Міністерство освіти і науки України
Харківський національний університет радіоелектроніки
(повне найменування вищого навчального закладу)

Факультет *Інфокомунікацій*
(повне найменування інституту, факультету (відділення))

Кафедра *Інформаційно-мережної інженерії*
(повна назва кафедри (предметної, циклової комісії))

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

другий (магістерський)
(рівень вищої освіти)

Дослідження та проектування локальної мережі підприємства
(тема)

Виконав: студент 2 курсу групи *ІМІм-20-1*
Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва спеціальності)
Тип програми *освітньо-професійна*
(освітньо-професійна або освітньо-наукова)
Освітня програма *Інформаційно-мережна інженерія*
(повна назва освітньої програми)
Гузей О.І.
(прізвище та ініціали)

Керівник *доц. Скорик Ю.В.*
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ *Безрук В.М.*
(підпис) (прізвище, ініціали)

2021 р.

Не містить відомостей, заборонених
до відкритого публікування

Керівник_____ /*Ю.В. Скорик*

Студент _____ / *О.І. Гузей*

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

(повне найменування вищого навчального закладу)

Факультет *Інфокомунікацій*

Кафедра *Інформаційно-мережної інженерії*

Рівень вищої освіти *другий (магістерський)*

Спеціальність *172 Телекомунікації та радіотехніка*

(код і повна назва)

Тип програми *освітньо-професійна*

(освітньо-професійна або освітньо-наукова)

Освітня програма *Інформаційно-мережна інженерія*

(повна назва)

ЗАТВЕРДЖУЮ

Зав. кафедри «ІМІ»

_____ проф. Безрук В.М.

(підпис)

«*08*» *листопада* 2021 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові *Гузей Ользі Івановні*

(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження та проектування локальної мережі підприємства*

керівник роботи *доц., к.т.н. Скорик Юлія Валеріївна*

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом ВНЗ від «*08*» *листопада* 2021 р. № *1674 Ст*

2. Термін подання студентом роботи до екзаменаційної комісії *13.12.* 2021 р.

3. Вихідні дані до роботи *Проектування локальної мережі підприємства Worknest. Розрахунок мережевого обладнання. Проектування логічної організації підприємства в Packet Tracer.*

4. Перелік запитань, що необхідно опрацювати в роботі

Вступ

1 *Вибір структури та топології організації*

2 Структурована кабельна система організації

3 Вибір мережного обладнання

4 Логічна організація ЛМЗ

Висновки

5. Перелік графічного матеріалу із зазначенням креслень, схем, плакатів, комп'ютерних ілюстрацій *слайди презентації в форматі Power Point 16 слайдів (назва роботи, вступ та мета роботи, визначення, класифікація і топологія ЛМ, інформація про компанію Worknest, безпека ЛМ, протоколи, налаштування маршрутизатора і комутатора, логічна схема ЛМ організації, висновки)*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Ознайомлення із завданням. Уточнення ТЗ.	08.11.21-10.11.21	
2	Пошук джерел за темою роботи	11.11.21-12.11.21	
3	Виконання практичної частини роботи	13.11.21-16.11.21	
4	Розробка розділу 1	17.11.21-22.11.21	
5	Розробка розділу 2	23.11.21-27.11.21	
6	Розробка розділу 3	28.11.21-02.12.21	
7	Висновки	03.12.21-04.12.21	
8	Оформлення пояснювальної записки	05.12.21-09.12.21	
9	Оформлення презентаційного матеріалу. Підготовка додо захисту роботи. до захисту роботи	10.12.21-13.12.21	

Дата видачі завдання *08 листопада* 2021 р.

Студент _____ Гузей О.І.
(підпис) (прізвище та ініціали)

Керівник роботи _____ доц. Скорик Ю.В.
(підпис) (посада, прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка: 67 с., 11 рис., 3 додатки, 10 джерел.

Предметом дослідження є підприємство з розробки програмного забезпечення. 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.

Методи дослідження – аналітичний та практичний.

Показані теоретичні і практичні сторони побудови локальної комп’ютерної мережі підприємства на прикладі компанії «Worknest». 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 «Worknest». 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, ТОПОЛОГІЯ, WORKNEST, TP-LINK, МЕРЕЖА, ДАНІ, МАРШРУТИЗАТОР, КОМУТАТОР, ETHERNET, MAC-АДРЕС.

ABSTRACT

Explanatory note: 67 pp., 11 figures, 3 addition, 10 sources.

The subject of the study is a software development company. The object of study is local computer networks.

The purpose of the qualification work is the design of a local area network and to show the features of a local computer network: structure, classification, purpose, topology, technical support.

Research methods are analytical and practical.

Theoretical and practical aspects of designing a local computer network of the enterprise are shown on the example of the company "Worknest". Literature sources on the classification of local computer networks were analyzed, network equipment was proposed according to the selected characteristics, and recommendations were provided for configuration for each of the elements of the local computer network of the company "Worknest". Familiarization was made with the tools for ensuring the protection of information and trade secrets of the local network, namely: firewalls, proxy servers, VPN and protocols. Quantitative and qualitative evaluation of network equipment was carried out for the purpose of fast data exchange between individual departments or employees and significant funds savings.

LOCAL NETWORK, TOPOLOGY, WORKNEST, TP-LINK, NETWORK, DATA, ROUTER, SWITCH, ETHERNET, MAC ADDRESS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ....8
ВСТУП....10
1 ВИБІР СТРУКТУРИ ТА ТОПОЛОГІЇ ОРГАНІЗАЦІЇ....11
1.1 Концепція локальної мережі....11
1.2. Структура локальних комп'ютерних мереж....12
1.3. Класифікація локальних комп'ютерних мереж....13
1.4. Топологія локальних мереж....15
2 СТРУКТУРОВАНА КАБЕЛЬНА СИСТЕМА ОРГАНІЗАЦІЇ....20
3 ВИБІР МЕРЕЖНОГО ОБЛАДНАННЯ....23
3.1 Критерії до вибору мережного обладнання....23
3.2 Опис необхідного обладнання....23
3.2.1 Маршрутизатор ЛМЗ організації....24
3.2.2 Мережний комутатор для будинку....27
3.2.3 Мережний комутатор для поверху....29
3.2.4 Комутатор некерований для групи....30
3.2.5 Кабель для передачі даних по мережі....32
3.3 Безпека локальної мережі....34
4 ЛОГІЧНА ОРГАНІЗАЦІЯ ЛМЗ....42
4.1 Розбиття мережі на підмережі на основі IP-адрес....42
4.2 Налаштування комутаторів і маршрутизаторів....43
4.2.1 Налаштування маршрутизатора в програмному інтерфейсі....43
4.2.2 Налаштування комутатора в програмному інтерфейсі....43
4.3 Використані канальні технології....44
ВИСНОВОК....47
ПЕРЕЛІК ПОСИЛАНЬ....48
ДОДАТОК А....49

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ВК – Вузол комунікації

ГГц – Гігагерц

Гб – Гігабайт

ЛМ – Локальна мережа

СКС – Структурована кабельна система

AI – Artificial intelligence

ARP – Address Resolution Protocol

BGP – Border Gateway Protocol

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

DoS – Denial of Service

FTP – File Transfer Protocol

IEEE – Institute of Electrical and Electronics Engineers

IPSec – IP Security

IT – Information Technology

LAN – Local Area Network

MAC-адрес – Media Access Control

MITM – Man-In-The-Middle

ODM – Original Design Manufacturer

OSI – The 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

WEP – Wired Equivalent Privacy

WI-FI – Wireless Fidelity

WPA – Wi-Fi Protected Access

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 домашньої WI-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 «Worknest».

1 ВИБІР СТРУКТУРИ ТА ТОПОЛОГІЇ ОРГАНІЗАЦІЇ

1.1 Концепція локальної мережі

Локальна мережа (ЛМ) - мережа обміну даними, що належить та керується однією організацією. Її можна визначити як цілісну інформаційну систему, яка дозволяє спільно використовувати всі ресурси корпоративної мережі та оптимізувати процес. Локальні мережі поділяються на установчі (офісні мережі фірм, мережі організаційного управління та інші мережі) та мережі управління технологічними процесами на підприємствах.

Більшість локальних мереж з'єднують робочі станції та персональні комп'ютери. Кожен вузол (окремий комп'ютер) у локальній мережі має свій власний процесор, за допомогою якого він виконує програми, але також може отримувати доступ до даних та пристроїв у будь-якому місці локальної мережі. Таким чином, багато користувачів мають можливість спільно використовувати такі пристрої, як принтери або дані. Користувачі можуть використовувати локальну мережу для спілкування один з одним, надсилаючи електронну пошту або беручи участь у чаті.

Локальна мережа в кваліфікаційній роботі будується на основі міжнародної компанії WorkNest.

WorkNest - це міжнародна сервісна аутстафф-компанія, яка створює в Україні центри досліджень та розробок та спеціалізовані групи для IT-компаній, а також надає офшорні та наземні технологічні рішення для задоволення зростаючого попиту на висококласну IT-робочу силу [9]. WorkNest надає спеціальні команди, які ідеально адаптовані до потреб проекту. Завдяки компанії WorkNest створюються інноваційні програмні продукти та сильні команди для досягнення поставлених цілей. Для довготривалої роботи із закордонними клієнтами залучені експерти, які можуть створювати сучасні та конкурентні

продукти для користувачів на досить високому професійному рівні у таких бізнес-сферах як:

- 3D modelling;
- AI;
- App Development;
- E-commerce;
- UI/UX;
- Data Analysis;
- Machine Learning;
- Data Science.

Один з офісів компанії знаходиться у центрі Харкова, він займає 3 поверхи та налічує 30 робочих місць.

1.2. Структура локальних комп'ютерних мереж

Для створення локальної мережі зазвичай, крім підключених комп’ютерів, потрібні три основні компоненти: мережеві карти, кабель і програмне забезпечення. У рамках розробки дипломної роботи можна представити класифікацію в контексті таких ознак:

- топологія: геометричне розташування пристроїв у мережі. Наприклад, пристрої можуть бути розташовані у вигляді кільця або прямої лінії.
- протоколи: правила та специфікації кодування для відправлення даних (найпоширенішим є Ethernet з урахуванням TCP/IP). Протоколи також визначають, чи використовує мережу однорангову або клієнт-серверну архітектуру.
- носій: пристрої можуть бути підключені через кручену пару, коаксіальні кабелі або оптоволоконні кабелі.

Фізичні властивості ЛМ, керовані програмним забезпеченням, включають інтерфейси, які називаються блоками доступу до мережі, які з'єднують комп'ютери з мережами. Ці пристрої є мережними картами, встановленими на

материнських платах комп'ютерів. Їх завдання - забезпечити з'єднання, контролювати доступність, задати чи буферизувати швидкість передачі даних, запобігти помилкам і колізіям під час передачі, а також збирати дані з локальної мережі в зручному вигляді [8].

Спосіб доступу до мережі полягає в виклику абонента за його мережевим ім'ям з комутацією каналів у вузлі комунікації (ВК). Спосіб комутації каналів передбачає підключення абонентів через ВК при передачі повідомлення. При цьому ВК може організувати пріоритетний доступ до мережі абонентів [1].

Перевагами такого виду мережі:

- простота та низька вартість підключення користувачів мережі;
- простота управління мережею;
- можливість підключення та відключення абонентів без переривання мережі.

Також вона має недоліки:

- швидкість передачі повідомлень залежить від кількості абонентів, інтенсивності прийому та передачі повідомлень та технічних можливостей ВК;
- надійність мережі визначається надійністю ВК;
- велика загальна протяжність і низька ефективність використання фізичного середовища передачі сигналу.

Для підвищення надійності ВК побудовані за модульним принципом, що передбачає робочі та резервні модулі. Система діагностики оцінює функціонування робочого модуля, при необхідності перемикає мережу на роботу з резервним модулем [1].

1.3. Класифікація локальних комп'ютерних мереж

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

Таблиця 1.1 — Класифікація локальних мереж

По ролі персонального комп’ютера у мережі	мережі із сервером
	одноранговi (рівноправні) мережі
По структурі (топології) мережі	одновузлові («зірка»)
	магістральні («шина»)
	кільцеві («кільце»)
	комбіновані
За способом доступу користувачів до ресурсів та абонентів мережі	мережі з підключенням користувача за вказаними адресами абонентів за принципом комутації каналів (зірка)
	мережі з централізованим (програмним) керуванням підключення користувачів до мережі («кільце» та «шина»)
	мережі із випадковою дисципліною обслуговування користувачів («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 (постійних або змінних)
	непріоритетні, коли всі користувачі мають рівні права доступу до мережі

Продовження табл.1.1

З розміщення даних у компонентах мережі	з центральним банком даних;
	з розподіленим банком даних;
	з комбінованою системою розміщення даних.

1.4. Топологія локальних мереж

Під топологією (компонуванням, конфігурацією, структурою) комп'ютерної мережі зазвичай розуміється фізичне розташування комп'ютерів мережі один щодо одного та спосіб з'єднання їх лініями зв'язку. Важливо, що поняття топології належить до локальних мереж, у яких структуру зв'язків можна легко простежити. У глобальних мережах структура зв'язків зазвичай прихована від користувачів і дуже важлива, оскільки кожен сеанс зв'язку може здійснюватися особистим шляхом [7].

Існують такі базові топології мережі:

Шина (bus) – всі комп'ютери паралельно підключаються до однієї лінії зв'язку (рис. 1.1).

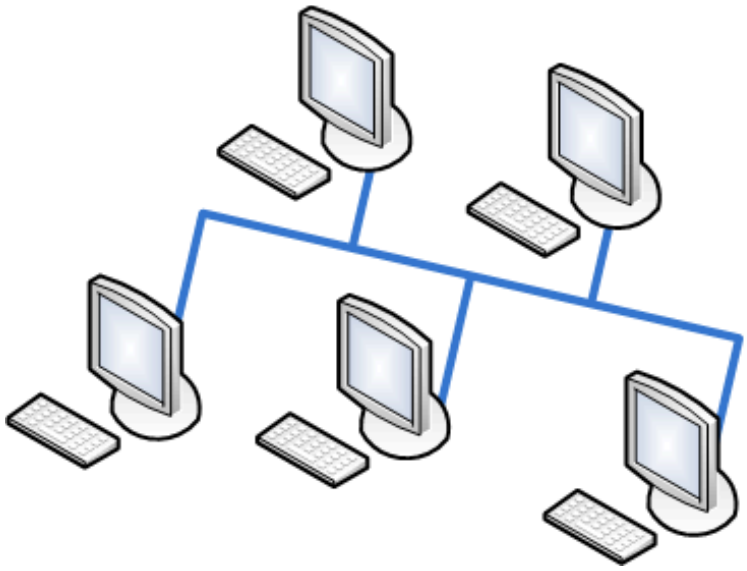

Рисунок 1.1 – Мережна топологія шина

Зірка (star) - буває двох основних видів:

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

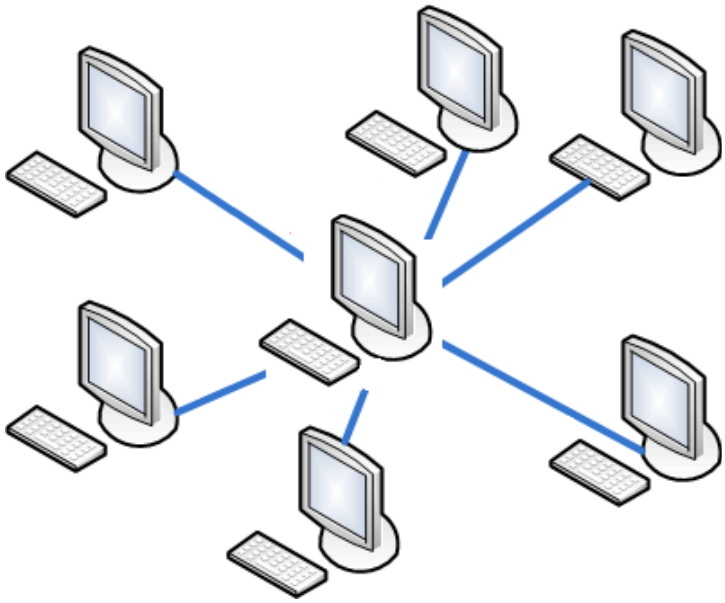

Рисунок 1.2 – Активна зірка

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

У центрі мережі з даною топологією міститься не комп'ютер, а спеціальний пристрій — комутатор (рис. 1.3).

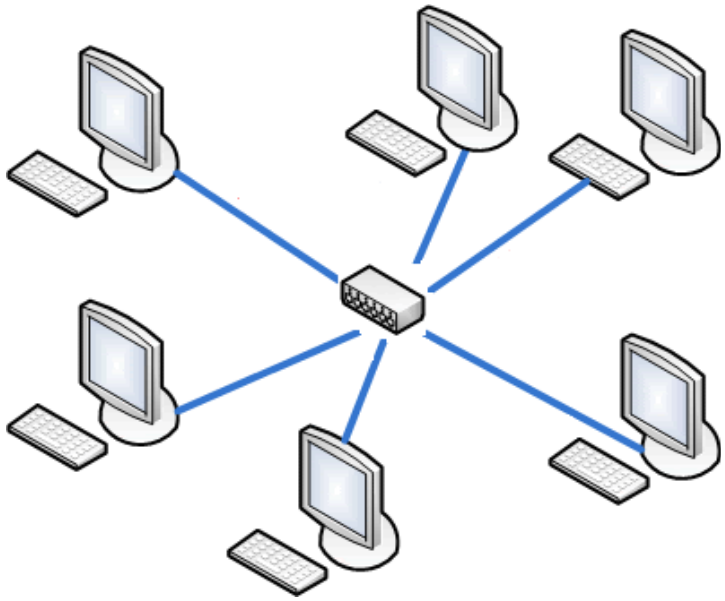

Рисунок 1.3 – Пасивна зірка

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

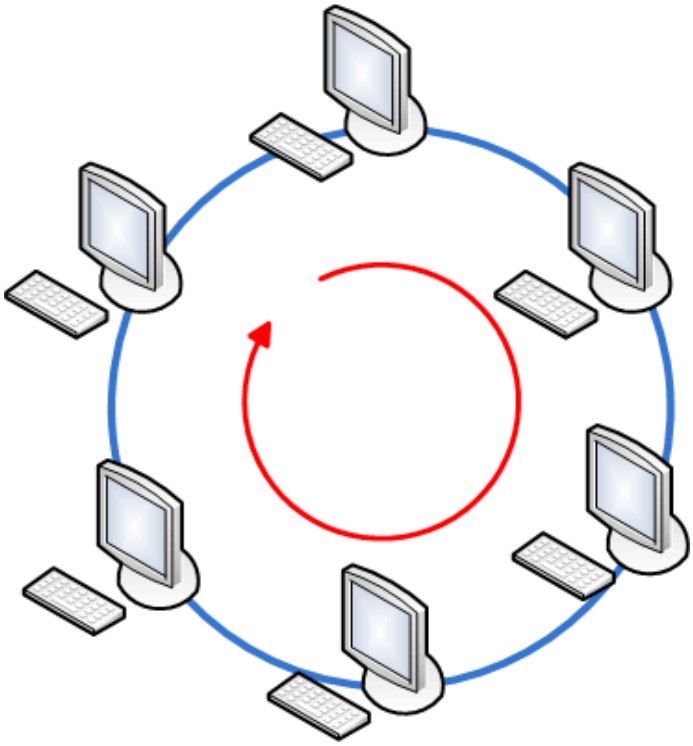

Рисунок 1.4 – Мережна топологія кільце

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:

- склад необхідних 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 топологій 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 [2]:

- досить велика кількість обслуговуваних робочих місць;
- розумна вартість мережі;
- така мережа забезпечує просте рішення в реалізації та експлуатації мережі;
- простота модифікації мережі при необхідності.

2 СТРУКТУРОВАНА КАБЕЛЬНА СИСТЕМА ОРГАНІЗАЦІЇ

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

У СКС 4 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 Fast Ethernet (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 схема розроблена з урахуванням властивих їй особливостей конструкції. Кабелі

будуть проходити вздовж стіни в спеціально відведених каналах. Кабель тягнеться на верхні поверхи біля сходового отвору.

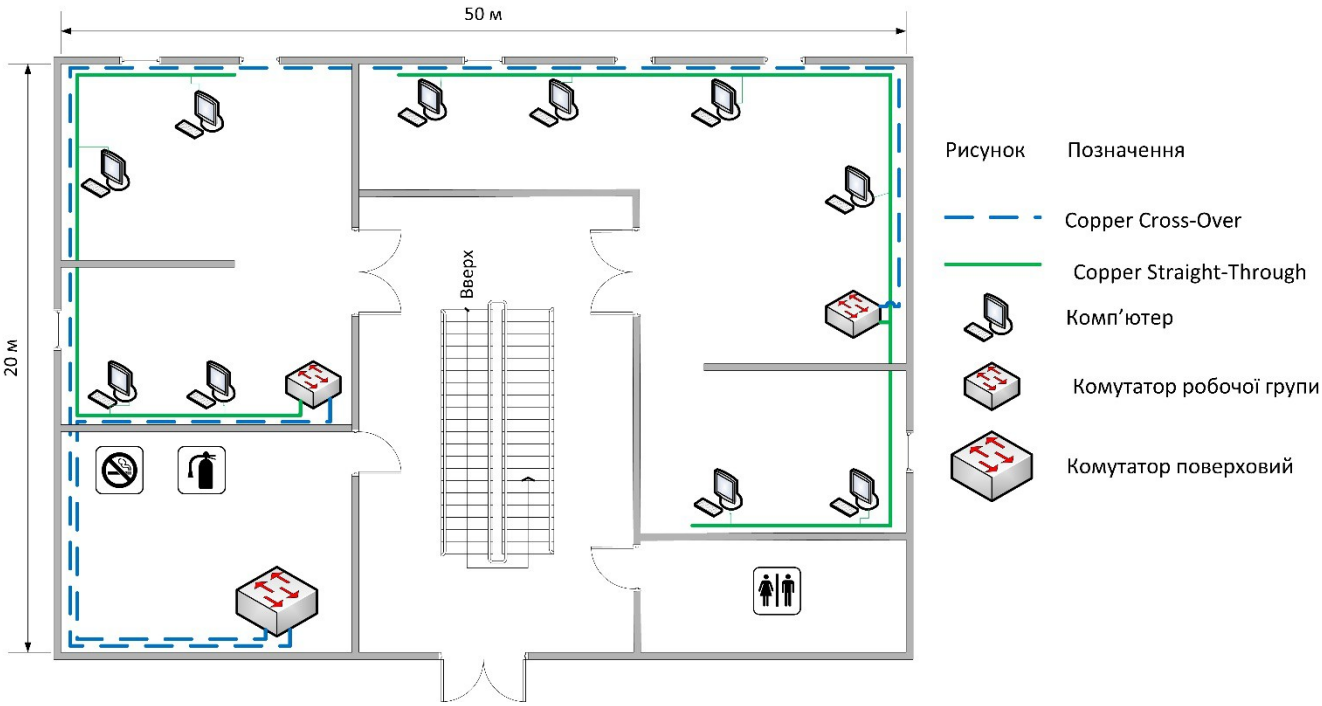

Рисунок 2.1 — Організація поверхів

– 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 оптичних кабелях. Вертикальна підсистема також включає супутнє обладнання, що використовується для прокладки кабелю через будівлю.

Схема будівлі офісу компанії Worknest (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 Fast Ethernet (з урахуванням перспективи розвитку).

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

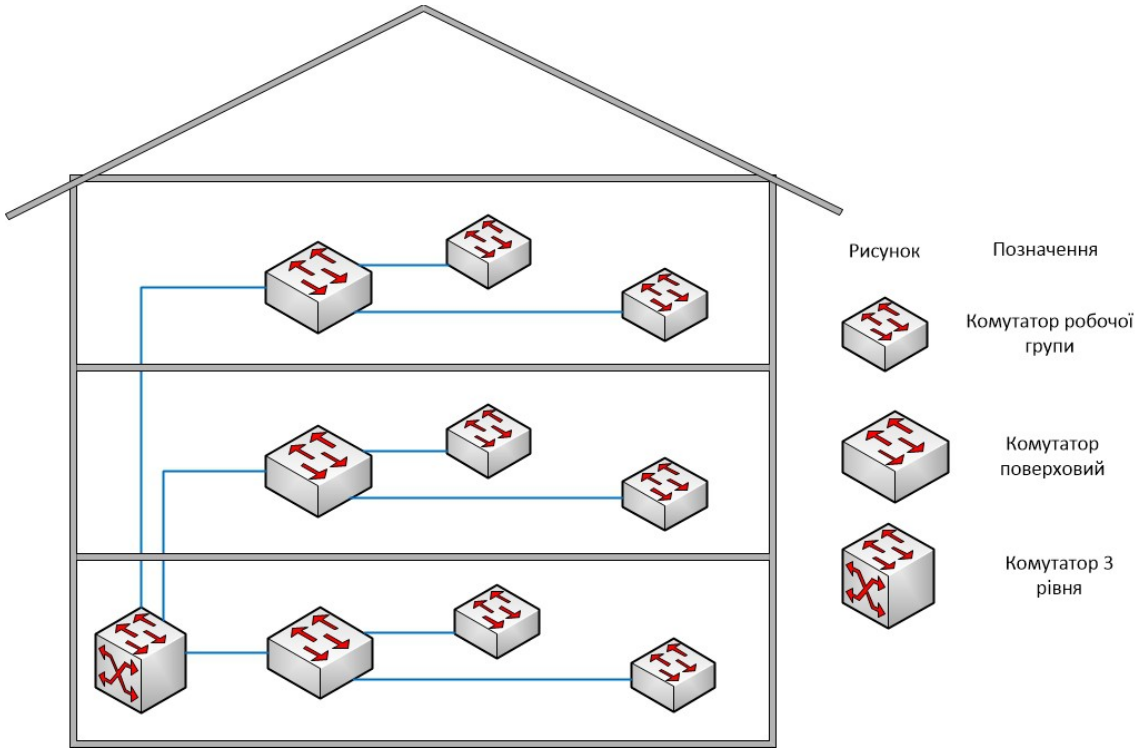

Рисунок 2.2 — Організація будівлі компанії

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 обрала мережне обладнання фірми TP-Link.

Компанія заснована у 1996 році в місті Шеньчжень. Засновниками (засновниками) є два брати Чжао Цзяньцзюнь та Чжао Цзясін. Назва TP-Link є скороченням від "Twisted Pair" - кручена пара, "link" - з'єднання. Згодом TP почали трактувати як Trust and Performance [10].

2005 року 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 [10].

Продукти TP-Link включають високошвидкісні кабельні модеми, 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 Kasa Smart 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.

3.2.1 Маршрутизатор ЛМЗ організації

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

Рисунок 3.1 – Зовнішній вигляд маршрутизатора

Опис:

TP-LINK Archer C5400X оснащений 1.8 ГГц 64-бітним чотирьохядерним процесором, 3 співпроцесорами та 1 ГБ оперативної пам'яті, забезпечує максимум потужності всім додаткам, онлайн-сервісам, а також виключає можливість затримки під час роботи [6].

Основні характеристики обладнання перелічені в табл. 3.1.

Таблиця 3.1 — Характеристики маршрутизатора TP-LINK Archer C5400X

Характеристики бездротової мережі	
Стандарт Wi-Fi 5	IEEE 802.11ac/n/a 5 ГГц IEEE 802.11n/b/g 2,4 ГГц
Швидкість Wi-Fi AC5400	5 ГГц: 2167 Мбіт/с (802.11ac) 5 ГГц: 2167 Мбіт/с (802.11ac) 2,4 ГГц: 1000 Мбіт/с (802.11n)
Тип антени	Зовнішня / Незнімна
Кількість антен	8
Захист інформації	WPA, WEP, EAP
Характеристики провідної мережі	
Вхідний інтерфейс (WAN)	10/100 / 1000BASE-T Ethernet (MDI / MDIX)
Процесор	Чотирьохядерний 64-розрядний процесор 1,8 ГГц
Кількість WAN портів	1 шт.
Кількість LAN портів	8 шт.
Доп. порти і роз'єми	2 порта USB 3.0
Підтримувані файлові системи	NTFS, exFAT, HFS+, FAT32
Підтримувані функції	Apple Time Machine FTP-сервер Мультимедійний сервер Сервер Samba
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

Продовження табл.3.1

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 Оновлення повітрям TP-Link ID DDNS
Прокидання NAT	Перекидання портів Port Triggering DMZ UPnP
IPTV	IGMP Proxy IGMP Snooping Міст Тегування VLAN

Продовження табл.3.1

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	
Комплект поставки	Wi-Fi роутер Archer C5400X Адаптер живлення Кабель Ethernet RJ45 Посібник із швидкого налаштування

3.2.2 Мережний комутатор для будинку

Мережевий комутатор TP-Link TL-SG1016D (рис. 3.2).

Рисунок 3.2 – Зовнішній вигляд комутатора

Опис:

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.

Таблиця 3.2 ─ Характеристики мережного комутатора TP-Link TL-SG1016D

Характеристики	
Інтерфейси	16 портів 10/100/1000 Мбіт/с з автоузгодженням, з роз'ємами RJ45 (авто-MDI/MDIX)
Стандарти та протоколи	IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3x
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	100-240VAC, 50/60Hz
Енергоспоживання	Максимум: 9,26Вт (220В/50Гц)
Розміри (ШхДхВ)	294 x 180 x 44 мм
Швидкість передачі пакетів	238 Млн. пакетів у сек.
Таблиця MAC адрес	8000 записів
Кадри Jumbo	10 Кбайт
Метод передачі	Store-and-Forward (Зберігання та передача)
Сертифікація	FCC, CE, RoHS

Продовження табл.3.2

Комплект поставки	16-портовий гігабітний настільний/монтований у стійку комутатор Кабель живлення Інструкція користувача Комплект деталей для монтажу у стійку Гумові ніжки
Комутаційна здатність	32 Гбіт/с

3.2.3 Мережний комутатор для поверху

Мережний комутатор TP-LINK TL-SG1024 (рис. 3.3).

Рисунок 3.3 – Зовнішній вигляд комутатора

Опис:

24-портовий гігабітний комутатор TL-SG1024 підтримує останні енергозберігаючі технології, за допомогою яких можливо збільшити пропускну спроможність мережі зі значно меншими енерговитратами. Пристрій автоматично 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 для мережевого середовища швидкості для забезпечення максимальної пропускної здатності. Таблиця MAC-адрес на 8000 записів забезпечує хорошу масштабованість навіть великих мереж. Комутатор також підтримує контроль потоку IEEE 802.3x для повнодуплексного режиму та контроль зворотного потоку для напівдуплексного режиму, щоб уникнути перевантажень та забезпечення надійної передачі даних.

Основні характеристики обладнання перелічені в табл. 3.3.

Таблиця 3.3 – Характеристики мережевого комутатора TP-LINK T1700G-28TQ

Апаратні характеристики	
Стандарти і протоколи	IEEE 802.3i, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3x
Інтерфейс	24 портів 10/100/1000 Мбіт/с з автоузгодженням, з роз'ємами RJ45 (авто-MDI/MDIX)
Середовище передачі даних	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, 5e або вище (макс. 100 м)
Джерело живлення	100~240 перем. струму, 50/60 Гц
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	35,7 мільйонів пакетів за секунду
Таблиця MAC адрес	8000 записів
Кадри jumbo	10 Кбайт
QoS	802.1p/DSCP QoS*
Метод передачі	Store-and-Forward (Зберігання та передача)

3.2.4 Комутатор некерований для групи

Комутатор некерований TP-LINK TL-SG1218MP (рис. 3.4)

Рисунок 3.4 — Зовнішній вигляд комутатора

Опис:

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.

Таблиця 3.4 – Характеристики комутатора некерованого TP-LINK TL-SG1218MP

Апаратне забезпечення	
Інтерфейси	16 гігабітних портів RJ45 PoE+ 2 гігабітні комбо RJ45/SFP-слоти
Стандарти та протоколи	IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3x, IEEE 802.3af, IEEE 802.3at, IEEE 802.1q, IEEE 802.1p

Продовження табл.3.4

Середовище передачі даних	10BASE-T: неекранована кручена пара

	категорій 3, 4, 5 (макс. 100 м)
	EIA/TIA-568 100 Ом екранована кручена пара (макс. 100 м)
	100BASE-TX: неекранована кручена пара категорій 5, 5e (макс. 100 м)
	EIA/TIA-568 100 Ом екранована кручена пара (макс. 100 м)
	1000BASE-T: неекранована кручена пара категорій 5, 5e, 6 або вище (макс. 100 м)
	EIA/TIA-568 100 Ом екранована кручена пара (макс. 100 м)
	1000BASE-X MMF, SMF
Джерело живлення	100–240 В змінного струму, 50/60 Гц
Порти PoE+ (RJ45)	Стандарти: 802.3at/802.3af Порти PoE: 1–16 Бюджет PoE: 250 Вт
Розміри (Ш × Д × В)	440×180×44 мм
Максимальне енергоспоживання	21,4 Вт (220 В / 50 Гц, без підключених пристроїв живлення) 286,64 Вт (220 В / 50 Гц, з підключеними пристроями живлення 250 Вт)
Продуктивність	
Комутаційна матриця	36 Гбіт / с
Швидкість передачі пакетів	26,78 млн пакетів за секунду
Таблиця MAC-адрес	8K записів
Додаткові функції	Сумісність із пристроями стандарту IEEE 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.

3.2.5 Кабель для передачі даних по мережі

Кабель FTP cat.5e CCA VKcable, 305м (рис. 3.5).

Рисунок 3.5 – Зовнішній вигляд кабелю

4-парний FTP-кабель категорії 5е 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, Fast Ethernet (100BASE-TX), Token Ring 16/100 Мбіт/с, Gigabit Ethernet (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.

Кабель складається з 4 пар провідників, скручених разом. 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.

Таблиця 3.5 – 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
Кількість жил	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 високі ризики 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) [4].

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 [5].

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 мережевих адміністраторів. 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 фішинговий 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 дані [5].

Під 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.

3.3.1 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 XArp та 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 [4].

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 типу комунікації; разом вони утворюють так званий стек протоколів. Ці програми, 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) [4].

PGP

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) під час 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 ідентифікує процес застосування в Інтернеті. Перевагою використання протоколів 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 себе за 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-2453 і визначається за допомогою звичайного пароля, який передається відкритим текстом. Такий захист слабкий, якщо зловмисник 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 [5].

4 ЛОГІЧНА ОРГАНІЗАЦІЯ ЛМЗ

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 Packet Tracer для моделювання мереж на базі обладнання Cisco Sys. План розміщення обладнання представлений у Додатку А.

4.1 Розбиття мережі на підмережі на основі IP-адрес

Згідно з тим, що маємо офіс компанії Worknest, то 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) — хостовой. 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	Адрес підмережі 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 [3].

- interface GigabitEthernet5/0.1;
- encapsulation dot1Q 10;
- ip address 192.168.0.1 255.255.255.240.

Налаштування DHCP:

- Ввімкнення;
  - service dhcp.
- Оголошуємо пул та ім’я рідного домена;
  - ip dhcp pool 1;
  - network 192.168.0.0 255.255.255.240;
  - default-router 192.168.0.1;
  - domain-name write.
- Виключаємо з пулу адреси;
  - ip dhcp excluded-address 192.168.0.1;
  - ip dhcp excluded-address 192.168.0.17;
  - ip dhcp excluded-address 192.168.0.33;

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;
  - switchport trunk encapsulation dot1q;
  - switchport mode trunk.

- Налаштування адреси в VLAN;
  - interface Vlan10;
  - ip address 192.168.0.1 255.255.255.240.
- Налаштування статичного транка до маршрутизатора.
  - interface GigabitEthernet0/1;
  - switchport trunk encapsulation dot1q;
  - switchport mode trunk.

На поверховому комутаторі прописуємо наступні команди:

- Налаштування статичного транка до домового комутатора 3 рівня;
  - interface FastEthernet0/1;
  - switchport mode trunk.
- Налаштування access портів;

Призначення порту комутатора в VLAN:

- interface FastEthernet0/2;
- switchport access vlan 60;
- switchport mode access.

4.3 Використані канальні технології

В якості канальних технологій використовувалися Fast Ethernet та Gigabit Ethernet.

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

- збільшення пропускної здатності сегментів мережі до 100 Мб/с;
- збереження методу довільного доступу Ethernet;
- збереження зірчастої топології мереж і обслуговування традиційних засобів передачі даних — витої пари і волоконно-оптичного кабелю.

Ці параметри дозволяють здійснити поступовий перехід від мереж 10Base-T — найпопулярнішого варіанту Ethernet на сьогоднішній день — до високошвидкісної мережі, яка зберігає значну безперервність з добре відомою

технологією: Fast Ethernet 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 [3]:

– 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 багатомодового 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 Gigabit Ethernet — 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 [3].

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 включає такі типи:

– 1000BASE-SX — сегмент на багатомодовому 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.

ВИСНОВОК

У процесі виконання кваліфікаційної роботи на основі аналізу вихідних даних та загальних принципів проектування локальних мереж була розроблена мережа підприємства «Worknest». 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.

ПЕРЕЛІК ПОСИЛАНЬ

1. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы - Учебник для ВУЗов, 2-е издание/ В.Г. Олифер, Н. А Олифер. СПб.: Питер, 2004 - 864с., ил.
2. Смирнов И. Г. Структурированные кабельные системы – проектирование, монтаж и сертификация. – М: Экон-Информ, 2005 г.
3. Сэм Хелеби, Денни Мак-Ферсон. Принципы маршрутизации в Internet. – М:»Вильямс». – 2001. – 448 с.
4. B. Mitchell, What Is a Network Sniffer?, 2016, [online], [cit. 2018-04- 22]. Available: <https://www.lifewire.com/definition-of-sniffer817996>
5. A. A. Ghorbani and W. Lu, M. Tavallaee, Network Intrusion Detection and Prevention, Springer, US, 2010, 216 p.
6. Каталог оборудования: маршрутизаторы [Электронный ресурс].http://itel.com.ua/ – Загл. с экрана.
7. Задонский А.Ю. Построение корпоративных систем управления ИБ // Защита информации Inside. – 1, 2006 – 42 с.
8. Акропов П.Ц. Компьютерные сети. Принципы, технологии, протоколы. 2006г
9. Офіційний сайт компанії Worknest [Электронный ресурс].https://www.work-nest.com/ – Загл. с экрана.
10. Офіційний сайт компанії TP-Link [Электронный ресурс]. https://www.tp-link.com/uk-ua/ – Загл. с экрана.