміна DNS. Після спуфінгу ARP спуфінг DNS є найпопулярнішим варіантом MITM атаки. Є й інші методи

спуфінгу DNS. Мета цього - стати жертвою підроблених веб-сайтів, фішингових веб-сайтів, які прагнуть отримати логін або особисті данііПід час DoS-атаки зловмисник зазвичай генерує багато безглуздого трафіку, такого як неповні TCP-з'єднання, пошкоджені IP-пакети, вимоги до веб-сайтів, створені роботами та інші ретельно відібрані методи. Це призводить до того, що служба або веб-сайт перестають працювати, і жертва не може користуватися ними. При успішній атаці нормальний сервіс або мережевий трафік порушується, і власник зазнає збитків.

Інструменти для запобігання атаки

Існує безліч інструментів та способів виявлення спуфінгу ARP. Зазначені інструменти зазвичай прості в установці і є добрим помічником для користувачів. Призначення засобів виявлення - попередити користувачів, що вони стали жертвою атаки. Недоліком є те, що такі інструменти лише інформують про реальну загрозу, але вони не можуть захистити нас від атаки. Якщо ми хочемо запобігти атаці, ми повинні зробити більш складні кроки, переважно шляхом правильної установки перемикача.

Для кожної операційної системи є інструменти, які допомагають виявляти атаки. Оскільки ми зосередилися на моделюванні атак MITM через Windows, ми вирішили використати інструмент, розроблений для вищезгаданої операційної системи. Цей інструмент називається XARPта сумісний з усіма версіями Windows. Інструмент регулярно перевіряє кеш ARP та порівнює його з тим, який запам'ятав. Якщо він додав ще один запис з новою IP-адресою, він запам'ятає його. Однак, якщо кеш ARP змінює MAC-адресу на IP-адресу, він інформує користувача про можливу атаку. Недоліком є те, що кожна станція має бути захищена, і якщо ми використовуємо DHCP-сервер, легко генеруються помилкові тривоги, тому що MAC-адреса може бути змінена з іншої причини. XARP включає чотири рівні безпеки. Користувач має можливість вибрати потрібний рівень.

Рекомендуємо вибирати базовий рівень. Якщо ми виберемо більш високий рівень безпеки, може статися так, що XARP часто необґрунтовано попереджатиме

нас. На ПК жертви ми запустили XARP до моделювання атаки ARP-спуфінгу. У списку ми можемо побачити записи, які визначають наші пристрої – маршрутизатор та комп'ютери зловмисників та жертви. Кожен запис містить IP- та MAC-адресу.

Найкращий захист – використання якісних керованих комутаторів. Наприклад, комутатори від Cisco, які мають функцію DAI. DAI заснований на захопленні всіх запитів та відповідей ARP та перевірці їхньої автентичності перед оновленням локального кеша ARP комутатора. Він аналізує пакети ARP у реальному часі та виключає ті, які визначені як неприпустимі чи небезпечні. Такий аналіз використовує базу даних дійсних IP-MAC-адрес, які можуть бути створені адміністраторами мережі вручну або динамічно за допомогою DHCP Snooping. Для великих мереж ми рекомендуємо використовувати комутатори з функцією перевірки пакетів ARP. Ми дозволили статичні елементи, повторно змоделювавши ARP-спуфінг, і можемо сказати, що успішно запобігли цій атаці .

В основному, безпека локальних мереж залежить від програмного забезпечення. До них належать:

– брандмауери (міжмережеві екрани). Це проміжні елементи комп’ютерної мережі, які служать для фільтрації вхідного та вихідного трафіку – знижується ризик несанкціонованого доступу до інформації;
– проксі–сервери. Обмежити маршрутизацію між WAN та LAN;
– VPN – вони дозволяють передавати інформацію по зашифрованим каналам;
– протоколи, які необхідні для створення безпечного з'єднання та встановлення контролю над елементами локальної мережі.

Мережний протокол – це набір правил, який дозволяє з'єднувати і обмінюватися даними між двома або більше комп'ютерами, включеними в мережу. Насправді різні протоколи часто описують лише різні сторони одного типукомунікації;разомвониутворюютьтакзванийстекпротоколів.Ціпрограми, вбудовані в операційну систему і спеціалізовані, шифрують дані. Існують протоколи інформаційної безпеки на прикладному рівні (протокол PGP), на транспортному рівні (протокол SSL/TLS), на рівні мережі (протокол IPSec).

PGP (Pretty Good Privacy) протокол безпеки інформації електронної пошти. Це протокол прикладного рівня, який не належить до мережі зв’язку (він належить до інформаційно-комунікаційної мережі).

PGP – це повний пакет для електронної пошти, що забезпечує конфіденційність повідомлень, аутентифікацію (автентичність джерела повідомлення та цілісність повідомлення за допомогою цифрового підпису). Хоча PGP є прикладним рівнем, аналіз у цьому розділі його алгоритмів безпеки служить для розуміння інших алгоритмів безпеки, які використовуються в мережах зв’язку.

SSL

Протокол SSL (Secure Sockets Layer) використовується для створення безпечного каналу зв'язку між комп'ютерами на основі TCP. Творцем протоколу є Netscape. SSL використовує асиметричне шифрування під час створення сеансу зв’язку та передачі ключів, але симетричне шифрування використовується під час передачі даних. Цей протокол використовує метод діалогу (рукостискання) підчас створення сеансу зв’язку (на рівні сеансу). При цьому сторони набувають впевненості в тому, з ким мають справу, і в тому, що не було заміни партнера на лінії зв'язку. На основі діалогу сторони формують загальний симетричний ключ для швидкої передачі даних.

TLS

Безпека транспортного рівня (TLS), стандартизована в RFC 2246. Цей механізм розташований як підрівень між транспортним і прикладним рівнями TCP/IP. TLS – це версія протоколу Security Sockets Layer (SSL). Сокет – це комбінація номера порту транспортного рівня та IP – адреси. Сокет однозначно ідентифікуєпроцесзастосуваннявІнтернеті.Перевагоювикористанняпротоколів інформаційної безпеки на рівні програми є можливість оптимальної побудови механізму захисту залежно від вимог конкретної програми. Перевага SSL / TLS полягає в тому, що він забезпечує прозорість безпеки для додатків.

IPSec

Протокол IPSec, механізми реалізації якого розташовані нижче

транспортного рівня еталонної моделі TCP/IP на мережевому рівні. Основною перевагою IPSec, який підтримує широкий спектр додатків, є можливість шифрування та аутентифікації всього потоку даних на рівні IP. Захист можна надати будь-якій програмі, тобто IPSec прозорий для програм.

Механізми захисту на рівні IP за допомогою протоколу IPSec забезпечують інформаційну безпеку не тільки для мережевих додатків, які мають власні вбудовані інструменти, але і для програм, які не мають таких можливостей.

Протокол IPSec забезпечує захист для обміну даними в різних комп'ютерних мережах: локальних, корпоративних і відкритих глобальних мережах, таких як Інтернет.

Протоколи маршрутизації RIP, OSPF і BGP вразливі до фальсифікації повідомлень між сусідніми маршрутизаторами. Зловмисник може видавати себеза новий або існуючий маршрутизатор. Відправляючи нелегітимні повідомлення про оновлення маршрутизації RIP або OSPF, він може порушити схему маршрутизації в мережі або направити частину трафіку в систему через свій комп’ютер,тобто зможе прослухати, змінити або знищити передані дані. До таких повідомлень, зокрема, належать повідомлення про нелегітимні оновлення маршрутизації RIP і OSPF на другому рівні, а BGP - на третьому рівні TCP/IP. Реалізація таких загроз інформаційній безпеці відноситься до таких атак, як відмова в обслуговуванні (DoS – Denial of Service). Протокол аутентифікації (автентичність джерела) повідомлень у RIP і OSPF визначається стандартом RFC- 2453івизначаєтьсяза допомогоюзвичайного пароля,якийпередається відкритим текстом. Такий захист слабкий, якщозловмисник має можливість прослуховувати мережу.

RFC-2082 визначає більш потужний механізм захисту - аутентифікацію повідомлень, що передбачає аутентифікацію джерела повідомлень між сусідніми маршрутизаторами, а також цілісність цих повідомлень (тобто автентичність їх отримання від джерела). Алгоритм такої аутентифікації такий. Секретний ключ додається до повідомлення про оновлення маршрутизації RIP, OSPF або BGP. Відправник генерує хеш-функцію відповідно до стандартизованого протоколу MD5 такого повідомлення в поєднанні з ключем. Хеш-функція є односторонньою

функцією і не може відновити вихідне повідомлення, що містить спільний ключ сусідніх маршрутизаторів. Повідомлення про оновлення маршрутизації разом із отриманою хеш-функцією пересилається одержувачу. Сам секретний ключ по мережі не передається. Одержувач виконує ту ж операцію: бере отримане повідомлення, додає до нього свою копію секретного ключа, обчислює хеш-функцію і порівнює результат з отриманою хеш-функцією. Якщо воно не збігається, то повідомлення відхиляється.

4 ЛОГІЧНА ОРГАНІЗАЦІЯ ЛКМ

Для розробки проекту необхідно уявити логічну структуру сформованої схеми ЛКМ організації з мережевим обладнанням.

Насамперед потрібно побудувати план розміщення комп'ютерів, маршрутизаторів, комутаторів та їх інтеграції. Для цього використаємо програмний комплекс відповідних пакетів програм моделювання – програму PacketTracer для моделювання мереж на базі обладнання CiscoSys. План розміщення обладнання представлений у Додатку А.

4.1 Розбиття мережі на під мережі на основі IP-адрес

Згідно з тим,що маємо офіс компанії «*LanetNetwork»*т о використаємо простір «сірих» IP-адресів: 192.168.0.0 (підмережа відповідає поверху).

Будинок офісу складається з 3 поверхів, тобто 3 підмережі, кількість вузлів 30.

Є мережа 192.168.0.0/24 і стоїть завдання отримати 3 мережі поменше. На 3 рівних не ділиться — можна на 2,4,8,16,32 і т.п У вихідній мережі два октету (192.168) є мережевою частиною IP адреси і два (0.0). Найпростішим варіантом розбиття буде збільшення префікса з /24 до /28. Таким чином, ми отримуємо в наше розпорядження весь третій октет. А саме указано в табл. 4.1.

Таблиця 4.1 – Адреса підмережі

Дім	Поверхи	Адреса під мережі та маска
1	1	192.168.0.0/28
	2	192.168.0.16/28
	3	192.168.0.32/28

4.2 Налаштування комутаторів і маршрутизаторів

4.2.1 Налаштування маршрутизатора в програмному інтерфейсі

На маршрутизаторі налаштовуємо один підінтерфейс з IP-адресою і маскою підмережі для кожної VLAN. Кожен підінтерфейс використовує інкапсуляцію

802.1Q:

– interface GigabitEthernet5/0.1;

– encapsulation dot 1Q10;

– ipaddress192.168.0.1255.255.255.240.

НалаштуванняDHCP:

– ввімкнення;

– service dhcp.

Оголошуємо пул та ім’я рідного домена;

– ipdhcppool1;

– network192.168.0.0255.255.255.240;

– default-router192.168.0.1;

– domain-namewrite.

– виключаємозпулу адреси;

– ipdhcpexcluded-address192.168.0.1;

– ipdhcpexcluded-address192.168.0.17;

– ipdhcpexcluded-address192.168.0.33.

4.2.2 Налаштування комутатора в програмному інтерфейсі

На домовому комутаторі 3 рівня прописуємо такі команди:

– налаштування статичного транка до поверхових комутаторів;

– interface FastEthernet0/1;

– switch port trunk encapsulation dot 1q;

– switch port mode trunk.

– налаштування адрес VLAN;

– ipaddress192.168.0.1255.255.255.240.

– налаштування статичного транка до маршрутизатора.

– interface GigabitEthernet0/1;

– switch port trunk encapsulation dot 1q;

– switch port mode trunk.

На поверховому комутаторі прописуємо наступні команди:

– налаштування статичного транка додомовогокомутатора3рівня;

– interface FastEthernet0/1;

– switch port mode trunk.

Налаштування access портів; Призначення порту комутаторавVLAN:

– interface FastEthernet0/2;

– switch port access vlan60;

– switch port mode access.

4.3 Використані канальні технології

В якості канальних технологій використовувалися FastEthernet та Gigabit Ethernet.

Технологія Fast Ethernet є спадкоємицею класичної технології Ethernet. Її основними перевагами є:

– збільшення пропускної здатності сегментів мережі до100Мб/с;

– збереження методу довільного доступу Ethernet;

– збереження зірчастої топології мережі обслуговування традиційних засобів передачі даних – витої пари і волоконно-оптичного кабелю.

Ці параметри дозволяють здійснити поступовий перехід від мереж10Base-T. Найпопулярнішого варіанту Ethernet на сьогоднішній день – до високошвидкісної мережі,яка зберігає значну безперервність з добре відомою технологією: FastEthernet не вимагає фундаментальної перепідготовки персоналу та заміни обладнання на всіх вузлах мережі. Офіційний стандарт 100Base-T (802.3u) встановлює три різні специфікації для фізичного рівня (з точки зору семирівневої моделі OSI) для підтримки наступних типів кабельних систем :

- 100Base-TX для двохпарного кабелю на неекранованої витої пари UTP категорії 5, або екранованої витої пари STP Type 1;
- 100Base-T4 для чотирьохпарного кабелю UTP категорії 3, 4 або 5 неекранованої витої пари;
- 100Base-FX для багатоходового волоконно-оптичного кабелю.

Технологія Gigabit Ethernet є подальшим розвитком стандартів 802.3 для

мереж Ethernet з пропускною здатністю 10 і 100 Мбіт/с. Основна мета GigabitEthernet – значно збільшити швидкість передачі даних, зберігаючи сумісність із існуючими мережами на основі Ethernet. Необхідно забезпечити можливість передачі даних між сегментами, що працюють з різною швидкістю, що, крім іншого, дало б можливість спростити архітектуру існуючих мостів і комутаторів, що використовуються у великих промислових мережах.

Мережа Gigabit Ethernet підтримує той самий метод повнодуплексного доступу, який зарекомендував себе у Fast Ethernet, і використовує ті самі формати пакетів (кадрів) та їх розміри. Не потрібно перетворення протоколу для з'єднань Ethernet і Fast Ethernet. Єдине, що потрібно, це координація обмінних курсів.

З появою надшвидкісних серверів і поширенням найсучасніших персональних комп'ютерів високого класу переваги Gigabit Ethernet стають все більш очевидними. Таким чином, 64-розрядна системна шина PCI, яка вже є стандартом де-факто, повністю забезпечує швидкість передачі даних, необхідну для такої мережі. В даний час номенклатура сегментів мережі Gigabit Ethernet включаєтакітипи:

- 1000BASE-SX– сегмент на багатоходовому волоконно-оптичному кабелі з довжиною хвилі світлового сигналу 850 нм (довжиною до 550 метрів);
- 1000BASE-LX – сегмент на багатомодовому (до 550 метрів) і одномодовому (до 5000 метрів) волоконно-оптичному кабелі з довжиною хвилі світлового сигналу 1300 нм;
- 1000BASE-CX – сегмент на екранованій витій парі (до 25 метрів) - на практиці практично не реалізований;
- 1000BASE-T (стандарт IEEE 802.3ab) — відрізок на зчетвереній неекранованій витій парі категорії 5 (до 100 метрів). Передача здійснюється по кожній парі в обох напрямках.

5 ТЕХНІКО-ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ

Серед положень технічного завдання дипломної роботи було вказано техніко-економічну доцільність, отже вибір раціонального мережевого обладнання із багатьох критеріїв.

Обладнання було обране із урахуванням:

- наявності необхідних нам характеристик обладнання;
- його вартості;
- вартість використання та обслуговування;
- якості та надійності.

Загальна вартість обладнання, без урахування кабелів, роз'ємів та кабельних якорів:

Таблиця 5.1 — Вартість мережевого обладнання

Мережеве обладнання	Кількість, шт	Вартість за шт.	Разом
МаршрутизаторTP-LINKArcherC5400X	4	1 166,00 грн	4 664,00 грн
Мережевий комутатор TP-LinkTL-SG1016D	1	1 449,00 грн	1 449,00 грн
Мережний комутатор TP-LINKTL-SG1024	1	1 299,00 грн	1 299,00 грн
Сервер ARTLINE Business T24 v01	1	26 454,00 грн	26 454,00 грн
Мережева карта Frime PCI-E x1 GigabitEthernet RTL8111C	2	229,00 грн	448,00 грн
		Всього:	34314,00 грн

Для складання кошторису посивного обладнання необхідно провести обрахунок довжини кабелів, монтажних коробів та кількості роз'ємів. Для цього було добавлено розміри кімнат та насічки на схемі, аби можна було зручно порахувати довжину кабелів та монтажних коробів(рис. 5.1).

Результатом приблизного обчислення довжини потрібних кабелів було отримано загальне число — 220,5 м кабелю FTP 5e (рис. 5.2), що складається з:

- 1– поверх – 57 м;
- 2– поверх – 53 м;

– 3– поверх – 65 м;

– з’єднання комутатора – 45,5 м.

Спершу слід згадати, що ці обчислення є зовсім приблизними. Для того, аби гарантувати, що нам вистачить кабелю, нам слід купувати кабель із запасом по довжині. Найкраще підходили для цього вибору кабелю одного виробника Vinga (рис. 5.3):

– бухта 305м кабелю мідного (3 999,00 грн.).

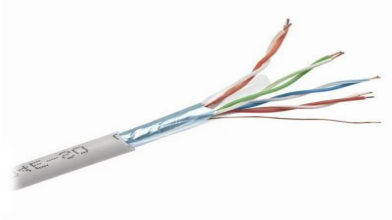

Рисунок 5.2 – Кабель FTP cat.5e CCAVKCABLE,

Рисунок 5.3– Бухта 305 м мережевого кабелю FTP cat. 5e CCA VKCABLE

За приблизними підрахунками загальна довжина монтажного короба становить 70м. А саме:

– 1– поверх — 14м;

– 2– поверх — 17м;

– 3– поверх — 20м;

– з’єднання комутатора — 19м.

Розуміючи, що слід купити монтажний короб із запасною довжиною, помножимо це число на 1,5. Тоді варто закупити — 70м × 1,5 = 105 м монтажного коробу.

При виборі монтажного короба необхідно зважати на його ширину, адже у ньому повинні вміститись ті кабелі, які ми збираємось помістити у нього. Тож, зважаючи, що кабель матиме товщину близько 5мм, звернемо увагу до ділянки, де ми плануємо прокладати разом найбільше кабелів. Це 7 кабелів разом.

Простими математичними обчисленнями можна отримати результат, з якого ми можемо зробити висновок, що монтажний короб повинен бути щонайменше 4см аби можна було прикріпити всі кабелі на кліпси. Отже було обрано монтажний короб NeomaxUltra 40×25 (рис. 7.4), адже він оптимально підходить нам. Такий монтажний короб продається упаковками по 24 м за ціною 34,10 грн/м. Нам потрібно всього 4 повні упаковки та 9м.

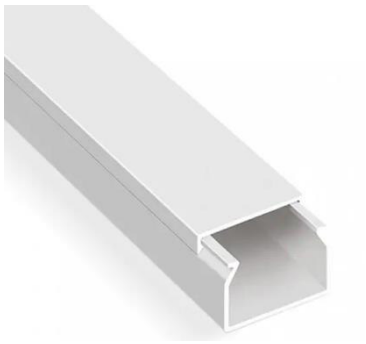

Рисунок 5.4 — Монтажний короб Neomax Ultra 40×25

Потрібно також обчислити кількість та загальну вартість роз’ємів RJ-45 (рис. 5.5). Отже, кількість таких роз’ємів становить кількості з’єднань цього інтерфейсу. За нашими підрахунками кількість таких з’єднань становить 78шт.

Проте, як було вказано вище, варто купити трохи більше, тобто “із запасом”. Нехай це буде пакет 100шт.(рис. 7.6).

Рисунок 5.5 – Роз’єм RJ-45

Рисунок 5.6 — Упаковка Vinga RJ-45 100 шт.

Таблиця 5.3 — Вартість пасивного обладнання.

Пасивне обладнання	Довжина, м /кількість, шт	Вартість за шт/м	Всього
Кабель FTP 5E CCAVKCABLE	305м	13,11грн	3 999,00 грн
Монтажний короб	105м	34,10 грн	3 580,00 грн
Роз’єм RJ-45	100шт	2,00 грн	200,00 грн
		Всього:	7 779,00 грн

Тепер, коли у нас є вартість різного обладнання, що нам потрібне, аби досягнути мети дипломної роботи, ми можемо узагальнити всю вартість проєкту на таблиці 5.4

Таблиця 5.4 – Загальна вартість усього обладнання

Мережеве обладнання	Пасивне обладнання	**Всього**
34 314,00 грн	7 779,00 грн	42 093,00 грн

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ

Приміщення, в яких планується установка та подальша робота з комп'ютерами , повинні відповідати проектній документації будинку, погодженій з уповноваженими державними органами. Крім того, роботодавець повинен враховувати чинні санітарні нормативи освітлення, вимоги до параметрів мікроклімату (температура, відносна вологість), ступеня і сили вібрації, звукового шуму і вогнестійкості приміщення, а також характеристики електромагнітного, ультрафіолетового та інфрачервоного полів.

Конкретні показники зазначених санітарних норм див. у ДСанПіН 3.3.2.007-98.

6.1 Вимоги щодо приміщення

Площа приміщень в кімнатах із робочими місцями за комп’ютерами повинна розраховуватись із максимальною кількістю не більше 12-и осіб та по 6 $м^2$ на робоче місце.

Природнє світло повинно бути переважно зліва.

Відстань між робочими місцями має бути принаймні 2 м.

Відстань між боковими поверхнями моніторів – не менше 1,2 м.

З урахуванням розмірів алфавітно–цифрових знаків і символів, екран монітора має знаходитись на відстані 400мм-800мм.

Робоче крісло повинно бути підйомно-поворотним та регулюватись щодо висоти і куту нахилу, а також куту нахилу спинки.

Висота поверхні сидіння має коригуватись в межах 260-460мм.

Столи повинні бути одномісні для роботи із персональними комп’ютерами.

Конструкція повинна передбачати:

Дві поверхні. Одна для розміщення монітору, а інша для розміщення клавіатури.

Ширина поверхонь повинна бути не менше 700мм і глибину не менше 600-800мм.

6.2 Освітлення

У кожному із приміщень повинно бути як штучне освітлення, так і природнє. Вікна повинні бути переважно орієнтовані на півнч та північний схід, обладнані жалюзями, занавісками, зовнішніми навісами тощо.

Освітленість повинна бути не менше 400 лк на робочих поверхнях, та не більше 200 лк освітлення на поверхні екранів моніторів.

Як штучні джерела освітлення доцільно застосовувати люмінісцентні лампи у приміщеннях з робочими місцями за комп'ютерами.

Використання світильників без розсіювачів та екрануючих решіток не допускається.

6.3 Мікроклімат

Приміщення із робочими місцями за комп'ютерами повинні бути обладнані засобами вентиляції або кондиціонером для забезпечення організованого повітрообміну.

Допускаються наступні параметри мікроклімату:

– Температура - 19,5±0,5 °С
– Відносна вологість повітря - 60±5 %
– Швидкість руху повітря не більше 0,1 м/с

Необхідними є щоденні вологі прибирання.

6.4 Заходи безпеки на робочому місці

Перед початком роботи необхідно:

– впорядкувати робоче місце;

– очистити екран відео терміналу від пилу та інших забруднень;

– відрегулювати освітленість на робочому місці, упевнитись в відсутності відбиття на екрані;

– упевнитись в наявності захисного заземлення та підключення екранного провідника до корпусів системного блока, відео терміналу;

-– включити комп'ютер.

Неприпустимими дії під час виконання роботи: зберігання біля відео термінала та ПК паперу, дискет, інших носіїв інформації; забороняється торкатися одночасно екрана монітора та клавіатури; торкатися задньої панелі системного блока при включеному живленні; переключати роз'єднувачі інтерфейсних кабелів периферійних пристроїв при включеному живленні; допускати потрапляння вологи на поверхню системного блоку, ВДТ, клавіатуру та інших пристроїв; самостійно відкривати та ремонтувати обладнання.

Після закінчення роботи :

– вимкнути електроживлення ПК у порядку, який встановлений Інструкцією користувача ПК;

– від'єднати шнури електроживлення та кабелів від електромережі;

– вимкнути вилку силового кабелю з розетки;

– прибрати робоче місце .

Аварійна ситуація:

– коротке замикання у мережі електроживлення обладнання з можливим загоранням;

– ураженням працівника електричним струмом.

При ураженні працівника електричним струмом відключити електромережу, звільнити потерпілого від контакту із струмовідними частинами, застосовуючи діелектричні захисні засоби.

Оживлення організму необхідно проводити до повного відновлення дихання потерпілим або до прибуття лікаря.

Санітарно-гігієнічні вимоги

Працівник, який працює з ПК, постійно перебуває під впливом небезпечних та шкідливих виробничих факторів: електромагнітних полів, інфрачервоного та іонізуючого випромінювань, шуму і вібрації, статичної електрики. Крім цього, працівник піддається значному розумовому та психоемоційному навантаженню, напрузі зорової та м'язової діяльності.

Впродовж робочої зміни передбачено перерви для відпочинку та вживання їжі (обідні перерви). Через кожні дві години роботи за ВДТ передбачається 15

хвилин на перерва для відпочинку очей. Для психологічного розвантаження працівників, що виконують роботи з обслуговуванням ПК, створена кімнатах психологічного розвантаження під час регламентованих перерв, або наприкінці робочого дня.

Ергономіка та виробнича естетика робочого місця

Організація робочого місця передбачає: правильне розташування робочого місця у виробничому приміщенні; вибір виробничих меблів; раціональне компонування комп'ютерного обладнання на робочому місці; урахування характеру та особливостей трудової діяльності.

Конструкція робочого місця користувача відео терміналу забезпечує підтримання оптимальної робочої пози з такими ергономічними характеристиками: ступні ніг - на підлозі або на підставці для ніг; стегна – в горизонтальній площині; передпліччя - вертикально; лікті - під кутом 70º–90º, до вертикальної площини; зап'ястя зігнуті під кутом не більше 20º, відносно горизонтальної площини, нахил голови – 15º–20º, відносно вертикальної площини.

Все вказане обладнання розміщується на основному робочому столі з лівого боку.

Висота робочої поверхні столу для відео терміналу 680–800мм, а ширина – забезпечує можливість виконання операцій в зоні досяжності моторного поля. Розміри столу: висота – 725мм, ширина – 600–1400мм, глибина – 800мм–1000мм. Робочий стіл для відео терміналу обладнаний підставкою для ніг шириною 400мм з можливістю регулювання по висоті. Підставка має рифлену поверхню та бортик на передньому краї заввишки 10 мм.

Робоче сидіння користувача відео терміналу та персональної ПК має такі основні елементи: сидіння, спинку та знімні підлокітники. Робоче сидіння є підйомно-поворотним, регулюється за висотою, кутом нахилу сидіння та спинки. Поверхня сидіння є плоскою, передній край -заокруглений.

Екран відео термінала розташовуються на оптимальній відстані від очей користувача (800 мм).

Розташування екрану відео терміналу забезпечує зручність зорового спостереження у вертикальній площині під кутом +30º від лінії зору працівника.

Клавіатура розміщена на спеціальній, регульованій за висотою, робочій поверхні окремо від столу на відстані 300мм від краю, ближчого до працівника. Кут нахилу клавіатури складає 10º.

Колір є найбільш ефективним засобом естетичного рівня виробничого інтер'єру. За допомогою кольору вирішуються питання: забезпечення психофізіологічного комфорту; емоційно-естетичний вплив на працівника.

На робочому місці стіни фарбують у світлий колір. Що сприяє працездатності працівника, зменшує втому очей.

Опалення та вентиляція

Приміщення обладнане системою опалення для підтримки температури повітря не нижче встановленої. Для приміщень з електронно-обчислювальною технікою передбачено центральне опалення. Застосовують кондиціювання на робочому місці, а також природне провітрювання.

Виробниче освітлення

Приміщення для обслуговування, ремонту та налагодження ПК має природне і штучне освітлення. Робоче місце з відео терміналом відносно світлових прорізів розміщується так, що природне світло падає збоку, переважно зліва, на відстані не менше 1 м від стін .

Природне світло проникає через бічні світлопрорізи, зорієнтовані на північ, і забезпечують коефіцієнт природної освітленості (КПО) не нижче 1,5 %. Вікна приміщення мають регулювальні пристрої для відкривання, а також жалюзі.

Загальне освітлення виконане у вигляді переривчатих ліній світильників, що розміщуються збоку від робочого місця, паралельно лінії зору працівника. На робочому місці застосовано світильники, що відносяться до класу Н (переважно прямого світла).

Яскравість світильників загального освітлення в зоні кутів випромінювання від 50º до 90º, відносно вертикалі в подовжній і поперечній площинах складає не більше 200 кд/м^2 , а захисний кут світильників є не більшим 40º.

Рівень освітленості на робочому столі є в межах 500 лк. Світильники місцевого освітлення мають напівпрозорий відбивач світла з захисним кутом 40º.

Захист від випромінювань

Електромагнітне випромінювання монітора відповідає нормам, а саме: напруженість змінного електричного поля не перевищує 10 В/м на відстані 0,3 м від центру екрану та 1 В/м при 0,5 м навколо монітора; напруженість змінного магнітного поля не перевищує 200 мА/м на відстані 0,3 м від центру екрану та 20 мА/м при 0,5 м навколо монітора.

Гранично допустима напруженість електростатичного поля на робочих місцях не повинна перевищувати рівнів, наведених в ДГСТ.

Захист від шуму та вібрації

Рівні шуму під час виконання робіт з ПК у виробничому приміщенні не перевищують 60 дБ.

На робочому місці присутня незначна вібрація, яка гаситься за рахунок віброізоляції. Віброізоляція реалізовується за допомогою спеціальної прокладки під системний блок, що послаблює передачу вібрацій робочому столу.

Вимоги до персоналу

Усі працівники, які виконують роботи, пов'язані з експлуатацією, обслуговуванням ПК, підлягають обов'язковому медичному огляду – попередньому під час оформлення на роботу та періодичному на протязі трудової діяльності .

Посадові особи та спеціалісти, інші працівники підприємств, які організовують та виконують роботи, пов'язані з експлуатацією ПК, проходять підготовку (підвищення кваліфікації), перевірку знань з охорони праці та питань пожежної безпеки. Допускати до роботи осіб, що в установленому порядку не пройшли навчання, інструктаж та перевірку знань з охорони праці та пожежної безпеки, забороняється.

Забороняється допускати осіб, молодших 18 років, до самостійних робіт в електроустановках та на електрообладнанні під час профілактичного обслуговування, налагодження, ремонту ПК .

До робіт з обслуговування ПК допускаються особи, що мають кваліфікаційну групу з електробезпеки не нижче П.

6.5 Протипожежний захист

Приміщення по вибухово-безпечній і протипожежній безпеці відноситься до категорії В.

Приміщення за ступенем вогнестійкості відноситься до 2 ступеню.

Протипожежний захист приміщення досягається застосуванням установок автоматичної пожежної сигналізації.

Система пожежної сигналізації складається з пожежних датчиків (пристроїв для формування сигналу про пожежу), які включені у сигнальну лінію (шлейф), приймально-контрольного приладу, ліній зв'язку.

Пожежні датчики перетворююсь прояви пожежі в електричний сигнал, який по лініях зв'язку надходить до контрольно-приймального приладу. Контрольно-приймальний прилад здійснює приймання інформації від пожежних датчиків, виробляє сигнал про виникнення пожежі чи несправності, передає цей сигнал. На підприємстві застосовуються димові датчики, які реагують на аерозольні продукти горіння. Як засіб пожежогасіння використовується вуглекислотний вогнегасник типу ВВ-2. Він знаходиться на видному місці та кріпиться на стіні спеціальним тримачем на висоті 1,5 м від підлоги. На робочому місці можливі причини пожеж неелектричного і електричного характеру. При прийнятті на роботу та щороку працівники проходять інструктаж з питань пожежної безпеки.

ВИСНОВКИ

У процесі виконання дипломної роботи на основі аналізу вихідних даних та загальних принципів проектування локальних мереж була розроблена мережа підприємства «*LanetNetwork»* Розроблена мережа включає в себе 1 будинок, у будівлі розташовано до 3 підрозділів, у кожному підрозділі до десяти робочих місць.

Підбір активного обладнання здійснювався відповідно до топології мережі, а також послідовності команд для налаштування активного обладнання. При виборі обладнання перевага надавалася техніці компанії TP-Link, як компанії, що виробляє сучасне обладнання в цій сфері, що відповідає показнику ціна–якість. Під час проектування використано таке обладнання: мережевий комутатор для будинку, мережевий комутатор для поверху, комутатор некерований для групи, маршрутизатор організації та кабель для передачі даних по мережі виробника VKcable.

У ході проекту були отримані знання про мережне обладнання, починаючи від комутаторів рівня доступу до маршрутизаторів рівня ядра. Було накопичено досвід налаштування цих пристроїв.

У роботі також були розглянуті такі важливі питання, як поняття локальної комп’ютерної мережі, її класифікація, структура, призначення, основні характеристики, топологія та технічне забезпечення, а також, безпека локальної мережі.

Розроблено схему адресації, яка передбачає можливе розширення мережі в майбутньому.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Комп'ютерні мережі: [навчальний посібник] / А. Г. Микитишин, М. М. Митник, П. Д. Стухляк, В. В. Пасічник. — Львів: «Магнолія 2006», 2013ю — 256 с. ISBN 978-617-574-087-3

2 Буров Є. В. Комп'ютерні мережі: підручник / Євген Вікторович Буров. — Львів: «Магнолія 2006», 2010. — 262 с. ISBN 966-8340-69-8

3 Фігурнов В.Е., “IBM PC для користувача”, 1998.

4 Камалян А.К., Кульов С.А., Назаренко К.М. та ін Комп'ютерні мережі та засоби захисту інформації: Навчальний посібник / Камалян А.К., Кульов С.А., Назаренко К.М. ВДАУ, 2003.-119с.

5 Малишев Р.А. Локальні обчислювальні мережі: Навчальний посібник / РГАТА. 2005. - 83 с.

6 Оліфер В.Г, Оліфер Н.А. Мережеві операційні системи / В.Г. Оліфер, Н.А. Оліфер. - СПб.: 2002. - 544 с.: Іл.

7 Оліфер В.Г., Оліфер Н.А. Комп'ютерні мережі. Принципи, технології, протоколи / В.Г. Оліфер, Н.А. Оліфер. - СПб.: Пітер, 2002 .- 672 с.: Іл.

8 Герасименко В.Г., Нестеровський І.П., Моніторенко В.В. та ін Обчислювальні мережі та засоби їх захисту: Навчальний посібник / Герасименко В.Г., Нестеровський І.П., Моніторенко В.В. та ін - ВДТУ, 1998. - 124 с.

9 Галіцин В.К., Левченко Ф.А. Багатокористувацькі обчислювальні системи та мережі.– К.:КНЕУ, 1998.–360с.

10 Горлач В.М., Макар В.М. Побудова та адміністрування мереж Ч.1. Основи мережних технологій. Тексти лекцій.– Львів: Львів. ун–т, 1999.

11 http://www.mikrotik.com.ua/

12 http://uk.wikipedia.org/wiki/комунікаційна_мережа

13 http://www.compress.ru/Temp/3292/index.htm

14 http://uk.wikipedia.org/wiki/DNS

ДОДАТОК 1

ДЕМОНСТРАЦІЙНИЙ МАТЕРІАЛ

1 Тема дипломної роботи (стор.1)

2 Топології локальних мереж (стор. 11 рис. 1.1, стор. 11 рис. 1.2, стор. 12 рис. 1.3)

3 Ієрархічна топологія (стор. 14 рис. 1.5)

4 Організація мережі будівлі (стор. 17 рис. 2.2)

5 Структурована кабельна система (стор. 16 рис. 2.1)

5 Вибір мережевого обладнання (стор. 21 рис. 3.2, стор. 23 рис. 3.3, стор. 24 рис. 3.4)

7 Маршрутизатор TP-LINK Archer C5400X (стор. 19 рис. 3.1)

8 Протоколи безпеки (стор. 32)