

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ  
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І СИСТЕМ

КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРОЕКТУВАННЯ

**Пояснювальна записка**  
до кваліфікаційної випускної роботи

на тему: «Міська ділянка корпоративної мережі «А-банку»»

Виконав:

студент 2 курсу, групи WEBC-1811  
напряму підготовки 126 – «Інформаційні  
технології та системи»

Янко Н. К.

Керівник:

к.т.н., професор Колесніков К. В.

Рецензент:

к.т.н., доцент Землянський О.М.

Черкаси 2020

# Черкаський державний технологічний університет

(назва вузу)

Факультет ФІТІС Кафедра Інформаційних технологій проектування

Напрямок підготовки 126 “Інформаційні технології і системи”

Спеціалізація - Web- технології, Web- дизайн

ЗАТВЕРДЖУЮ:

Зав.кафедрою \_\_\_\_\_ Прокопенко Т.О.

« 06 » 02 \_\_2020 г.

## ЗАВДАННЯ

На кваліфікаційну випускную роботу студентів

*Янку Нікиті Кристововичу*

(прізвище, ім'я, по батькові)

1. **Тема роботи** Міська ділянка корпоративної мережі «А-банку»  
керівник проекту (роботи) Колесніков Костянтин Васильович, к.т.н., доцент,  
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)  
затверджені наказом Черкаського державного технологічного університету від 19.02.2020  
№ 71/01

2. **Термін здачі студентом закінченого проекту (роботи)** 17.06.2020

### 3. Вихідні дані до проекту (роботи)

Мережа даних повинна бути побудована з урахуванням організаційно-адміністративної структури банку. Мережа має забезпечити можливість безпечного інформаційного обміну, бездротовий доступ в мережу Internet, та можливість передачі даних по аналоговим лініям зв'язку. Топологія сегменту – радіальна; – з'єднання з центральним офісом (ЦО) – радіальне. Число периферійних відділень (ПВ) - 20. Періодичність опитування (періодичність сеансів) – 8 годин. Обсяг сеансового масиву – не менш 200 Мб. Спрямованість інформаційного потоку – двостороння однакового обсягу: висхідний потік (від периферії до ЦО) – відомості про виконання планів, доручень, наказів, вказівок, фінансові щоденні звіти; спадний потік (від ЦО до периферії) – контроль обсягу звітів, команди керування філіями. Інформаційний обсяг потоків у шлюзах не більше 3,0 Гб/добу; рівень інформаційної безпеки - C2. Імовірність втрат пакетів –  $10^{-5}$ ; Імовірність хибного спрацьовування системи захисту –  $10^{-6}$ . Імовірність помилки 1 на  $10^{-6}$ .

### 4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити)

Вступ; 1. Характеристика аналогів і прототипів банківських мереж; 2. Аналіз принципів побудови мереж; 3. Побудова серверного сегменту мережі банку; 4. Розрахунок параметрів проектованої мережі; 5. Організація безпеки інформаційного обміну в мережі

Висновки; Додатки; Список літератури.

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

1. Топологія сегменту мережі банку

2. Схема електрична загальна

3. Схема інформаційних потоків

4. Перелік елементів

5. Специфікація

6. Заходи щодо безпеки інформації у мережі

6. Консультанти з проекту (роботи) із зазначенням розділів проекту, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання\_\_\_\_\_

Керівник\_\_\_\_\_ Колесніков К. В. \_\_\_\_\_  
(підпис)

Завдання прийняв до виконання\_\_\_\_\_ Янко Н. К. \_\_\_\_\_  
(підпис)

Календарний план

Пор. №	Назва етапів дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1.	Постановка задачі	02.03.	виконано
2.	Аналіз та уточнення постановки задачі	12.03	виконано
3.	Пошук та аналіз аналогів	19.03	виконано
4.	Вибір мережевої архітектури та топології	29.04	виконано
5.	Проектування мережі та розрахунки	09.05	виконано
6.	Інформаційно- патентний пошук	13.05	виконано
7.	Заходи щодо безпеки інформації у мережі	20.05	виконано
8.	Оформлення результатів в записку, креслення, малюнки	22.05	виконано
9	Кафедральний захист роботи	22.05	виконано
10.	Подання роботи на відгук та рецензію	10.06.	виконано
11.	Захист випускної роботи	17. 06	

Студент-дипломник\_\_\_\_\_ (підпис)

Керівник проекту \_\_\_\_\_ (підпис)



## Анотація

У кваліфікаційній випускній роботі представлений міський сегмент розподіленої банківської мережі. Під час створення мережі використано сучасні технології та обладнання для синтезу систем подібного типу. Усі основні креслення розроблені за допомогою Microsoft Visio .

Комп'ютерна система забезпечує можливість безпечного інформаційного обміну, доступ до мережі Internet, та можливість передачі даних по аналоговим та цифровим лініям зв'язку.

Робота містить 71 листів записки пояснення, 6 розділів, 18 малюнків, 6 креслень та 5 таблиць, використано 25 джерел та інтернет посилань. Застосовано 5 програмних продуктів.

В першому розділі обґрунтовано постановку завдання.

В другому розділі представлено аналітичний огляд трьох аналогів корпоративних мереж серед підприємств та організацій.

В третьому розділі проаналізовано принципи побудови мережних комп'ютерних систем.

В четвертому розділі побудовано міський серверний сегмент мережі банку.

В п'ятому розділі розраховано параметри проектованої мережі.

В шостому розділі організовано безпеку інформаційного обміну в мережі із використанням електронного цифрового підпису.

**КЛЮЧОВІ СЛОВА:** корпоративна мережа банку, інформаційні потоки, апаратне забезпечення, пропускна спроможність, інформаційна безпека, криптографія.



## **Аннотация**

В данной выпускной работе представлен городской сегмент корпоративной сети А-банка. При создании сети использованы современные технологии и оборудование для синтеза систем подобного типа. Все основные чертежи разработаны с помощью Microsoft Visio.

Компьютерная система обеспечивает возможность безопасного информационного обмена, доступ к сети Internet, и возможность передачи данных по цифровым и аналоговым линиям связи.

Работа содержит 71 лист пояснительной записки, 6 разделов, 18 рисунков, 6 чертежей и 5 таблиц, использовано 25 источников и интернет ссылок. Использовано 5 программных продуктов.

В первом разделе обосновано постановку задачи. Во втором разделе представлен обзор трех аналогов корпоративных сетей среди предприятий и организаций. В третьем разделе описаны принципы построения таких компьютерных систем. В четвертом разделе построен серверный сегмент сети банка. В пятом разделе рассчитаны основные параметры проектируемой сети. Шестой раздел посвящён организации безопасности информационного обмена в банковской сети с использованием электронной цифровой подписи.

**КЛЮЧЕВЫЕ СЛОВА:** распределенная корпоративная сеть банка, информационные потоки, аппаратное обеспечение, пропускная способность, информационная безопасность, криптография.

## **Abstract**

In this thesis project was presented to the distributed network of a bank. When creating network uses modern technologies and equipment for the synthesis of this type. All major drawings developed using Microsoft Visio 2016.

The computer system provides the ability to secure information exchange, access to the Internet, and the ability to transfer data over analog lines.

Project contains 71 letters, 18 figures, 5 tables and 6 drawings, applied 25 sources and internet links, 5 applied software.

In the first chapter setting reasonable objectives. The second section provides an overview of three unique corporate networks of enterprises and organizations. In the third section describes the principles of building such computer systems. In the fourth section built server segment of the network. In the fifth chapter of the parameters of the designed network. The sixth section is devoted to the organization of information exchange security in the banking network using an electronic digital signature.

**KEYWORDS:** distributed network of a bank, information flows, hardware, bandwidth, information security, cryptography.

## ЗМІСТ

ВСТУП .....	4
1. ПОСТАНОВКА ЗАВДАННЯ .....	6
2. ХАРАКТЕРИСТИКА АНАЛОГІВ І ПРОТОТИПІВ БАНКІВСЬКИХ МЕРЕЖ.....	8
2.1 Корпоративна мережа «Черкаського облавтодору» .....	8
2.2 Корпоративна мережа Черкаської облдержадміністрації .....	9
2.3 Корпоративна мережа ВАТ «Ощадбанк» .....	10
Висновки до розділу 2 .....	122
3. АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ МЕРЕЖ.....	133
3.1 Технологія VPN .....	133
3.2 Технологія Frame Relay.....	145
3.3 Технологія Fast Ethernet.....	166
3.4 Технологія Gigabit Ethernet.....	188
3.5 10 GB Ethernet .....	189
3.6 PPPoE .....	219
3.7 MPLS.....	213
Висновки до розділу 3 .....	255
4. ПОБУДОВА СЕРВЕРНОГО СЕГМЕНТУ МЕРЕЖІ БАНКУ.....	266
4.1 Опис предметної області.....	266
4.2 Вибір комутаторів.....	28
4.3 Вибір ADSL модема .....	288

					ЧДТУ 201850.005 ПЗ			
Зм	Лист	№ докум.	Підпис	Дата	Міська ділянка корпоративної мережі «А-банку». Пояснювальна записка	Літ.	Лист	Листів
Розроб.		Янко Н.К.				Н	2	62
Перевір.		Колесніков К.В.						
Рецензент		Землянський О.М.						
Н. Контр.		Колесніков К.В.						
Затверд.		Прокопенко Т.О.						

ФІТІС, кафедра ІТП,  
Група WEBC-1811



4.4	Вибір файл сервера.....	29
4.5	Вибір сервера .....	31
4.6	Вибір робочої станції .....	311
4.7	Вибір брандмауера .....	322
	Висновки до розділу 4 .....	34
5.	РОЗРАХУНОК ПАРАМЕТРІВ ПРОЕКТОВАНОЇ МЕРЕЖІ .....	35
5.1	Розрахунок пропускної спроможності мережі .....	35
5.2	Розрахунок VPN-сервера .....	41
5.3	Система з кількома серверами .....	42
	Висновки до розділу 5 .....	46
6.	ОРГАНІЗАЦІЯ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ОБМІНУ В МЕРЕЖІ..	47
	Висновки до розділу 6 .....	52
	ВИСНОВКИ.....	53
	ДОДАТОК А	
	ЧДТУ201850.005 Міська ділянка корпоративної мережі А-банку	54
	СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ .....	60

					ЧДТУ 201850.005 ПЗ	Арк.
						3
Змн.	Арк.	№ докум.	Підпис	Дата		

## ВСТУП

Корпоративна мережа - це складна система, що включає в себе безліч найрізноманітніших складових: комп'ютери різних типів, системне і застосовне програмне забезпечення, мережеві плати (адаптери), хаби (концентратори), свічі (комутатори) і роутери (маршрутизатори), кабельну систему, тощо. Системні адміністратори, та їхні колеги – інтегратори повинні опікуватися тим, щоб ця громіздка і дуже дорога мережа як найкраще справлялася з обробкою інформаційних потоків, що циркулюють між підрозділами та співробітниками підприємства і дозволяла приймати їм оптимальні раціональні рішення, що забезпечують успіх підприємства в жорсткій конкурентній боротьбі.

Головний принцип VPN (Virtual private network) мережі базується на використанні каналів глобальної мережі (GAN), яка забезпечує зв'язок між територіально віддаленими підрозділами компанії без необхідності будови віддалених філій компанії.

Кожній корпоративній мережі властиві такі характеристики: швидкість передачі, сумісність, якість обслуговування, продуктивність, латентність, надійність, розширюваність, масштабованість та безпека. [1]

В границях однієї відомчої мережі можливо:

- організувати проксі- серверний доступ до інтернет;
- дзвінки відеоконференцій (Skype, Zoom, Hangouts) в межах компанії;
- створити корпоративну електронну пошту, голосову пошту, факси; єдиний електронний документообіг компанії;
- створення корпоративної IP-телефонії;
- загальні архиви документів, єдині корпоративні довідники та сервіси;
- автоматизований аудит даних систем відеоспостереження;
- програмну та апаратну модернізацію автоматизації робочих місць;

					ЧДТУ 201850.005 ПЗ	Арк.
						4
Змн.	Арк.	№ докум.	Підпис	Дата		

- дистанційний режим доступу до файл-серверів з базами даних (БД), пристроїв введення та виведення інформації;
- безпеку передачі даних та захисту корпоративної інформації від (НСД) несанкціонованого доступу.

Актуальність даної кваліфікаційної випускної роботи по створенню міської ділянки корпоративної мережі банківської установи поза сумнівом.

Під час виконання кваліфікаційної випускної роботи поставлені такі цілі та завдання:

- 1) Проаналізувати аналоги та прототипи існуючих корпоративних мереж серед підприємств;
- 2) Дослідити принципи побудови даних комп'ютерних систем, а також обрати технологію, яка буде задіяна при її синтезі;
- 3) Розробити топологію серверного сегменту мережі підприємства в кілька етапів:
  - дослідити предметну область А- банку;
  - провести інформаційне дослідження даної мережі;
  - обрати необхідне апаратне та програмне забезпечення, яке буде задіяно під час побудови топології;
- 4) Розрахувати параметри проектованої мережі;
- 5) Організувати безпеку інформаційного обміну в мережі;
- 6) Зробити висновки щодо виконання випускної роботи.

Обов'язкові параметри мережі наведено в розділі «Постановка завдання».

					ЧДТУ 201850.005 ПЗ	Арк.
						5
Змн.	Арк.	№ докум.	Підпис	Дата		



## 1. ПОСТАНОВКА ЗАВДАННЯ

**1. Призначення мережі передачі даних.** Мережа даних має бути побудована з урахуванням організаційно-адміністративної структури банку. Мережа має забезпечити можливість безпечного інформаційного обміну, доступ до мережі Internet, та можливість передачі даних по аналоговим лініях зв'язку.

1. **Топологія мережі** – радіальна (зіркоподібна). Центр мережі – м. Черкаси, вул. Хрещатик 188, Філія АТ «А-банк».
2. **Первинна мережа** – призначені промислові канали ТЧ (телефонні канали).
3. **Режим обміну** – інформаційний потік двосторонній.
4. Повинно забезпечуватись сполучення з телефонною мережею загального користування (ТМЗК) та мережею Internet.

### 5. Технічні вимоги

5.1 Топологія мережі – комбінована:

- сегмент – моноканал;
- з'єднання з центральним офісом (ЦО) – радіальне.

5.2 Число периферійних відділень (ПВ) до 20:

- у сегменті до 5;
- у мережі до 115.

5.3 Періодичність опитування (періодичність сеансів) – 8 годин.

5.4 Обсяг сеансового масиву – не менше 200 Мб.

5.5 Вектори інформаційного потоку – двосторонній однакового обсягу:

- Висхідний (up stream) потік (від периферії до ЦО) – відомості про виконання доручень, наказів, вказівок, операційні звіти;
- спадний потік (від ЦО до периферії) – контроль обсягу звітів, команди керування філіями.

5.6 Обсяг інформаційних потоків у шлюзах не більше 1 Гб/добу.

5.7 Вимоги до рівня безпеки - безпека інформаційного обміну на рівні С2.

					ЧДТУ 201850.005 ПЗ	Арк.
						6
Змн.	Арк.	№ докум.	Підпис	Дата		

Небезпечні події і явища:

- У спадному потоці - перехоплення керування банківським процесом, модифікація команд керування;
- У висхідному потоці- несанкціоноване читання відомостей про розмір фінансових потоків й модифікація даних про розмір потоків.

5.8 Імовірність втрат пакетів –  $10^{-5}$ .

5.9 Імовірність хибного спрацьовування системи захисту –  $10^{-6}$ .

5.10 Ймовірність помилки -  $10^{-6}$ .

					ЧДТУ 201850.005 ПЗ	Арк.
						7
Змн.	Арк.	№ докум.	Підпис	Дата		



## 2. ХАРАКТЕРИСТИКА АНАЛОГІВ І ПРОТОТИПІВ БАНКІВСЬКИХ МЕРЕЖ

Корпоративна мережа А-банку в Черкасах складається із декілька філій, яка взаємодіє із банкоматами, обмінюючись інформацією. Крім того, вони взаємодіють із зовнішніми системами. Корпоративна мережа забезпечує цю передачу інформації, а також доступ до інтернету.

До існуючих аналогів розроблюваного серверного сегменту банку можна віднести такі рішення:

1. Корпоративна мережа «Черкаського облавтодору»;
2. Корпоративна мережа Черкаської облдержадміністрації;
3. Корпоративна мережа ВАТ «Ощадбанк»

### 2.1 Корпоративна мережа «Черкаського облавтодору»

Мережа виконує завдання що до дистанційного керування районними філіями Автодору, облік та аудит стану фінансування, автоматизоване ведення БД, контроль обсягу поточного виробництва та здійснення ремонтних робіт автошляхів та узбічч, нагляд за станом розв'язок, мостів, пандусів та труб. Епіцентр мережі - Черкаси, філії - районні центри. Топологія корпоративної мережі аналога приведена на рисунку 2.1. [14]

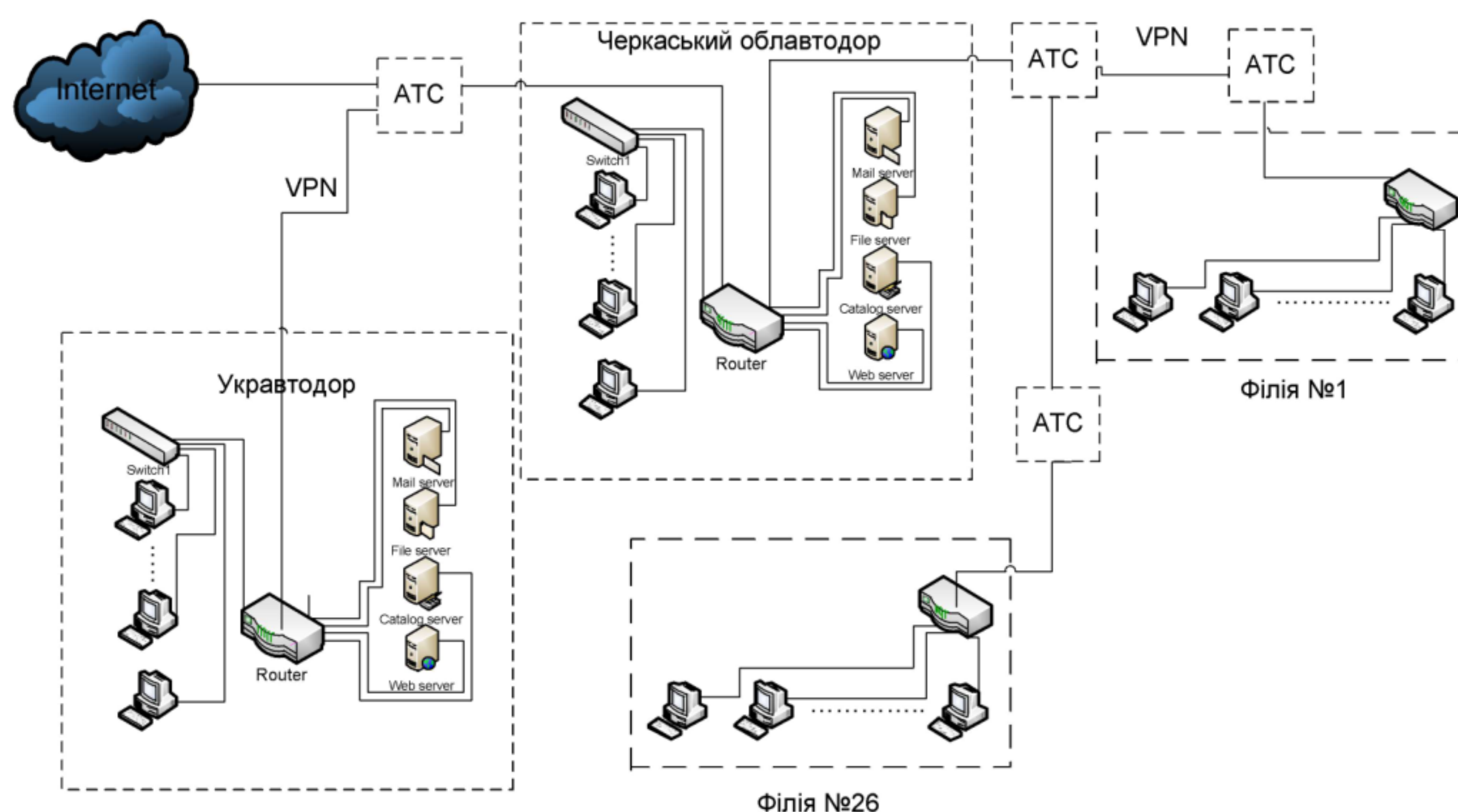


Рисунок 2.1- Корпоративна мережа «Черкаського облавтодору»

					ЧДТУ 201850.005 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		8



Сполучення з іншими мережами забезпечується каналами телефонної мережі загального користування.

Топологія мережі: з'єднання філій з головним офісом - радіальне. Об'єм сеансу - 310 Мбайт.

Мережа налічує: 4 сервери та 250 хостів.

Укравтодор з'єднується з головним офісом «Облавтодору» за технології VPN. Черкаський «Облавтодор» з'єднується з філіями за технологій IP-VPN і xDSL. Безпека інформаційного обміну на рівні С2.

**2.2 Корпоративна мережа Черкаської облдержадміністрації**

Топологія – розподілена «зірка». Центр – Черкаси; периферійні центри – районні центри Черкаської області. Мережа побудована на оптичних та телефонних каналах (ТМЗК). Топологія корпоративної мережі приведена на рисунку 2.2. [16]

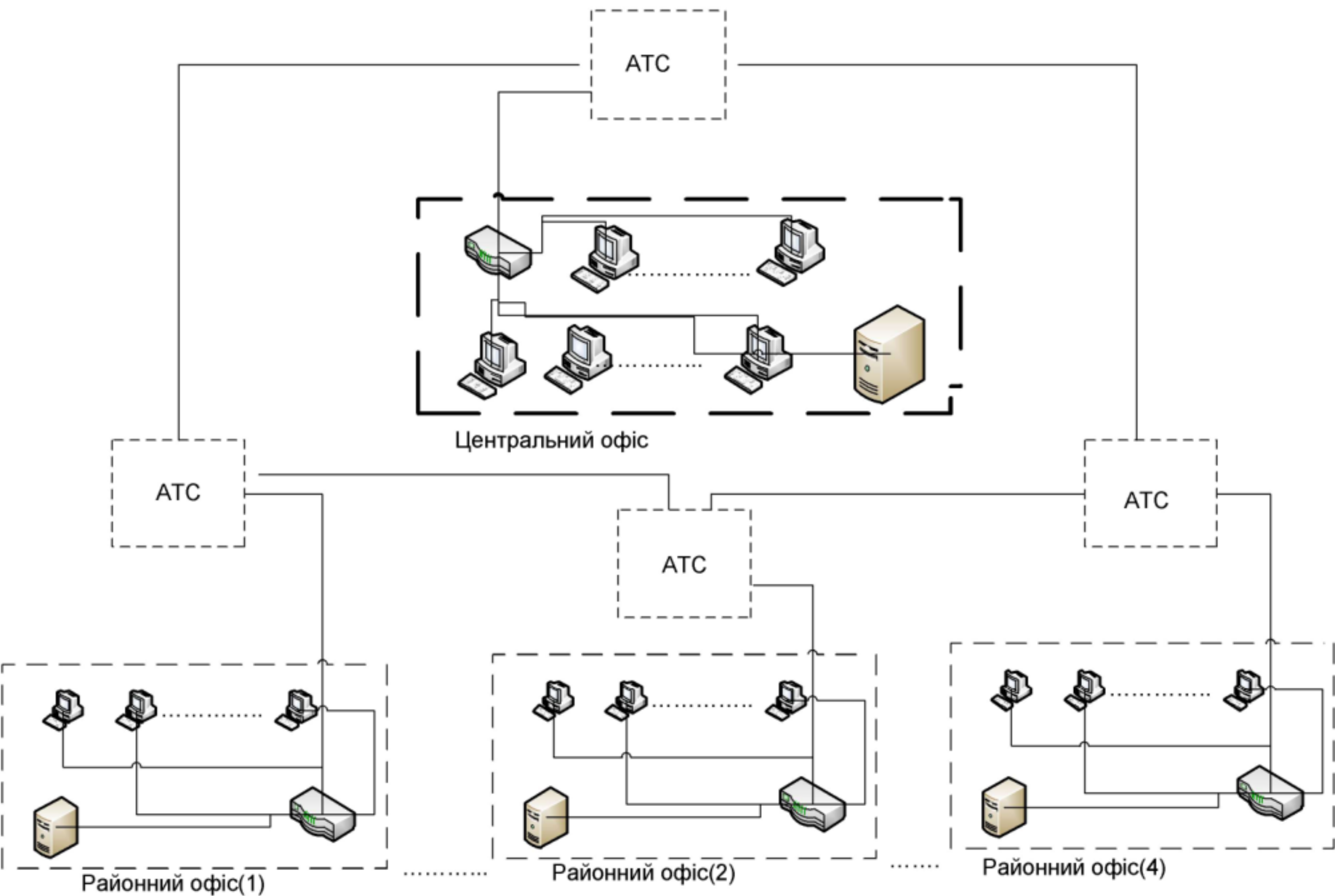


Рисунок 2.2 - Корпоративна мережа Черкаської облдержадміністрації

Кожний районний офіс має до 25 робочих станцій, сполучених Fast Ethernet з'єднаннями, а зв'язок з центральним офісом реалізовано по каналу ТЧ за допомогою технології IP-VPN. В кожній районій раді є власний



локальний сервер з локальною БД, з управляючими програмами і т.і. Комутатори цих частин під'єднані до головного комутатора адміністрації, який в свою чергу з'єднаний з сервером.

Регіональні центри зв'язані з мережею інтернет двома оптичними каналами. Один канал призначений для внутрішнього трафіку, а другий канал для веб – трафіку, який генерується користувачами інтернет сайту облдержадміністрації, відвідувачами сайту адміністрації та працівниками інших компанії, які користуються веб – інтерфейсом сайту. Добова частка інформації сеансу становить - 625 Мегабайтів. Безпека інформаційного обміну зафіксована на рівні С2.

### **2.3 Корпоративна мережа ВАТ «Ощадбанк»**

Враховуючи територіальну розподіленість філій банку, в якості транспорту магістралі узята мережа Frame Relay, (рисунок 2.3).

Топологія мережі міх: у сегменті – розподілена «зірка»; а філії сполучені з центром – топологією «дерево».

Первинна комп'ютерна мережа реалізована в двох видах: оптоволокну та телефонні канали ТЧ- мережа загального користування (ТМЗК).

Сполучення з іншими мережами виконано телефонною мережею загального користування (ТМЗК). [15]

Обсяг сеансового масиву – 1,15 Гбайт.

Забезпечена безпека інформаційного обміну (рівень С2).

					ЧДТУ 201850.005 ПЗ	Арк.
						10
Змн.	Арк.	№ докум.	Підпис	Дата		



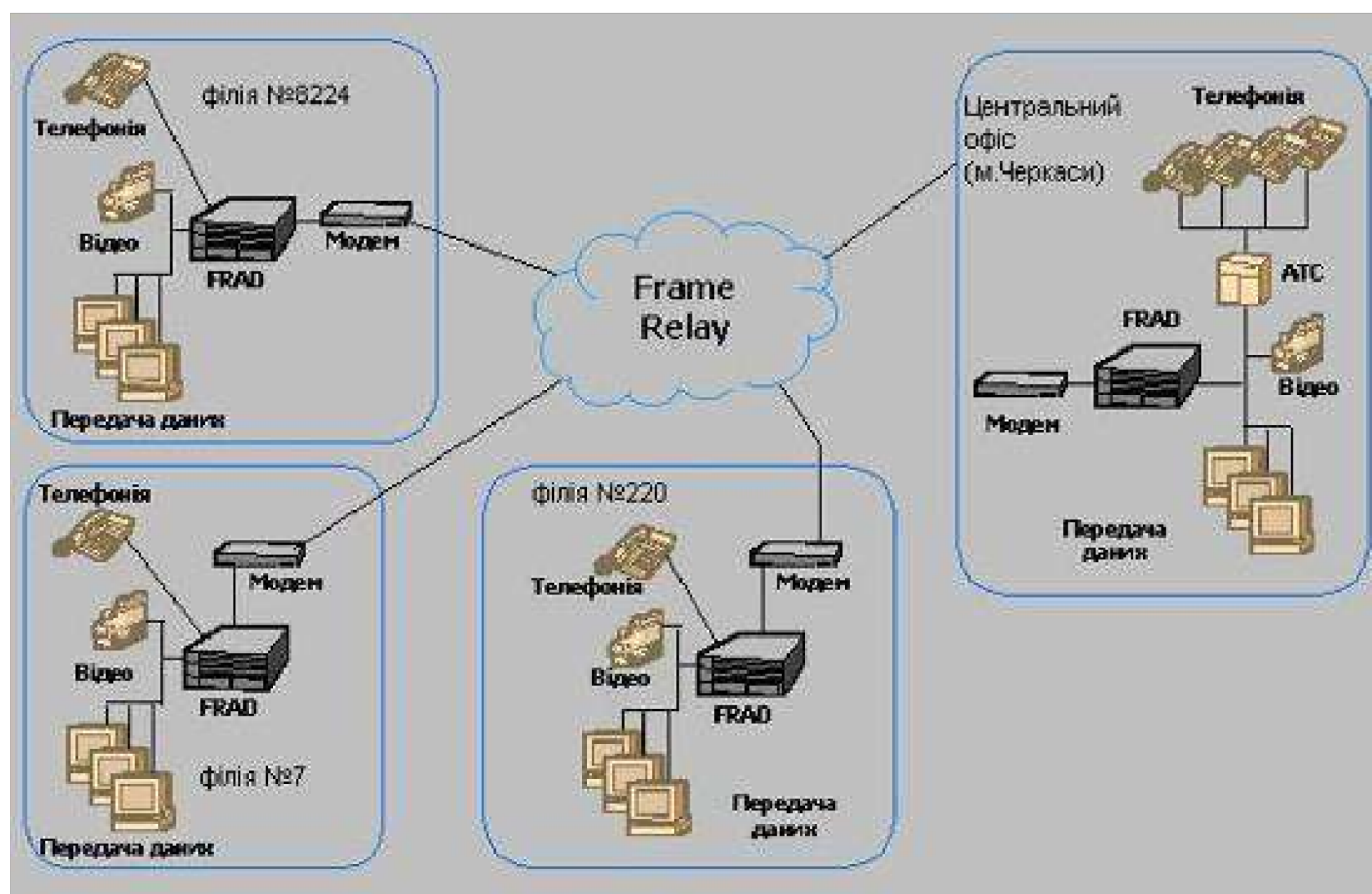


Рисунок 2.3 - Корпоративна мережа ВАТ «Ощадбанк»

Frame Relay гарантує можливість передачі даних з комутацією пакетів через інтерфейс між маршрутизаторами, мостами, головними машинами - мейнфреймами і обладнанням мережі (наприклад, комутуючими вузлами).

В таблиці 2.1 здійснено порівняння основних показників наведених вище аналогів. В усіх аналогах забезпечено рівень безпеки С2, вони мають однаковий режим обміну. Мережі «Черкаського облавтодору» та «Ощадбанку» використовують радіальні топології, а мережа облдержадміністрації – змішану. В залежності від об'єму інформації всі аналоги мають різний інформаційний обсяг потоків, найбільший він у корпоративної мережі ВАТ «Ощадбанк» - 1,15 Гбайт/добу. Крім того, ця мережа використовує технологію Frame Relay.



Таблиця 2.1 - Порівняльний аналіз прототипів корпоративних мереж

Параметри	Корпоративна мережа «Черкаського облавтодору»	Корпоративна мережа Черкаської облдержадміністрації	Корпоративна мережа ВАТ «Ощадбанк»
Інформаційний обсяг потоків за добу	310 Мбайт	625 Мбайт	1,15Гбайт
Безпека інформаційного обміну	(рівень C2)	(рівень C2)	(рівень C2)
Топологія мережі	Радіальна	Змішана	Радіальна
Використання технологій	VPN, IP-VPN,	VPN, IP-VPN	Frame Relay
Режим обміну	Інформаційний потік двосторонній	Інформаційний потік двосторонній	Інформаційний потік двосторонній
Канали	PSTN	PSTN	PSTN

## Висновки до розділу 2

Отже, в другому розділі приведені аналоги комп'ютерних систем серед підприємств до теми кваліфікаційної випускної роботи. Розроблена таблиця 2.1, в якій порівняні основні параметри і характеристики даних прототипів.

За результатами проведеного дослідження структури інформаційних потоків, топології і конфігурації, зазначені переваги і недоліки прототипів комп'ютерних мереж для підприємств, визначено їх технології та обладнання, що задіяно в системі.

Дані порівняння допоможуть при виборі мережних технологій, апаратного та програмного забезпечення для проектованої мережі.

					ЧДТУ 201850.005 ПЗ	Арк.
						12
Змн.	Арк.	№ докум.	Підпис	Дата		

### 3. АНАЛІЗ ПРИНЦИПІВ ПОБУДОВИ МЕРЕЖ

#### 3.1 Технологія VPN

Технологія VPN (Virtual Private Network) для віддалених філій є відмінним методом сполучення окремих хостів або локальних мереж у віртуальній приватній мережі, із забезпеченням цілісності і безпеки інформації. Мережа VPN має властивості окремої приватної мережі і дозволяє передавати дані поміж декількома комп'ютерами через проміжну мережу (internetwork), наприклад Internet. В цей рік, коли вся держава потерпає від епідемії корона вірусу, коли як ніколи актуальним постає питання дистанційного навчання по захищених каналах зв'язку, тестування, віртуальних захистів дипломів та іспитів, ця технологія VPN набуває особливого значення.

Система безпеки VPN захищає всю корпоративну інформацію від несанкціонованого доступу. Вся інформація передається в зашифрованому вигляді. Найчастіше використовуваним алгоритмом кодування є 3DES, який забезпечує потрійне шифрування. Достовірність включає в себе перевірку цілісності даних та ідентифікацію користувачів VPN. Для побудови VPN необхідно мати на обох кінцях лінії зв'язку програми шифрування вихідного і дешифрування вхідного трафіку. Вони можуть працювати як на спеціалізованих апаратних пристроях, так і на ПК з такими ОС як Windows, Linux або NetWare.

Управління доступом, аутентифікації та шифрування - найважливіші елементи захищеного з'єднання. Основи «тунелювання» (tunneling), або інкапсуляція (encapsulation), - це спосіб передачі кадрів (пакетів) іншого протоколу через проміжну мережу.

VPN працює завдяки протоколу PPP (Point-to-Point Protocol), який був розроблений для передачі даних по телефонних лініях. PPP інкапсулює пакети IP, IPX і NetBIOS в кадри PPP і передає їх каналом "точка-точка".

					ЧДТУ 201850.005 ПЗ	Арк.
						13
Змн.	Арк.	№ докум.	Підпис	Дата		



Протокол PPP може використовуватися маршрутизаторами, з'єднаними виділеним каналом, або клієнтом і сервером RAS, з'єднаними віддаленим підключенням.

Основні компоненти PPP: інкапсуляція для мультиплексування декількох транспортних протоколів по одному каналу; протокол LCP; у якості протоколів аутентифікації використовують PAP, CHAP і ін.

Для формування тунелів VPN використовуються протоколи PPTP, L2TP, IPsec, IP-IP. [1]

Для апаратної та програмної реалізації VPN, окрім стандартного мережевого обладнання, потрібно використати шлюз (gate) VPN, що виконує функції по формуванню тунелів, централізованого управління, захисту інформації, контролю трафіку, тощо.

### 3.2 Технологія Frame Relay

Мережа Frame Relay (FR) є мережею з ретрансляцією кадрів, підтримує фізичний і канальний рівні OSI. Технологія FR використовує для передачі даних техніку віртуальних каналів (комутованих і постійних).

FR орієнтована на цифрові канали передачі даних хорошої якості, тому в ній відсутня перевірка виконання з'єднання між вузлами і контроль достовірності даних на канальному рівні. За рахунок цього мережі FR мають високу продуктивність. При виявленнях помилок в кадрах повторна передача кадрів не виконується, а спотворені кадри відкидаються. Контроль достовірності даних здійснюється на вищих рівнях моделі OSI.

Технологія FR використовується для маршрутизації протоколів локальних мереж через загальні (публічні) комунікаційні мережі. У мережах FR можлива передача трафіку чутливого до затримок (голосових і мультимедійних даних). У магістральних каналах FR використовуються волоконно-оптичні кабелі, а в каналах доступу застосовують недешева, але ж якісна вита пара категорій 5e - 7.

					ЧДТУ 201850.005 ПЗ	Арк.
						14
Змн.	Арк.	№ докум.	Підпис	Дата		





Рисунок 3.1 - Структурна схема мережі FR

На рисунку 3.1 представлена структурна схема мережі FR, де DTE – апаратура передачі даних ,DCE – кінцеве устаткування каналу ПД.

*Фізичний рівень FR* використовує цифрові призначені канали зв'язку, протокол фізичного рівня I.430/431.

#### *Канальний рівень FR*

У мережі FR використовується два типи віртуальних каналів постійні (PVC) та комутовані віртуальні канали. На каналному рівні потік даних структурується на кадри ( фрейми), поле даних в кадрі має змінну величину, але не більше 4096 байт. Канальний рівень реалізований протоколом LAR-F, який має два режими роботи: основний і такий, що керує. Віртуальному з'єднанню привласнюється певний номер DLCI - ідентифікатор з'єднання каналу даних.

Комутовані віртуальні канали використовуються для передачі імпульсного трафіку між двома пристроями DTE. Постійні віртуальні канали застосовуються для постійного обміну повідомленнями між двома пристроями DTE.

#### **Переваги мережі FR:**

- висока надійність роботи мережі;
- забезпечення передачі чутливого до часових затримок трафіку (голос, відеозображення).

					ЧДТУ 201850.005 ПЗ	Арк.
						15
Змн.	Арк.	№ докум.	Підпис	Дата		

### Недоліки мережі FR:

- висока вартість якісних каналів зв'язку;
- не забезпечується достовірність доставки кадрів.

### 3.3 Технологія Fast Ethernet

Технологія Fast Ethernet є розвитком технології Ethernet. Завдяки застосуванню нових методів кодування стало можливим:

- збільшення пропускної спроможності мережі до 100 Мб/с;
- збереження методу доступу CSMA/CD;
- збереження зіркової топології мереж і підтримка традиційних середовищ передачі - витії пари UTP і оптоволокна SMF (MMF).

Всі відмінності Fast Ethernet від Ethernet зосереджені на фізичному рівні, як вказано на рисунку 3.2. Тому розглядаючи FastEthernet, ми вивчатимемо тільки декілька варіантів її фізичного рівня.

Більш складна структура фізичного рівня технології Fast Ethernet викликана тим, що в ній використовуються три варіанти кабельних систем:

- волоконно-оптичний кабель SM, MM, використовуються два волокна;
- вита пара категорії 5, 100BaseT2, використовуються дві пари;
- вита пара категорії 3, 100BaseT4, використовуються чотири пари.

Fast Ethernet притаманно скорочення діаметру мережі до 200 м, та збільшення швидкості передачі в 10 разів в порівнянні з 10BaseT.

					ЧДТУ 201850.005 ПЗ	Арк.
						16
Змн.	Арк.	№ докум.	Підпис	Дата		



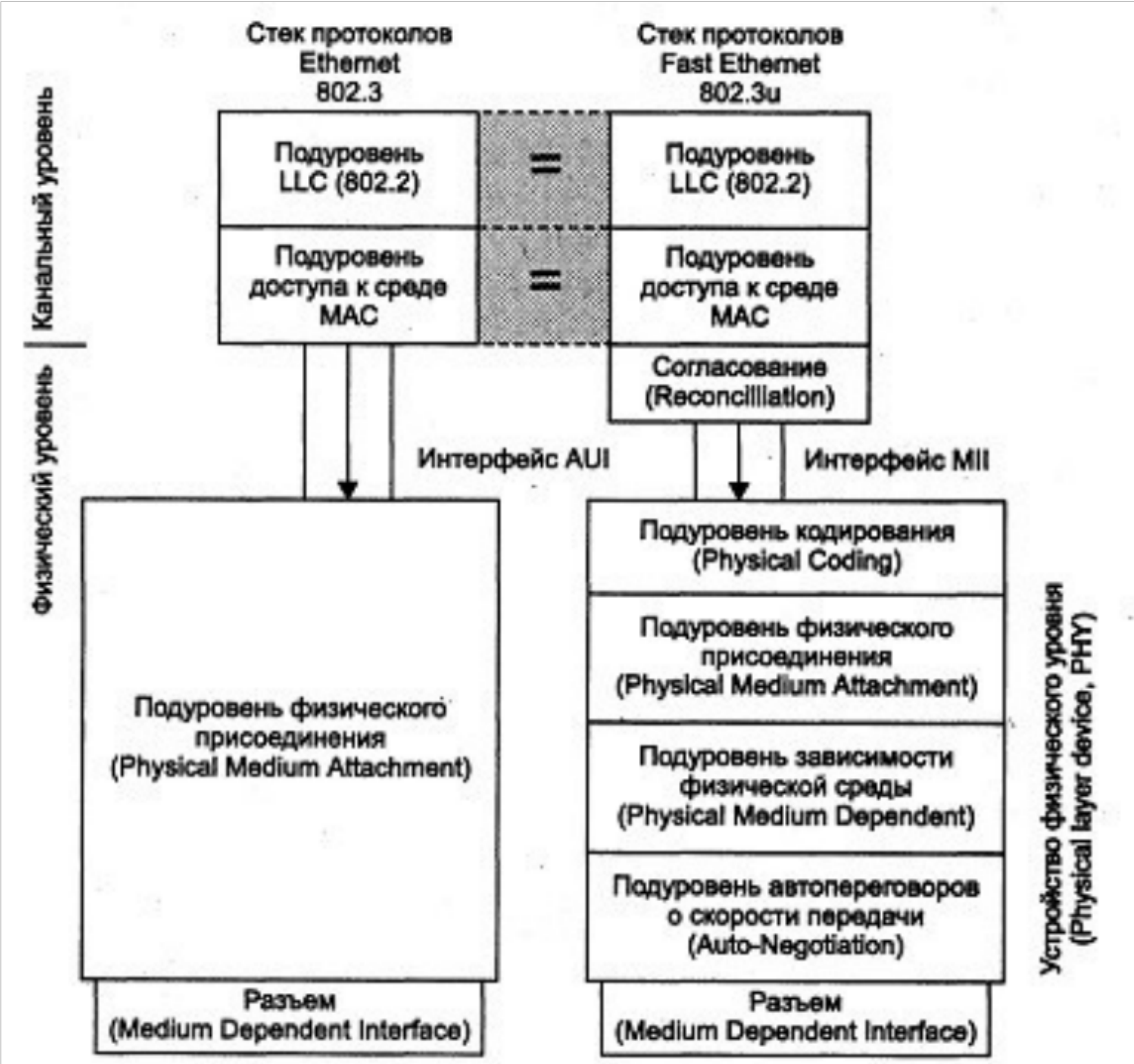


Рисунок 3.2 - Порівняння технології Fast Ethernet з технологією Ethernet

Мережі Fast Ethernet мають топологію "зірка - розподілена зірка", для сполучення використовують виту пару категорій 3-5 та хаби. Можна застосовувати й оптичні кабелі. Стандартна максимальна відстань між двома станціями - 210м. Між двома станціями не може бути більше двох репітерів. За допомогою стекових репітерів, біджей, роутерів та свічів до мережі можна приєднати будь- яку кількість ділянок Fast Ethernet.

На підставі наведеного аналізу можна виділити такі 2 коректні структури мереж:

модель 1 передбачає, що всі елементи мережі вносять максимальні (визначені стандартом для цих типів елементів) затримки;

модель 2 побудована на реальних затримках, однак має складні методики розрахунку цих затримок.

Робота мережі 100Base-TX та 100Base-FX на фізичному рівні ґрунтується на специфікації PMD ANSI, розроблену для волоконно-оптичних мереж. PCS одержує обмежені стартовими та стоповими бітами байти даних зі швидкістю 100 Мбіт/с в напівдуплексі і перетворює їх у безперервний



потік, передавання якого відбувається зі швидкістю 125 Мбіт/с у дуплексі. Для цього використовують кодування 4В5В .

### 3.4 Технологія Gigabit Ethernet

Технологію Gigabit Ethernet розроблено у 1997 році об'єднанням Gigabit Ethernet Alliance. У 1998 році технологію комітет IEEE 802 було затверджено стандартом 802.3z.

Характерні особливості:

- Швидкість передавання даних на верхніх рівнях – 1000 Мбіт/с.
- Збережені формати кадрів Ethernet.
- Збережений метод доступу CSMA/CD до середовища.
- Топологія – ієрархічне дерево на одному хабі з діаметром до 200 м.
- Використання комутаторів з повним дуплексом передавання даних.
- Фізичне середовище – оптоволокно, вита пара UTP 5е категорії.

Мінімальний розмір кадру збільшено з 64 байт до 512 байт (4096 біт). Це збільшило час подвійного обороту сигналу до 4096 bt. За потреби передати декілька коротких кадрів (наприклад, квитанцій) станціям дозволено збільшувати загальну довжину до 8192 байт. Типи кабелів та типі видів технології 802.3z, показані на таблиці [1].

### 3.5 10 GB Ethernet

Стандарт 10-гігабітного Ethernet містить у собі сім стандартів фізичного середовища для LAN, MAN, WAN і GAN. Відповідає стандарту IEEE 802.3ae і входить до ревізії стандарту IEEE 802.3.

Технологію 10GBASE-CX4 для коротких відстаней (до 15 м.), з використанням кабелю CX4 і конекторів InfiniBand, а також, і 10-гігабітну 10GBASE-SR (до 26 або 82 метрів, залежно від типу кабелю), 10GBASE - LX4 (240 до 300 метрів по багатомодовому волокну), не аналізуємо. З причин

					ЧДТУ 201850.005 ПЗ	Арк.
						18
Змн.	Арк.	№ докум.	Підпис	Дата		

обмежень діючих відстаней від 0,3 км та вище.

10GBASE -LR і 10GBASE -ER - ці стандарти підтримують відстані до 10 і 40 кілометрів відповідно.[1]

Наступні різновиди десятигігабітних технологій передавання даних 10GBASE-SW, 10GBASE- LW і 10GBASE- EW – використовують фізичний інтерфейс, сумісний за швидкістю і формату даних з інтерфейсом оптичних кабелів OC-192/STM-64, стандарту оптоволоконних мереж SONET/SDH. Вони подібні до стандартів 10GBASE-SR, 10GBASE-LR і 10GBASE-ER відповідно, оскільки використовують ті ж самі типи кабелів і відстані передачі. Стандарт для застосування СКС в приміщенні, чи поверсі 10GBASE-T, IEEE 802.3an-2006 – використовує виту пару категорії 6 (максимально - 55 метрів) і 6а (максимально 100 метрів). Для з'єднань серверів у ферму, чи кластер передбачена 10GBASE-KR – технологія 10-гігабітного Ethernet для крос-плат (backplane/midplane) модульних комутаторів/маршрутизаторів і серверів (Modular/Blade).

### 3.6 PPPoE

PPPoE (Point-to-point Protocol over Ethernet) — мережний протокол передачі кадрів канального рівня PPP через середовище Ethernet. Ця технологія, в основному, використовується xDSL-сервісами. Окрім передавання кадрів протокол надає додаткові можливості (автентифікації, стиснення, шифрування).

PPPoE – працює як тунельний протокол, який налаштовує (або інкапсулює) дані за протоколом IP, або за іншими протоколами канального рівня на PPP, через з'єднання Ethernet, але з програмними можливостями. PPP з'єднання використовується для віртуальних «дзвінків» на суміжну Ethernet-машину і встановлює з'єднання «крапка-крапка» для транспортування IP-пакетів. Саме головне, що це дозволяє застосовувати традиційне PPP-орієнтоване ПЗ для налаштування з'єднань, які

					ЧДТУ 201850.005 ПЗ	Арк.
						19
Змн.	Арк.	№ докум.	Підпис	Дата		



використовують не послідовний канал передавання даних, а пакетно-фреймову орієнтовану мережу (як Ethernet), а це дозволяє організувати класичне з'єднання з логіком та паролем для Інтернет-з'єднань. Також, динамічна IP-адреса по інший бік з'єднання призначається тільки коли PPPoE з'єднання відкрито.

Функціонування технології PPPoE відбувається наступним чином: Ethernet-середовище, та кілька з'єднаних мережевих карт, з апаратною адресацією кадрів MAC-адресами відправника та одержувача кадру, в залежності від типу кадру, прослуховують наявність сигналу передавання. Одну з карт слухає PPPoE-сервер. Клієнт посилає широкомовний Ethernet кадр, на який повинен відповісти PPPoE сервер. PPPoE сервер надсилає клієнту відповідь (адресу відправника кадру та свою MAC-адресу, адресу одержувача кадру - MAC-адресу клієнта і тип кадру - PPPoE Active Discovery Offer). Якщо в мережі декілька PPPoE серверів, то всі вони посилають відповідь. Відбувається класична процедура аутентифікації за клієнт-серверною технологією з наданням унікального ідентифікатору сесії і кадрам сесії. Віртуальний канал ідентифікується ідентифікатором сесії і апаратними MAC-адресами клієнта і сервера. Згодом у каналі «піднімається» PPP з'єднання, в яке інкапсулюється IP -трафік.

Зміна VPN на PPPoE виконується в такі кроки:

- 1) Відключення маршрутів LAN.
- 2) Видалення VPN з'єднання.

Для налаштування PPPoE «з нуля» необхідно тільки наступне:

- для захисту від конфліктів IP-адрес і атак необхідно відключення протоколу TCP / IP на мережевої карти ;
  - Створення PPPoE з'єднання з номером договору та паролем VPN.
- 3) зростає безпека: тепер користувачеві не страшні ніякі «атаки» через локальну мережу.

Технологія з'єднання PPPoE має такі переваги:

					ЧДТУ 201850.005 ПЗ	Арк.
						20
Змн.	Арк.	№ докум.	Підпис	Дата		



- відсутня проблема працездатності VPN-через-VPN, яка часто виникала у тих користувачів, хто використовував VPN для віддаленої роботи.
- з'являється можливість використання шлюзів IP-телефонії. Наприклад, модель D-Link DVG-2001S, з підтримкою PPPoE, налаштовується на з'єднання з сервісом sipnet.ua і вуаля – отримуємо стаціонарний телефон з безкоштовними дзвінками на міські номери.
- з'являється можливість використовувати роутери будь-яких моделей, а не тільки моделі, що підтримують VPN.

### 3.7 MPLS

MPLS є ефективною комунікаційною мережею, яка легко створює віртуальні канали між вузлами мережі і дозволяє інкапсулювати різні протоколи передачі даних.

MPLS може бути використаний для передачі різного виду трафіку, включаючи IP-пакети, фрейми SONET/SDH, кадри Ethernet і набору сигнальних протоколів, характерних для банкоматів. (рисунок 3.3).

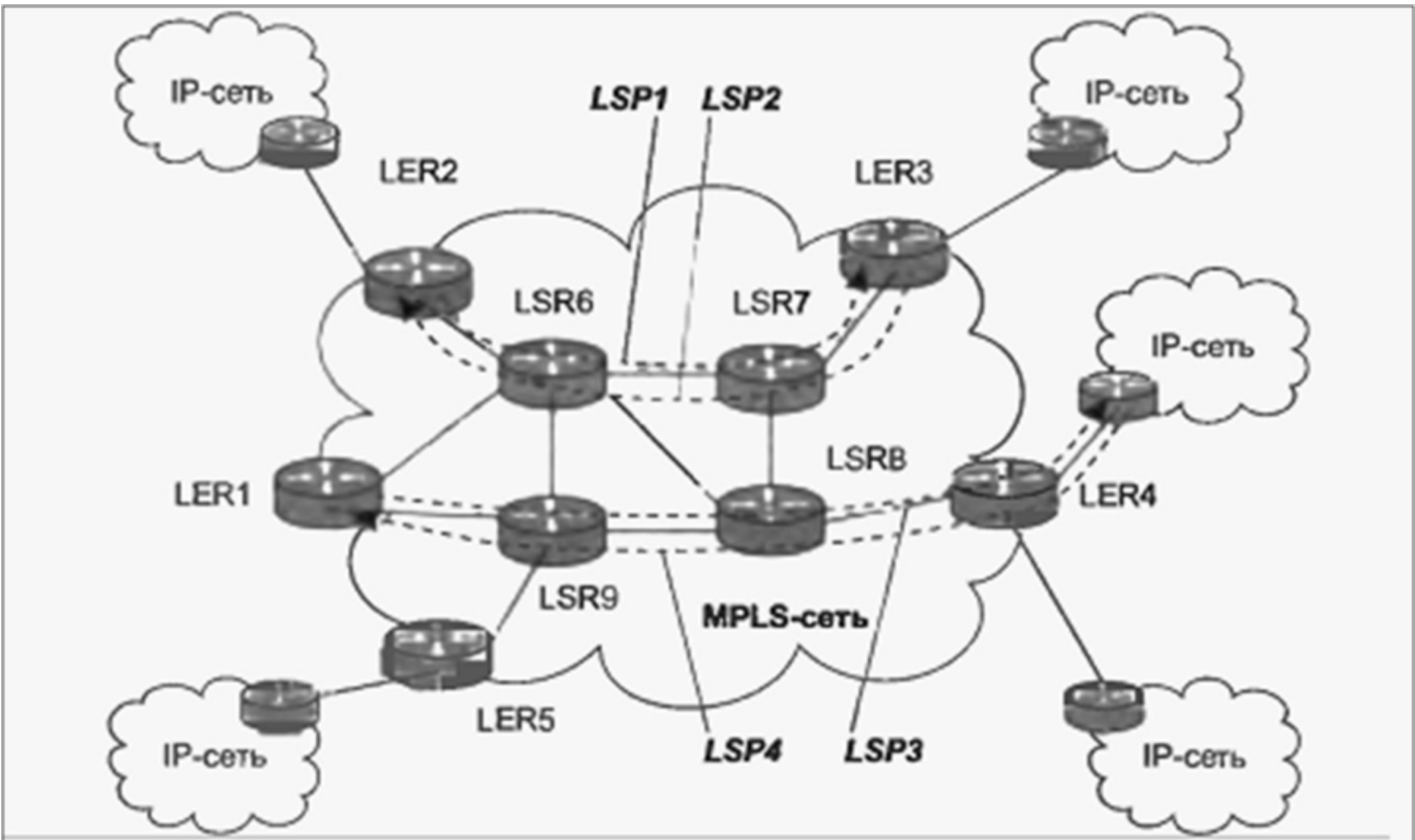


Рисунок 3.3 - MPLS-мережа

Багатопротокольність технологій MPLS полягає в тому, що вона використовує протоколи маршрутизації стеків TCP/IP, та IPX/SPX. В

останньому випадку замість протоколів маршрутизації RIP та OSPF застосовується протокол RIP IPX або ж NLSP, а загальна архітектура LSR зостанеться такою ж.

Головною перевагою технології MPLS є здатність надавати різноманітний транспортний сервіс в IP-мережах, і як найперше - сервіси віртуальних приватних мереж VPN. Цей сервіс може подаватися як на мережевому, так і на каналному рівні. Крім того, MPLS доповнює IP-мережі такою важливою властивістю, як передача трафіку у віртуальних каналах, що дозволяє вибирати потрібний режим передачі трафіку. Віртуальні канали MPLS забезпечують інженіринг трафіку, саме вони підтримують детерміновані маршрути.

Технологія меток в мультипротокольних мережах базована на обробці заголовка MPLS, який додається до кожного пакету даних. Заголовок складається з однієї або кількох «міток». Стеком міток називають кілька записів (міток) в заголовку MPLS. В кожному запису в стеку є наступні чотири поля:

- 1) Значення мітки. Займає 20 біт.
- 2) Клас трафіку (Traffic Class), необхідного для реалізації механізмів QoS (якість обслуговування) і наявного повідомлення про перевантаження (ECN). Має обсяг 3 біти.
- 3) Прапорець дна стеку (Bottom of stack). Якщо флаг (1 біт) має значення «одиниця», тобто встановлений, то поточна мітка остання в стеці.
- 4) Поле TTL (Time To Live). Поле «час життя» займає 8 біт.

У MPLS маршрутизаторі пакет з MPLS міткою комутується на наступний порт після пошуку мітки в таблиці комутації замість пошуку в таблиці маршрутизації.

Маршрутизатори, розташовані на вході або виході MPLS мережі називаються LER (Label Edge Router - граничний маршрутизатор міток). LER на вході в MPLS мережу додають мітку MPLS до пакету даних, а LER на

					ЧДТУ 201850.005 ПЗ	Арк.
						22
Змн.	Арк.	№ докум.	Підпис	Дата		



виході з MPLS мережі видаляє мітку MPLS з пакету даних. Маршрутизатори, виконують маршрутизацію пакетів даних, які покладаються тільки на значенні мітки називаються LSR (англ. Label Switching Router - комутуючий мітки маршрутизатор). У деяких випадках пакет даних який надійшов на порт LER вже може містити мітку, тоді новий LER додає другу мітку в пакет даних.

Мітки між LER і LSR розподіляються за допомогою LDP (Label Distribution Protocol - протокол розподілу міток). Для отримання повної картини MPLS мережі LSR постійно обмінюються мітками та інформацією про кожного сусіднього вузла, використовуючи стандартну процедуру. Віртуальні канали (тунелі), звані LSP (англ. Label Switch Path - Шляхи комутації міток) встановлюються провайдерами для вирішення різних завдань, наприклад для організації віртуальних приватних мереж або для передачі трафіку через мережу MPLS по вказаному тунелю. Багато в чому LSP нічим не відрізняється від PVC в мережах ATM або Frame Relay за винятком того, що LSP не залежать від особливостей технологій каналного рівня.

При описі віртуальних приватних мереж, заснованих на технології MPLS, розташовані на вході або виході мережі LER зазвичай називаються PE маршрутизатори (англ. Provider Edge - маршрутизатори на межі мережі провайдера), а вузли, що працюють як транзитні маршрутизатори, називаються P маршрутизатори (англ. Provider - маршрутизатори провайдера).

Існує два стандартних протокола управління тунелями в MPLS-мережі. LDP (англ. розподілу міток протоколу - протокол розподілу міток) і RSVP-TE, розширення RSVP (англ. Протокол резервування ресурсів - протоколу резервування мережевих ресурсів) для оптимізації та управління трафіком. Також існують розширення протоколу BGP, здатні керувати віртуальними каналами в MPLS-мережі.

					ЧДТУ 201850.005 ПЗ	Арк.
						23
Змн.	Арк.	№ докум.	Підпис	Дата		

MPLS не вказує тип даних, що передаються до MPLS тунелю. У разі, якщо виникає необхідність передати два різних типи трафіку між двома маршрутизаторами так, щоб вони по різному обробляли маршрутизаторами ядра мережі MPLS, необхідно встановити два різних MPLS тунелі для кожного типу трафіку.

З точки зору користувачів безперечними перевагами MPLS є істотне підвищення якості роботи (QoS) і значно спрощене побудова захисту доступу до VPN (Virtual Private Network). При використанні MPLS відпадає необхідність у додатковому шифруванні та інших підвищених заходах безпеки. До того ж по мережі на основі MPLS можуть передаватися будь-які дані, оскільки вміст пакета залишається незмінним протягом всього шляху - замінюються лише позначки. Як наслідок, користувачі можуть передавати з CHC, SPX/IPX-, IP-пакети з невирішеними адресами (RFC 1918), кадри Frame Relay або комірки ATM і т.д. Однак на відміну від віртуального каналу фіксований шлях MPLS надається у вигляді частини інтерфейсу IP, тому для його використання не доведеться робити ніяких спеціальних дій з налаштування. В кінцевому варіанті мережу на базі MPLS містить параметр, що описує, як відрізнити трафік цієї VPN. Так, при вступі на IP-інтерфейс Інтернет-провайдера потік IP-пакетів буде аналізуватися прикордонним пристроєм MPLS, і відповідають критерію VPN пакети будуть направлені по шляху MPLS для подальшої обробки. Подібна модель відкриває можливості для появи зовсім нових видів послуг, а саме: VPN з підтримкою Microsoft NetMeeting від може бути запущена на певний час на плановій основі для підтримки низки користувачів в кількох місцях, а по настанні встановленого терміну трафік буде автоматично маршрутизовуватися в MPLS VPN без втручання користувача. Шляхи MPLS будуть ліквідовані, і той же самий трафік буде оброблятися, як завжди, наприклад - спрямовуватися через Інтернет. Крім цього VPN на основі MPLS може виконувати й інші завдання, зокрема цілодобово підтримувати роботу критично важливих додатків. В

					ЧДТУ 201850.005 ПЗ	Арк.
						24
Змн.	Арк.	№ докум.	Підпис	Дата		



цьому випадку провайдер послуг визначає фіксований шлях на термін контракту з користувачем. MPLS може залишатися в межах мережі провайдера послуг, надаючи користувачам чималі переваги, а може вийти за її межі і захопити зовнішній край локальних мереж або використовуватися при побудові корпоративних глобальних мереж. До того ж чим ближче MPLS до додатків, тим більше потенційних переваг вона здатна надати.

Безсумнівно, використання MPLS у корпоративних глобальних мережах з великим трафіком більш виправдано, ніж застосування нової архітектури в невеликих ЛОМ, так як ізоляція трафіку в локальних мережах не є проблемою для більшості користувачів, а вимоги до захисту реалізуються зазвичай на рівні додатків, так що відділення одного користувача від іншого не представляється складним. Тим не менш необхідність забезпечення QoS виникає досить часто, однак при постійному зниженні цін на комутатори для локальних мереж збільшення потужності пристроїв обійдеться дешевше, ніж запровадження MPLS для управління ними. Корисною областю застосування MPLS в локальній мережі є відділення неінформаційних трафіку від трафіку даних, оскільки аудіо-та відеоінформація може передаватися комутаторами MPLS з точністю, порівняною з результатами роботи за прямим з'єднанням.

### Висновки до розділу 3

В ході виконання третього розділу випускної роботи проведено аналіз актуальних принципів та технологій побудови розподілених мереж.

Отже, обрано сім технологій: VPN, Frame Relay, Fast Ethernet, Gigabit Ethernet, 10 GB Ethernet, PPPoE та MPLS.

Досліджені їх характеристики та вказано на переваги та недоліки кожної з технологій.

					ЧДТУ 201850.005 ПЗ	Арк.
						25
Змн.	Арк.	№ докум.	Підпис	Дата		

#### 4. ПОБУДОВА СЕРВЕРНОГО СЕГМЕНТУ МЕРЕЖІ БАНКУ

Оскільки мережа не вимагає завеликих перепускних здатностей, логічно використати для її побудови технологію DSL, а саме один з її варіантів ADSL (Asymmetric Digital Subscriber Line).

Сегмент корпоративної мережі А - банку складається з центрального філіалу? в якому розміщено основну базу даних та мережі банкоматів, за обслуговування яких відповідає окремий VPN сервер.

Відділення складається з п'яти робочих станцій, а також окремого файл-сервера. Всі робочі станції та сервер підключені до комутатора. У складі кожного відділення обов'язково присутній брандмауер, а також модем, який дозволяє отримувати доступ до мережі за допомогою телефонної мережі загального користування.

Філія банку має підключення до ТМЗК. Також використано резервування баз даних. У відділенні банку встановлено web-сервер, за допомогою якого відбувається доступ до баз даних. Всі підключення до глобальної мережі захищені брандмауерами.

##### 4.1 Опис предметної області

АТ «А-Банк» засновано в 1992 році під назвою «Кієвприватбанк», правонаступником якого став Український кредитний банк. У 2006 році в банк введена тимчасова адміністрація. Через рік група фізичних осіб, зокрема, В. Медведчук та І. Суркіс, реалізувала 37,5% акцій Приватбанку. Нові власники додатково розмістили в банку гарантійний депозит, з метою поповнення статутного капіталу. В 2007 році установа була перейменована в А-Банк, з розміщенням головного офісу в м. Дніпропетровськ.

З 2015 року контроль над А-Банком здійснюють брати Суркіси. Головні акціонери - Григорій (32,2%) , Ігор (32,43%), а також їх дочки Світлана (16,1%) і Марина (16,1%).

					ЧДТУ 201850.005 ПЗ	Арк.
						26
Змн.	Арк.	№ докум.	Підпис	Дата		



Універсальний комерційний банк Акцент-Банк (А-Банк) пропонує повний спектр фінансових послуг для своїх клієнтів і є учасником Фонду гарантування вкладів. Банк здійснює грошові перекази по території України і за її межі (Western Union, Unistream, Privat Money, Anelik, адресні перекази, Allure, MoneyGram, CoinStar) і входить в топ - 10 банків України (займаєсьоме місце).

Голова Правління А-Банку: Кандауров Ю. В. (з 03 вересня 2015 року).

**Реквізити**

Юридична назва

Акціонерне товариство «Акцент-Банк» (А-Банк)

МФО 307770 ЄГРПОУ 14360080 SWIFT UKCBUAUK

Главный офіс г. Днепр, ул. Батумская, 11 Email help@a-bank.com.ua

Банк незмінно входить до групи найбільших системних банків України, має розгалужену мережу банків-кореспондентів, яка включає фінансові установи із 110 країн світу. [3]. Розташування філії та банкоматів у місті Черкаси наведено на рис.4.1.

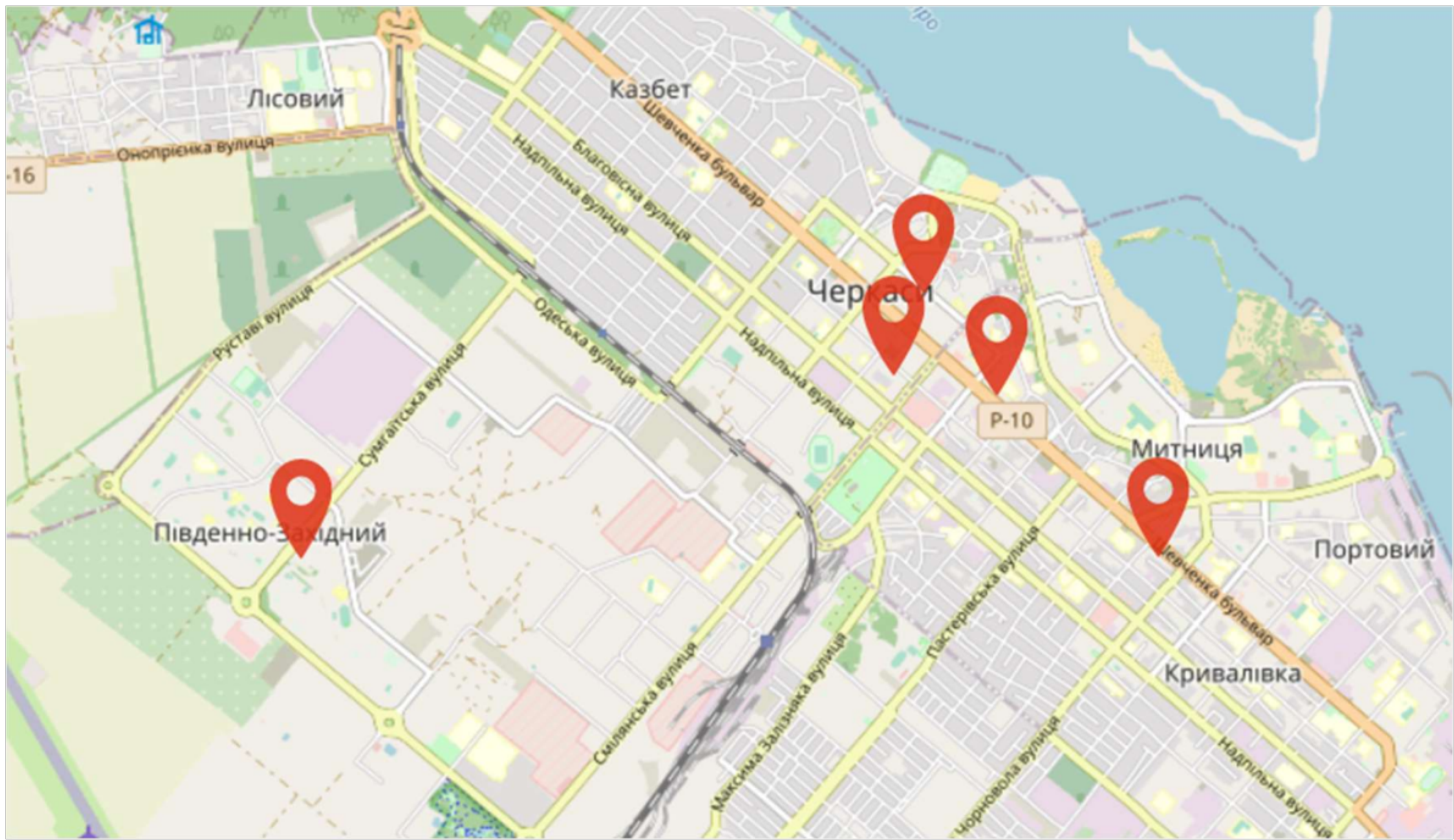


Рисунок 4.1 - Розташування філій та банкоматів А - ьпнку



## 4.2 Вибір комутаторів

Для даної мережі був обраний комутатор 3COM 3C16792B-ME (рис.4.2). Вибір був здійснений за критерієм ціна-якість.



Рисунок 4.2 – Зовнішній вигляд комутатора 3COM 3C16792B-ME

3COM 3C16792B-ME призначений для невеликих офісів і віддалених філій, що вимагають високої продуктивності мережі для обміну великими файлами даних і зображень, доступ до інформації в режимі реального часу. Можна розширити свою мережу шляхом додавання комп'ютерів або пристроїв зі швидкістю до 200 Мбіт / с на кожен порт в дуплексному режимі.

Цей комутатор автоматично регулює швидкість мережних пристроїв зв'язку на 100 або 10 Мбіт / с, тому комутатор може містити цілий ряд робочих груп і додатків. Автоматичний MDI / MDIX на кожному порту спрощує розширення мережі за рахунок усунення найбільш поширених кабельних помилок. [7]

Не потрібно ніякого програмного забезпечення для налаштування. Ці комутатори оснащені безвентиляторним дизайном, який забезпечує безшумну роботу.

## 4.3 Вибір ADSL модема

Для даної мережі був обраний модем TP-LINK TD-W8968. Вибір був здійснений за критерієм ціна-якість.

					ЧДТУ 201850.005 ПЗ	Арк.
						28
Змн.	Арк.	№ докум.	Підпис	Дата		





Рисунок 4.3 – Зовнішній вигляд модема TP-LINK TD-W8968

Модем (рис.4.3) TP-LINK TD-W8968 - це універсальне та надійне підключення вашого будинку або офісу до Інтернету по швидкісному каналу ADSL. До порту USB можна підключити будь-який комп'ютер, а до порту Ethernet - другий комп'ютер, приставку для прийому інтерактивного цифрового телебачення або цілу мережу через комутатор. Нова платформа забезпечує максимально ефективну роботу на будь-якій телефонній лінії, включаючи лінії з охоронно-пожежної сигналізації. Щоб налаштувати підключення до Інтернету і послугу інтерактивного цифрового телебачення, не потрібно вдаватися в технічні подробиці. Досить вибрати інтернет-провайдера і тариф із запропонованого списку. Функція (QoS) дозволяє адміністраторам виділяти певну ширину каналу для кожного підключеного до мережі пристрою, що визначається за IP-адресою. Пристрої, які виконують важливі завдання, завжди мають в своєму розпорядженні необхідну ширину каналу, що запобігає закупорки трафіку іншими користувачами в мережі. [8]

Підтримка нової версії протоколу IP - IPv6 робить доступним підключення до інтернет нового покоління і спектр нових послуг, що істотно розширює можливості користувачів.

#### 4.4 Вибір файл сервера

Для того щоб правильно вибрати файл сервер необхідно виходити від числа користувачів робочих груп і характеру завдань, вимог до складу

					ЧДТУ 201850.005 ПЗ	Арк.
						29
Змн.	Арк.	№ докум.	Підпис	Дата		



обладнання і програмного забезпечення сервера, до його надійності і продуктивності. Для даної мережі буде використано сервер HPE ProLiant ML10 Gen9 (рис.4.4). [9]



Рисунок 4.4 - Зовнішній вигляд файл сервера

Файл сервер HPE ProLiant ML10 Gen9 найбільш економічна серія серверів, призначається для обслуговування робочих груп або відділу підприємства: файлових сервісів, сервісів друку. Невисока ціна робить даний сервер привабливим.

*Характеристики:*

Процесор: *Чотириядерний Intel Xeon Quad-Core E3-1225 v5 (3.3 - 3.7 ГГц)*

Материнська плата: *чипсет: Intel C236*

Тип оперативної пам'яті: *DDR4 UDIMM - 2133 МГц ECC (1 x 8 ГБ, всього слотів: 4, макс. пам'ять: 4 x 16 ГБ, DDR4-2133 МГц ECC)*

Контролер сховища: *Вбудований Intel RST SATA RAID*

Обсяг оперативної пам'яті: *8 ГБ*

Жорсткий диск: *2 x 1 ТБ (3.5", SATA 3, 7200 об/хв) HPE LFF*

*Максимум: 6 шт NHP SATA LFF*

Оптичний привод: *DVD+/-RW*

					ЧДТУ 201850.005 ПЗ	Арк.
						30
Змн.	Арк.	№ докум.	Підпис	Дата		



#### 4.5 Вибір сервера

Головними критеріями при виборі сервера являються надійність, швидкість реагування, порівняно невелика ціна.

Даним критеріям задовольняє сервер Dell PowerEdge T20.(рис.4.5). [10]



Рисунок 4.5 - Зовнішній вигляд сервера Dell PowerEdge T20

*Характеристики:* Тип процесора: Чотириядерний Intel Xeon Quad-Core E3-1225 v3 (3.2 ГГц)

Материнська плата Чипсет: Intel C226

Тип оперативної пам'яті: UDIMM DDR3 1600 МГц

Контролери SAS/SATA: Intel Rapid Storage Controller 12.X

Обсяг оперативної пам'яті: 4 ГБ

Жорсткий диск: 1 ТБ 3.5" 7200 об/мин SATA HDD

Додаткові характеристики: Пам'ять з кодом корекції помилок (ECC)

Інтегрована відеокарта Intel HD Graphics P4600

програмний RAID

Блок живлення: 290 Вт

#### 4.6 Вибір робочої станції

У відділенні передбачається встановлення робочих станцій Acer Aspire Z1-623 (рис.4.6). Банкомати встановлюються стандартні модель CSC/450 [11]

					ЧДТУ 201850.005 ПЗ	Арк.
						31
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 4.6 - Зовнішній вигляд Acer Aspire Z1-623

Характеристики робочих станцій:

Процесор: двоядерний Intel Celeron N3050 (1.6 ГГц)

Обсяг оперативної пам'яті: 4 ГБ

Тип відеокарти: Інтегрована, Intel HD Graphics

Обсяг HDD: 500 ГБ (SATA 6.0 Гбіт / с)

Порти: 3 x USB 2.0

1 x USB 3.0

1 x LAN (RJ45)

2 x Аудіо порта

Потужність: 65 Вт

Бездротові технології: Wi-Fi 802.11 b / g / n

Попередньо встановлене ПЗ: Windows 10 Enterprise

Розміри: 452 x 295 x 29.9 мм

Дисплей: 18.5 "WXGA (1366x768)

Тип пам'яті: DDR3 - 1600 МГц

#### 4.7 Вибір брандмауера

Для даної мережі був обраний брандмауер D-Link DFL-260E (Рис.4.7). DFL-260 забезпечує закінчене рішення для управління, моніторингу та

					ЧДТУ 201850.005 ПЗ	Арк.
						32
Змн.	Арк.	№ докум.	Підпис	Дата		



обслуговування безпечної мережі. Серед функцій управління: віддалене управління, політики управління смугою пропускання, блокування по URL / ключовим словам, політики доступу і SNMP. Також підтримуються такі функції мережевого моніторингу, як повідомлення по e-mail, системний журнал, перевірка стійкості і статистика в реальному часі.

Брандмауер DFL-260 використовує унікальну технологію IPS - компонентні сигнатури, які дозволяють розпізнавати і забезпечувати захист, як проти відомих, так і проти нових атак. [12]



Рисунок 4.7 – Зовнішній вигляд брандмауера

#### Продуктивність системи:

- Продуктивність міжмережевого екрана: 150 Мбіт / с
- Продуктивність VPN: 45 Мбіт / с
- Продуктивність IPS: 60 Мбіт / с
- Продуктивність антівіруса: 35 Мбіт / с
- Кількість паралельних сесій: 25,0005
- Кількість нових сесій (в секунду): 2,000
- Політики: 500
- Прозорий режим
- NAT, PAT
- H.323 NAT Traversal
- Application Layer Gateway
- Активна мережева безпека
- Резервування каналу WAN

					ЧДТУ 201850.005 ПЗ	Арк.
						33
Змн.	Арк.	№ докум.	Підпис	Дата		

### Мережеві функції:

- DHCP сервер / клієнт
- DHCP Relay
- IEEE 802.1q VLAN: 8
- VLAN на основі портів
- IP Multicast: IGMP v3

### Висновки до розділу 4

Під час виконання четвертого розділу роботи побудовано серверний сегмент міської ділянки корпоративної мережі А-банку (топологія мережі та схема електрична з'єднань знаходяться відповідно в ДОДАТКУ А).

Проведено аналітичне дослідження предметної області випускної роботи та розглянуто структуру банку. За критерієм ціна / продуктивність / якість обрано потрібне апаратне забезпечення для синтезу мережі.

					ЧДТУ 201850.005 ПЗ	Арк.
						34
Змн.	Арк.	№ докум.	Підпис	Дата		



## 5. РОЗРАХУНОК ПАРАМЕТРІВ ПРОЕКТОВАНОЇ МЕРЕЖІ

Використовуючи математичний апарат теорії систем масового обслуговування, можна обчислити залежність часу передачі кадрів від швидкості роботи глобальної мережі без підключення до реальних каналів. Такі обчислення дозволяють відповісти на безліч питань щодо продуктивності мережі: який середній час затримки кадрів на мості/маршрутизаторі, як може вплинути на величину цих затримок зростання швидкості роботи каналу зв'язку глобальної мережі і за яких умов зростання швидкості обміну інформацією по каналах глобальної мережі не приводить до істотного збільшення продуктивності моста/маршрутизатора.

### 5.1 Розрахунок пропускної спроможності мережі

**Дано:**

Число станцій – 20.

Число транзакцій (кадрів) від однієї станції – 1000.

Режим роботи - 8 годин. У час (ЧНН) найбільшого навантаження передається 20% від загальної кількості переданих кадрів.

Розмір кадру 80 байт. (Переводимо в біти  $80 \cdot 8 = 640$ )

**Знайти:**

- 1) швидкість надходження кадрів;
- 2) середню швидкість обслуговування;
- 3) ступінь використання обслуговуючого пристрою (вірогідність відсутності заявок);
- 4) середнє число об'єктів в черзі;
- 5) середній час знаходження заявки в системі;

**Рішення.**

1) У годину через вузол мережі проходить:

- при Гаусовому розподілі  $N = 1000 \cdot 20 \cdot 0,2 = 4000$  кадрів/год;

- при рівномірному розподілі  $N = 1000 \cdot 20 / 8 = 2500$  кадрів/год;

					ЧДТУ 201850.005 ПЗ	Арк.
						35
Змн.	Арк.	№ докум.	Підпис	Дата		

**Швидкість надходження кадрів** знайдемо діленням отриманих чисел на 3600:

- при Гаусовому розподілі  $4000 / 3600 = 1,1111$  кадрів/сек.
- при рівномірному розподілі  $2500 / 3600 = 0,6944$  кадрів/сек.

2) Для розрахунку середньої швидкості обслуговування слід задатися певним значенням швидкості роботи глобальної мережі. Всі обчислення легко повторити для іншого значення швидкості. Прийmemo швидкість обміну інформацією рівної 0,128 Мбіт/с або 131 072 біт/с. Тоді час, необхідний для передачі одного кадру довжиною 80 байт, складе 0,00061 секунди.

Очікуваний час обслуговування рівний 0,00488 сек., тоді середня швидкість обслуговування (величина, зворотня до очікуваного часу обслуговування) складе 204 кадрів за секунду.

З розрахунків виходить, що при таких швидкостях обслуговування і надходження кадрів даний канал справиться з трафіком, що надходить.

3) **Ступінь використання** технічних можливостей обслуговуючого пристрою (Р) в системі можна визначити, поділивши середню швидкість надходження заявок на середню швидкість обслуговування:

- при Гаусовому розподілі  $P = 1,1111 / 204 = 0,005$ , тобто 0,5%;
- при рівномірному розподілі  $P = 0,6944 / 204 = 0,003$ , тобто 0,3%.

Знаючи ступінь використання обслуговуючого пристрою, можна легко визначити вірогідність відсутності заявок (кадрів) в даний момент часу  $P_0$

$$P_0 = 1 - P.$$

- при Гаусовому розподілі  $P_0 = 100\% - 0,5\% = 99,5\%$ .
- при рівномірному розподілі  $P_0 = 100\% - 0,3\% = 99,7\%$ .

З'ясуємо, як формуються черги кадрів, і як впливають пов'язані з чергами затримки на процес передачі кадрів від однієї мережі до іншої.

4) У теорії масового обслуговування середнє число об'єктів (unit) в системі зазвичай позначається L, а середнє число об'єктів в черзі -  $L_q$ . Для

					ЧДТУ 201850.005 ПЗ	Арк.
						36
Змн.	Арк.	№ докум.	Підпис	Дата		



одноканальної системи  $L$  дорівнює середній швидкості надходження заявок, що ділиться на різницю між середньою швидкістю обслуговування і швидкістю надходження заявок:

- при Гаусовому розподілі  $L = 1,1111 / (204 - 1,1111) = 0,0055$ .
- при рівномірному розподілі  $L = 0,6944 / (204 - 0,6944) = 0,0034$ .

Таким чином, в буфері маршрутизатора і лінії зв'язку у будь-який момент знаходиться 2-3% одного кадру. Щоб визначити середнє число об'єктів в черзі ( $L_q$ ), перемножимо ступінь використання обслуговуючого пристрою ( $P$ ) на число об'єктів в системі ( $L$ ):

- при Гаусовому розподілі  $L_q = 0,0055 * 1,1111 = 0,0061$ .
- при рівномірному розподілі  $L_q = 0,0034 * 0,6944 = 0,0024$ .

Теорія масового обслуговування дозволяє розрахувати середній час знаходження об'єкту в системі ( $t_\omega$ ) і середній час очікування в черзі ( $t_{\omega q}$ ).

5) Середній час знаходження в системі є величиною, зворотною різниці між швидкістю обслуговування і швидкістю надходження заявок. Підставивши числа з нашого прикладу, знайдемо, що в даному випадку кожен кадр проводить в системі в середньому:

- при розподілі Гауса  $t_\omega = 1 / (204 - 1,1111) = 0,005$  с.
- при рівномірному розподілі  $t_\omega = 1 / (204 - 0,6944) = 0,00492$  с.

Черги в системі характеризуються ще часом очікування  $t_{\omega q}$ , яке рівне  $t_{\omega q} = t_\omega * P$ . Таким чином, для проектованої мережі:

- при Гаусовому розподілі  $t_{\omega q} = 0,005 * 1,1111 = 0,00555$  с.
- при рівномірному розподілі  $t_{\omega q} = 0,00492 * 0,6944 = 0,003416$  с.

Середньостатистичні значення параметрів мережі в залежності від величини пропускної спроможності наведені у табл.1.

					ЧДТУ 201850.005 ПЗ	Арк.
						37
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця 5.1 – Варіювання пропускної спроможності глобальної мережі:

Швидкість лінії (Мбіт/с)	-	0,1	0,5	1
Час передачі кадру, с	t	0,059	0,011	0,005
Середня швидкість обслуговування	C <sub>o</sub>	16	90	200
Ступінь використання каналу	P	0,07	0,012	0,005
Вірогідність відсутності кадрів в системі	$P_0 = 1 - P$	0,93	98,8	99,5
Середнє число об'єктів (всього)	L	0,07	0,013	0,007
Середнє число об'єктів в чергах	$L_q = L * P$	0,08	0,015	0,008
Повний час очікування	t <sub>ω</sub>	0,067	0,011	0,005
Час очікування в черзі	t <sub>ωq</sub> = t <sub>ω</sub> * P	0,004	1,2*10 <sup>-5</sup>	2,5*10 <sup>-5</sup>

Стосовно нашого варіанту таблиця варіювання пропускної спроможності глобальної мережі ( Таблиця 5.2) виглядає таким чином:



Таблиця 5.2 - Таблиця варіювання пропускної спроможності

Заняття лінії одним абонентом, годин	1	1	1	1	1
Швидкість кодування голосу, біт/с	19800	19800	19800	19800	19800
Трафік від одного абонента в добу, біт	71280000	71280000	71280000	71280000	71280000
Середня довжина кадру, біт	640	640	640	640	640
Число кадрів від одного абонента	111375	111375	111375	111375	111375
Загальне число кадрів	2338875	2338875	2338875	2338875	2338875
Швидкість надходження кадрів	649,6875	649,6875	649,6875	649,6875	649,6875
Швидкість лінії (біт/с)	256000	512000	1024000	2048000	4096000
Час передачі кадру, с	0,0025	0,00125	0,000625	0,0003125	0,00015625
Середня швидкість обслуговування	400	800	1600	3200	6400
Ступінь використання каналу	1,62421875	0,8121093 8	0,40605468 8	0,20302734 4	0,10151367 2
Вірогідність відсутності кадрів в системі $P_0=1-p$	-0,62421875	0,1878906 3	0,59394531 3	0,79697265 6	0,89848632 8
Середнє число об'єктів (всього)	- 1,60200250 3	5,3222453 2	1,68365669 2	1,25474819 3	1,11298299
Середнє число об'єктів в чергах	- 2,60200250 3	4,3222453 2	0,68365669 2	0,25474819 3	0,11298299
$L_q = L * P$	- 0,00400500 6	0,0066528 1	0,00105228 5	0,00039210 9	0,000215
Повний час очікування $t_w$	- 0,00650500 6	0,0054028 1	0,00042728 5	7,96088E- 05	2,18254E- 05
Час очікування в черзі $t_{wq} = t_w * P$	- 0,00650500 6	0,0054028 1	0,00042728 5	7,96088E- 05	2,18254E- 05

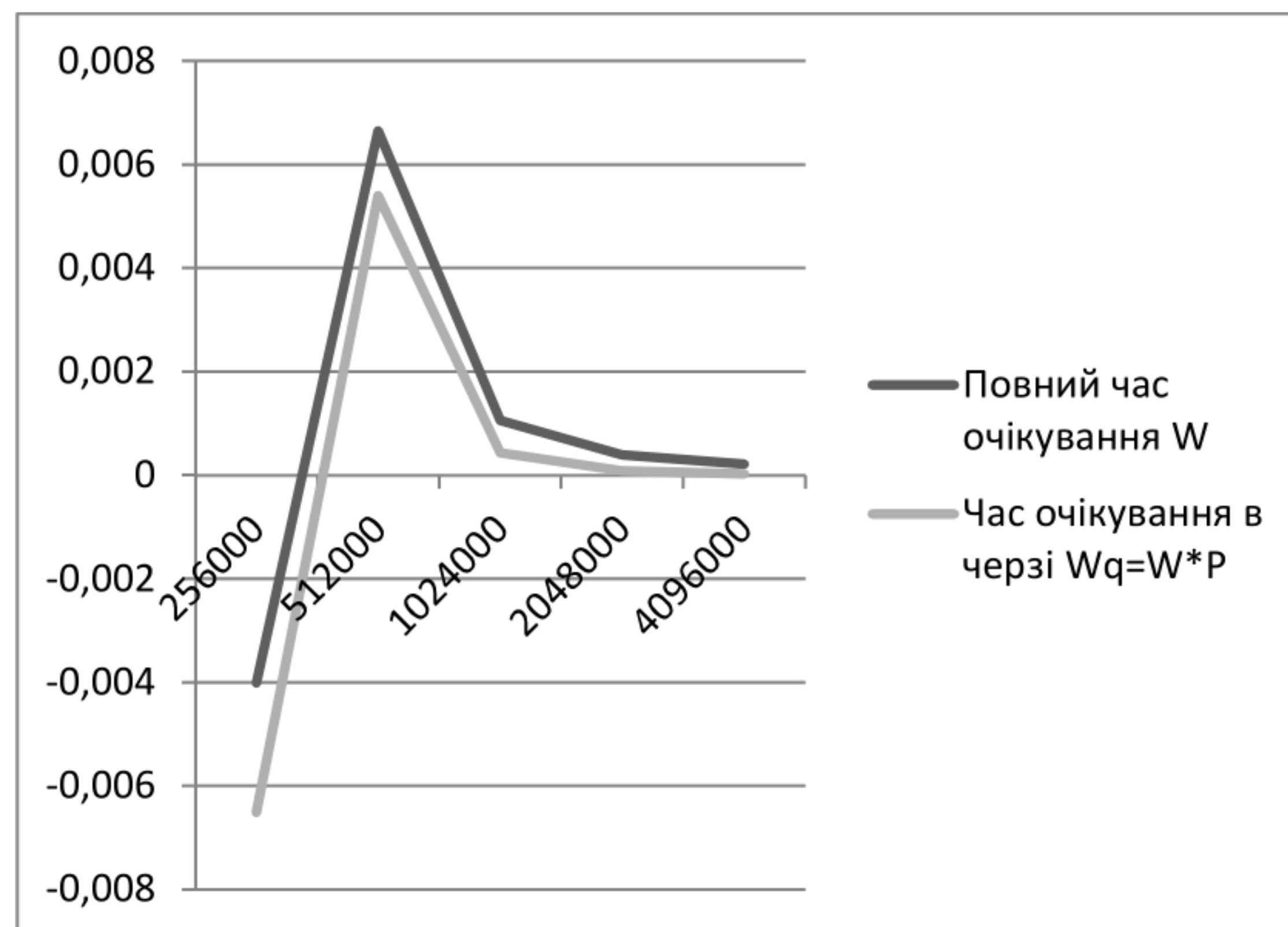


Рисунок 5.1 - Повний час очікування та час очікування в черзі

На рисунку 5.1 наведений повний час очікування  $t_{\omega}$  та час очікування в черзі  $t_{\omega q} = t_{\omega} * P$ .

Як бачимо, що при такому розподілі навантаження на канал його швидкість повинна бути не менше 512 Кбіт/с. На рисунку 5.2 вказані ступінь використання каналу та вірогідність відсутності кадрів у системі.

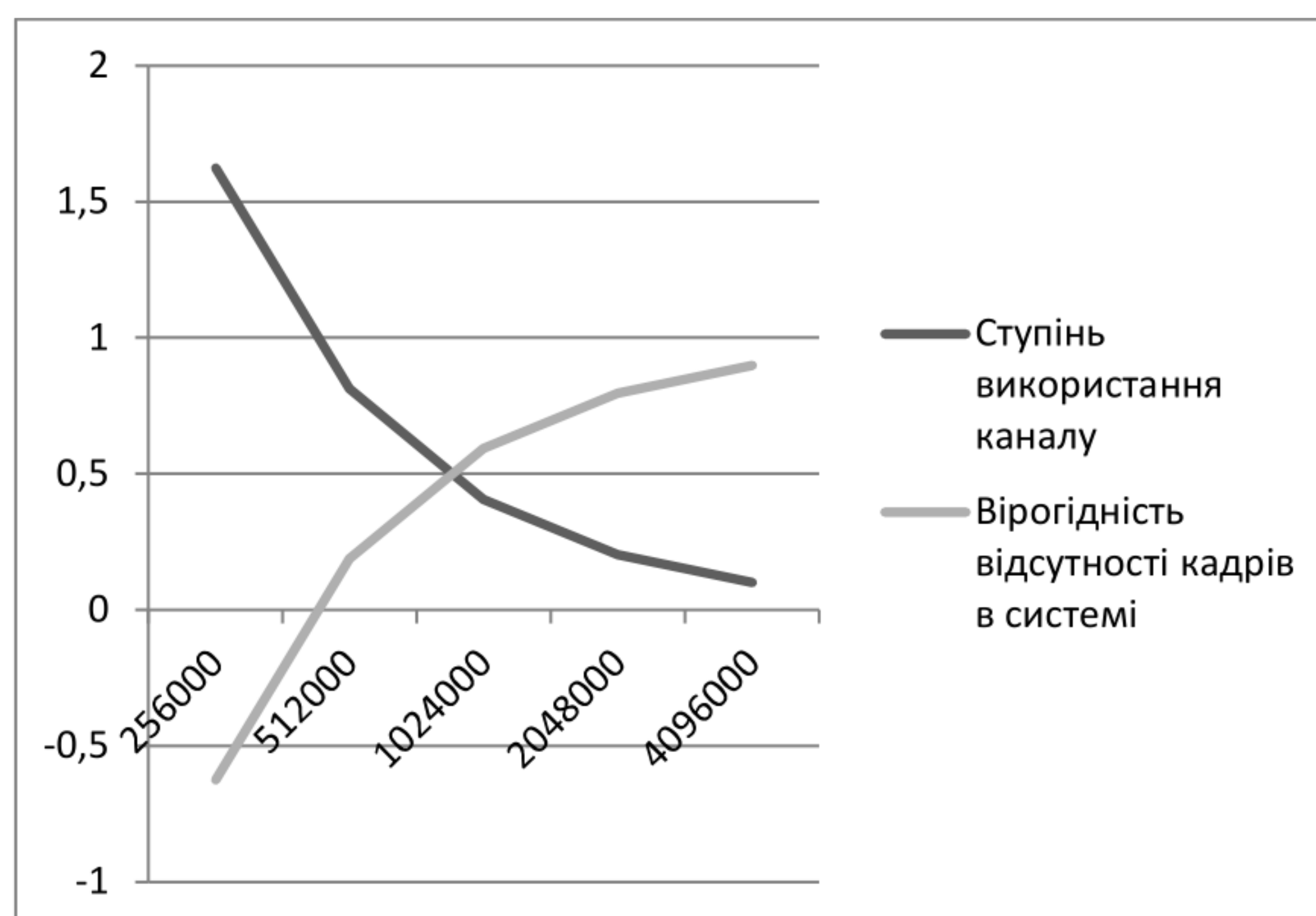


Рисунок 5.2 - Ступінь використання каналу  $P$ , вірогідність відсутності кадрів в черзі  $P_0$



## 5.2 Розрахунок VPN-сервера

У корпоративній мережі інтервали часу між надходженнями заявок незалежні. В цьому випадку заявки утворюють рекурентний потік (потік з обмеженою післядією). Простий потік може розглядатися як окремий випадок рекурентного потоку.

Як приклад рекурентного потоку можна розглядати потік Ерланга. Потоком Ерланга  $k$ -го порядку називається потік, у якого інтервали часу між моментами надходження двох послідовних заявок є сумою до незалежних випадкових величин, розподілених однаково по показовому закону з параметром  $\lambda$ . Потік Ерланга  $k$ -го порядку може бути отриманий з простого потоку викиданням підряд  $(k-1)$  заявок і збереженням кожної  $k$ -ї заявки.

Щільність розподілення інтервалу поміж двома сусідніми заявками в потоці Ерланга  $k$ -го порядку обчислюється за формулою:

$$P(\tau) = \frac{\lambda([\lambda\tau])^{k-1}}{(k-1)!} e^{-\lambda\tau}, (k = 1, 2, \dots);$$

де  $\lambda$  — інтенсивність початкового простого потоку заявок. При  $k=1$  має місце простий потік.

Виходячи із статистичних даних, на сервер для обробки поступає в середньому 500 пакетів за 1 хвилину.

*Знайдемо вірогідність того, що за 1 секунду на сервер не поступить жодного пакету, а також вірогідність надходження не більше трьох пакетів за 5 секунд.*

а) Обчислимо інтенсивність надходження пакетів на сервер (за секунду):

$$\lambda = 500/60 = 8,3 \text{ пакетів/сек.}$$

Обчислимо вірогідність того, що за 1 с. на сервер не поступить жодного пакету по формулі:

$$Pr(k, \tau) = \frac{\lambda([\lambda\tau])^{k-1}}{k!} e^{-\lambda\tau}$$

$$Pr(k, \tau) = 0,000248517$$

					ЧДТУ 201850.005 ПЗ	Арк.
						41
Змн.	Арк.	№ докум.	Підпис	Дата		



### 5.3 Система з кількома серверами

У таблиці 5.3 наведені формули для визначення основних параметрів в разі роботи з системою з безліччю серверів. Ці формули застосовні тільки для випадку використання моделі  $M / M / N$ . Тобто передбачається пуассоновський характер розподілу часів надходження елементів даних і експонентний характер часу обслуговування цих елементів. При цьому формула Пуассона для розподілу часу обслуговування може бути застосована для всіх  $N$  серверів. У всіх виразах використовується функція Ерланга  $C$ , яка, в одних випадках, визначає ймовірність того, що всі сервери зайняті в певний момент часу, а в інших випадках - ймовірність того, що кількість елементів даних, що знаходяться в даний момент часу в системі (очікують в черзі або обслуговуються), буде більше або дорівнює кількості серверів. Для обчислення функції  $C$  застосовна наступна формула:

$$C(N, u) = \frac{1 - K}{1 - \rho K},$$

де  $K$  - коефіцієнт пуассонівського розподілу.

Значення ця функція залежить від кількості серверів ( $N$ ), і їх утилізації ( $\rho$ ). Функцію Ерланга доводиться часто застосовувати при розрахунку черг, що значно ускладнює обчислення. Слід зазначити, що для системи з одним сервером ця функція значно спрощується. А саме:  $C=(1, u)=\rho$ .

Таке спрощення якраз і дозволяє для системи з одним сервером отримати красиві закінчені формули (таблиця 5.3).

					ЧДТУ 201850.005 ПЗ	Арк.
						42
Змн.	Арк.	№ докум.	Підпис	Дата		



Таблиця 5.3. Формули визначення параметрів системи з множиною серверів

$K = \sum_{l=0}^{N-1} \frac{(N \cdot \rho)^l}{l!} \bigg/ \sum_{l=0}^N \frac{(N \cdot \rho)^l}{l!}$	$\sigma_{\omega} = \frac{1}{(1-\rho)} \sqrt{C \cdot \rho \cdot (1 + \rho - C \cdot \rho)}$
$q = C \frac{\rho}{1-\rho} + N \cdot \rho$	$\Pr[T_{\omega} = t] = C \cdot e^{-N(1-\rho)t/T_q}$
$T_q = \frac{C}{N} \frac{T_s}{1-\rho} + T_s$	$T_d = \frac{T_s}{N(1-\rho)}$
$T_{\omega} = \frac{C}{N} \frac{T_s}{1-\rho}$	$\omega = C \frac{\rho}{1-\rho}$
$\sigma_{T_q} = \frac{T_s}{N(1-\rho)} \sqrt{C(2-C) + N^2(1-\rho)^2}$	$m_{T_{\omega}} = \frac{T_s}{N(1-\rho)} \cdot \ln \frac{100 \cdot C}{100-r}$

Головне вікно програми «Розрахунок параметрів мереж із N серверами» вказане на рис. 5.3.

На рис.5.4 зображено «Вікно з полями для вводу даних»,

а на рис. 5.5 – «Вікно з результати обчислень».

## Результати обчислень

Вхідні дані:

Робочих станцій \_\_\_\_\_ 20  
 Середній час обслуговування елементів, що надходять системою \_\_\_\_\_ 0,25  
 Відхилення часу, стандартне \_\_\_\_\_ 0,1  
 Швидкість надходження запитів від кожної робочої станції \_\_\_\_\_ 21  
 Максимально прийнятний час відповіді \_\_\_\_\_ 1,5 в 97% випадків  
 Збільшення утилізації серверу \_\_\_\_\_ 15%

Результат обробки даних:

Середня швидкість надходження елементів даних у систему(число елементів за секунду) \_\_\_\_\_ 7  
 Утилізація одного сервера \_\_\_\_\_ 0,875  
 Утилізація системи (інтенсивність трафіка) \_\_\_\_\_ 1,75  
 Функція Ерланга \_\_\_\_\_ 0,816666666666667  
 Коефіцієнт Пуасона \_\_\_\_\_ 0,642335766423358  
 Середній час відповіді \_\_\_\_\_ 0,25  
 Середній час відповіді, при збільшенні утилізації серверу \_\_\_\_\_ 0,2875  
 Середній розмір черги \_\_\_\_\_ 5,71666666666667  
 Процент завантаження до стану насиченості серверу \_\_\_\_\_ 330%  
 Середня кількість елементів даних у системі \_\_\_\_\_ 7,46666666666667  
 Середній час, який елементи даних проводять у системі \_\_\_\_\_ 1,06666666666667  
 Середній час, який елементи даних очікують на обслуговування \_\_\_\_\_ 0,81666666666667  
 Середній час, який елементи даних очікують на обслуговування, при збільшенні утилізації серверу \_\_\_\_\_ -22,7760080789025  
 Середній час обслуговування для елементів даних, що знаходяться в черзі \_\_\_\_\_ 1  
 Стандартне відхилення  $T_q$  \_\_\_\_\_ 1,01434160364686  
 Стандартне відхилення середньої кількості елементів даних в системі \_\_\_\_\_ 0,746666666666667

					ЧДТУ 201850.005 ПЗ	Арк.
						44
Змн.	Арк.	№ докум.	Підпис	Дата		



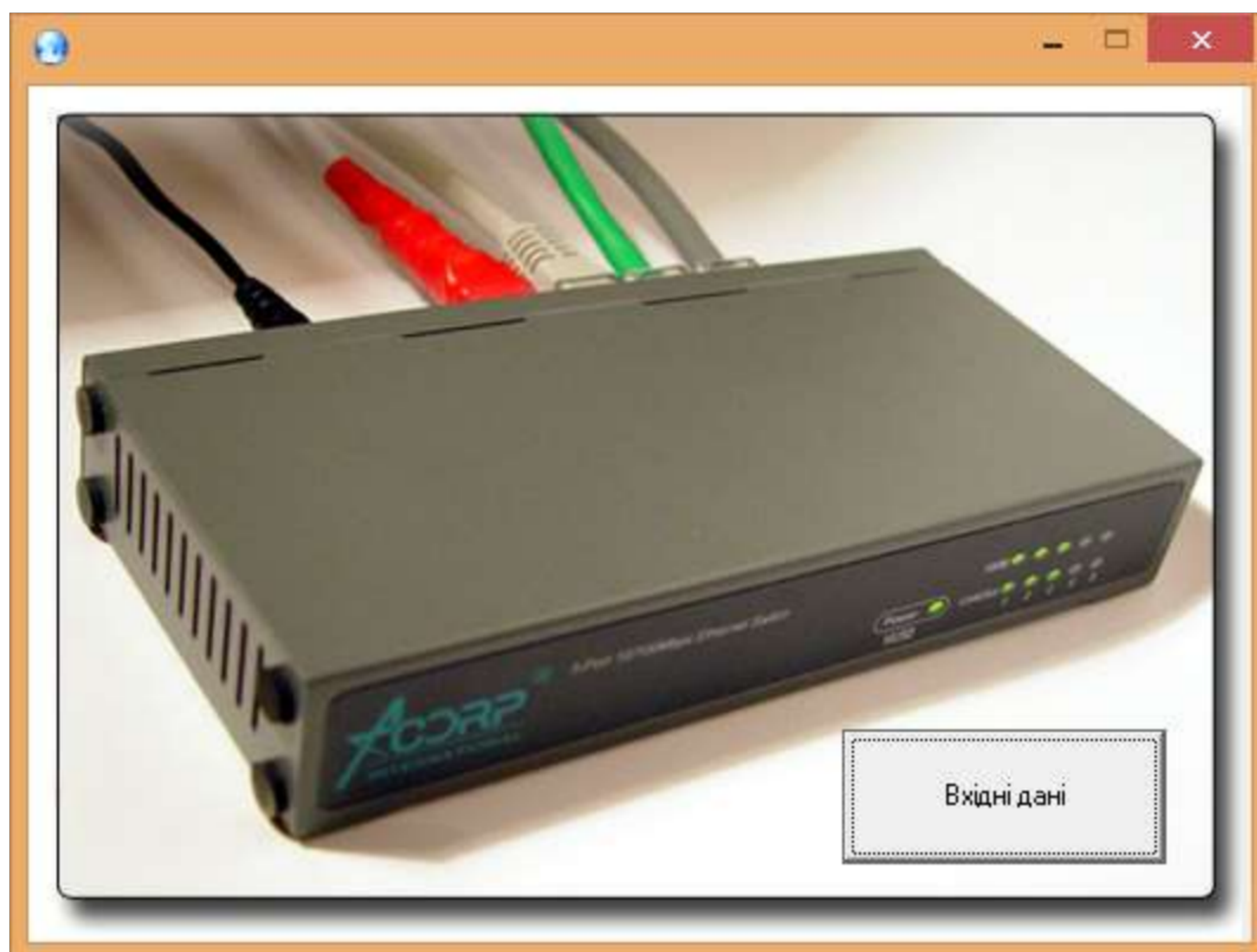


Рисунок 5.3 - Головне вікно програми «Розрахунок параметрів мереж із N серверами»

Кількість робочих станцій, A...	20
Середній час обслуговування поступаючих елементів системою, B (сек)...	0,25
Стандартне відхилення часу B, C (сек)...	0,10
Швидкість поступання запитів від кожної робочої станції, D (1/сек)...	21
Максимальний допустимий час для відповіді, E (сек)...	1,5
Число випадків, P (%)...	97
Збільшення утилізації серверу, Util (%)...	15
Кількість серверів, N...	2

OK Відміна

Рисунок 5.4 - Вікно з полями для вводу даних



×

Входные данные:

Рабочих станций \_\_\_\_\_ 20

Среднее время обслуживания поступивших элементов системой \_\_\_\_\_ 0,25

Стандартное отклонение этого времени \_\_\_\_\_ 0,1

Скорость поступления запросов от каждой рабочей станции \_\_\_\_\_ 21

Максимально приемлемое время ответа \_\_\_\_\_ 1,5 в 97% случаев

Увеличение утилизации сервера \_\_\_\_\_ 15%

Результат обработки данных:

Средняя скорость поступления элементов данных в систему(число элементов в секунду) \_\_\_\_\_ 7

Утилизация одного сервера \_\_\_\_\_ 0,875

Утилизация системы (интенсивность трафика) \_\_\_\_\_ 1,75

Функция Эрланга \_\_\_\_\_ 0,816666666666667

Коэффициент Пуассона \_\_\_\_\_ 0,642335766423358

Среднее время ответа \_\_\_\_\_ 0,25

Среднее время ответа, при увеличении утилизации сервера \_\_\_\_\_ 0,2875

Средний размер очереди \_\_\_\_\_ 5,716666666666667

Процент загрузки до достижения насыщенности сервера \_\_\_\_\_ 330%

Среднее количество элементов данных в системе \_\_\_\_\_ 7,466666666666667

Среднее время, которое элементы данных проводят в системе \_\_\_\_\_ 1,066666666666667

Среднее время, которое элементы данных ожидают обслуживания \_\_\_\_\_ 0,816666666666667

Среднее время, которое элементы данных ожидают обслуживания, при увеличении утилизации сервера \_\_\_\_\_ -22,7760080789025

Среднее время обслуживания для элементов данных находившихся в очереди \_\_\_\_\_ 1

Стандартное отклонение  $T_q$  \_\_\_\_\_ 1,01434160364686

Стандартное отклонение среднего количества элементов данных в системе \_\_\_\_\_ 0,746666666666667

Зберегти як...

Рисунок 5.5 - Вікно з результатами обчислень

### Висновки до розділу 5

В розділі проведено розрахунки основних параметрів проектованої міської ділянки мережі. Розраховано пропускну здатність мережі, навантаженість серверів та проведено розрахунок VPN-серверу.

Проведені розрахунки параметрів банківської мережі свідчать про коректність вибору апаратного комунікаційного обладнання, конфігурації серверів та робочих станцій, програмного мережевого забезпечення для моделі інформаційного обміну в мережах з чергами.

					ЧДТУ 201850.005 ПЗ	Арк.
						46
Змн.	Арк.	№ докум.	Підпис	Дата		



## 6. ОРГАНІЗАЦІЯ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ОБМІНУ В МЕРЕЖІ

**Завдання №1.** Шифр Цезаря. Використовуючи шифр Цезаря, зашифрувати власні: Прізвище, Ім'я, по Батькові.

**Завдання №2.** Алгоритм шифрування ДСТ 28147-89. В режимі заміни провести перший цикл алгоритму шифрування за вказаним ДСТ. Задля отримання 64 біт початкового тексту використати 8 літер з власних ПІБ. З метою отримання 256-бітного ключа вжити текст, що складається з 32 літер. Саме так, перший підключ містить перші 4 літери.

**Завдання №3.** Алгоритм шифрування RSA. Згенерувати відкритий і закритий ключі в алгоритмі RSA, для чого з першої сотні вибрати прості числа  $p$  і  $q$ . Зашифрувати повідомлення: П І Б.

**Завдання №4.** Функція гешування. Відшукати геш–образ власного прізвища, використовуючи геш–функцію  $H_i = (H_{i-1} + M_i)^2 \bmod n$ , де  $n = pq$ ;  $p, q$  узяти із завдання №3.

**Завдання №5.** Електронний цифровий підпис. Використовуючи геш–образ прізвища, обчислити електронний цифровий підпис по схемі RSA.

### Виконання завдання:

**Завдання №1.** Використовуючи шифр Цезаря, зашифрувати власні: Прізвище, Ім'я, по Батькові..

Початковий текст: «ЯНКО НІКІТА КРИСТОВОВИЧ».

Використовуємо алфавіт, що містить 33 букви і пробіл, після літери Я:

АБВГГДЕЄЖЗИІЙКЛМНОПРСТУФХЦЧШЩЬЮЯпробіл

Ключем в шифрі Цезаря є число 3. Кожна літера в початковому тексті зрушується за абеткою на 3 позиції. Таким чином, отримуємо:

Початковий текст                      ЯНКО НІКІТА КРИСТОВОВИЧ

					ЧДТУ 201850.005 ПЗ	Арк.
						47
Змн.	Арк.	№ докум.	Підпис	Дата		

Зашифрований текст      АПМРБПКМКФВБЬТЛУРДРДЛЩ

**Завдання №2. Алгоритм шифрування ДСТ 28147-89.** В режимі заміни провести перший цикл алгоритму шифрування за вказаним ДСТ. Задля отримання 64 біт початкового тексту використати 8 літер з власних ПІБ. З метою отримання 256-бітного ключа вжити текст, що складається з 32 літер. Саме так, перший підключ містить перші 4 літери.

Початкові дані для шифрування: ЯНКО\_НІК

Для ключа візьмемо послідовність, що складається з 32 букв:

*Павло повернувся додому о сьомій*

Для першого підключа X використовуємо перші 4 букви ключа: ПАВЛ.

Перекладаємо початковий текст і перший під ключ в двійкову послідовність:

початковий текст

Я	11000001
Н	11001110
К	11000001
О	11010011
-	00010000
Н	11001110
І	11010001
К	11000001

перший під ключ X0

П	11001111
А	11000000
В	11000010
Л	11001011

Таким чином, перші 64 біта визначають вхідну послідовність

L0:      11010001    11001000    11010000    11010111

					ЧДТУ 201850.005 ПЗ	Арк.
						48
Змн.	Арк.	№ докум.	Підпис	Дата		



R0: 11000101 11001101 11001010 11001110

наступні 32 біта визначають перший підключ

X0: 11001111 11000000 11000010 11001011

I. Знаходимо функцію перетворення  $f(R0, X0)$  ( ДОДАТОК1)

1). Обчислюємо суму R0 і X0 за mod  $2^{32}$

R0: 1100 0101 1100 1101 1100 1010 1100 1110

X0: 1100 1111 1100 0000 1100 0010 1100 1011

---

1001 0101 1000 1110 1000 1101 1001 1001

2). Проведемо перетворення в блоці підстановки

Результат підсумовування  $R0+X0$  за mod  $2^{32}$

1001 0101 1000 1110 1000 1101 1001 1001

перетворимо в блоці підстановки. Для кожного 4-бітового модуля знайдемо його адресу в Додатку (таблиця підстановки). Таким чином, п'ятий блок (1011) замінюється заповненням одинадцятого рядка і п'ятого стовпця в таблиці підстановки (1110).

номери блоків

8 7 6 5 4 3 2 1

1001 0101 1000 1110 1000 1101 1001 1001

відповідні номери рядків в таблиці підстановки

9 5 8 14 8 13 9 9

заповнення

2 15 3 11 14 0 3 11

результат

0010 1111 0011 1011 1110 0000 0011 1011

3). Циклічне зрушення результату п.2 на 11 біт вліво

0010 0100 1111 0101 1001 1101 1111 0101

Отже, знайдено значення функції  $f(R0, X0)$ :

0010 0100 1111 0101 1001 1101 1111 0101

II. Обчислюємо  $R1 = f(R0, X0) \oplus L0$ .

Результат перетворення функції  $f(R0, X0)$  складаємо з L0 за mod2:

L0: 1101 0001 1100 1000 1101 0000 1101 0111

					ЧДТУ 201850.005 ПЗ		Арк.
							49
Змн.	Арк.	№ докум.	Підпис	Дата			

f(R0,X0):	0010 0100	1111 0101	1001 1101	1111 0101
R1:	1111 0101	0011 1101	0100 1101	0010 0010

**Завдання №3. Алгоритм шифрування RSA.** Згенерувати відкритий і закритий ключі в алгоритмі RSA, для чого з першої сотні вибрати прості числа  $p$  і  $q$ . Зашифрувати повідомлення: П І Б.

### 3.1. Генерація ключів

Виберемо двоє простих чисел  $p = 17$  і  $q = 41$ .

Тоді модуль

$$n = pq = 17 \cdot 41 = 697$$

і функція Ейлера

$$\varphi(n) = (p-1)(q-1) = 16 \cdot 40 = 640$$

Закритий ключ  $d$  візьмемо з умов  $d < \varphi(n)$  і  $d$  взаємно просто з  $\varphi(n)$ , тобто  $d$  и  $\varphi(n)$  не мають загальних дільників.

Хай  $d = 9$ .

Відкритий ключ  $e$  вибираємо з умов  $e < \varphi(n)$  и  $de \equiv 1 \pmod{\varphi(n)}$ :  $e < 640$

$$9e \equiv 1 \pmod{640}.$$

Остання умова означає, що число  $9e-1$  повинно ділитися на 640 без залишку.

Отже, для визначення  $e$  потрібно підібрати таке число, що

$$9e-1 = 640k.$$

При  $k=17$  отримуємо  $9e=10880+1$  або  $e=1209$ .

У нашому прикладі

$(1209, 697)$  – відкритий ключ,  $(9, 697)$  – секретний ключ.

### 3.2. Шифрування

Представимо шифроване повідомлення «ЯНК» як послідовність цілих чисел. Хай літера «Я» відповідає числу 2, літера «Н» - числу 21 і літера «К» - числу 16.

Зашифруємо повідомлення, використовуючи відкритий ключ  $(1209, 697)$ :

$$C_1 = (2^{1209}) \bmod 697 = 175;$$

$$C_2 = (21^{1209}) \bmod 697 = 270;$$

$$C_3 = (16^{1209}) \bmod 697 = 620.$$

					ЧДТУ 201850.005 ПЗ	Арк.
						50
Змн.	Арк.	№ докум.	Підпис	Дата		



Таким чином, початковому повідомленню (2, 21, 16) відповідає криптограма (175, 270, 620).

### III. Розшифрування

Розшифруємо повідомлення (175, 270, 620), користуючись секретним ключем (9,697):

$$M_1 = (175^9) \bmod 697 = 2$$

$$M_2 = (270^9) \bmod 697 = 21$$

$$M_3 = (620^9) \bmod 697 = 16$$

В результаті розшифрування було отримано початкове повідомлення (2, 21, 16), тобто "ЯНК".

**Завдання №4. Функція гешування.** Відшукати геш-образ власного прізвища, використовуючи геш-функцію  $H_i = (H_{i-1} + M_i)^2 \bmod n$ , де  $n = pq$ ;  $p, q$  узяти із завдання №3.

Гешоване повідомлення «ЯНКО\_НІК». Візьмемо двоє простих числа  $p=17, q=41$ . Визначимо  $n=pq=17*41=697$ . Вектор ініціалізації  $H_0$  виберемо рівним 11 (вибираємо випадковим чином). Слово «ЯНКО\_НІК» можна представити послідовністю чисел (2, 15, 2, 20, 22, 32, 18, 6) по номерах букв в абетці. Таким чином

$n=697, H_0=11, M_1=2, M_2=15, M_3=2, M_4=20, M_5=22, M_6=32, M_7=18, M_8=6$ .

Використовуючи формулу

$$H_i = (H_{i-1} + M_i)^2 \bmod n,$$

отримаємо геш-образ повідомлення «ЯНКО\_НІК»:

$$H_1 = (H_0 + M_1)^2 \bmod n = (11 + 2)^2 \bmod 697 = 841 \bmod 697 = 144$$

$$H_2 = (H_1 + M_2)^2 \bmod n = (144 + 15)^2 \bmod 697 = 23409 \bmod 697 = 408$$

$$H_3 = (H_2 + M_3)^2 \bmod n = (408 + 2)^2 \bmod 697 = 180625 \bmod 697 = 102$$

					ЧДТУ 201850.005 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		51

$$\begin{aligned}
H_4 &= (H_3 + M_4)^2 \bmod n = (102 + 20)^2 \bmod 697 = 576 \bmod 697 = 678 \\
H_5 &= (H_4 + M_5)^2 \bmod n = (678 + 22)^2 \bmod 697 = 467856 \bmod 697 = 169 \\
H_6 &= (H_5 + M_6)^2 \bmod n = (169 + 32)^2 \bmod 697 = 33489 \bmod 697 = 33 \\
H_7 &= (H_6 + M_7)^2 \bmod n = (33 + 18)^2 \bmod 697 = 1936 \bmod 697 = 542 \\
H_8 &= (H_7 + M_8)^2 \bmod n = (542 + 6)^2 \bmod 697 = 310249 \bmod 697 = 84
\end{aligned}$$

У результаті отримуємо геш-образ повідомлення «ЯНКО\_НІК», рівне 84.

**Завдання №5. Електронний цифровий підпис.** Використовуючи геш-образ прізвища, обчислити електронний цифровий підпис по схемі RSA.

Нехай геш-образ Прізвища дорівнює 84, а закритий ключ алгоритму RSA рівний (9, 697). Тоді електронний цифровий підпис повідомлення, що складається з Прізвища, обчислюється за правилом:

$$s = 84^9 \bmod 697 = 594.$$

Для перевірки ЕЦП, використовуючи відкритий ключ (1209, 697), знайдемо

$$H = 594^{1209} \bmod 697 = 84.$$

Оскільки геш-кодування-образ повідомлення співпадає із знайденим значенням H, то підпис визнається справжнім.

## Висновки до розділу 6

Під час виконання даного розділу роботи організовано безпеку інформаційного обміну в ділянці корпоративній мережі. Розглянуто сім основних класів рівнів безпеки. Для даної мережі використовується рівень С2 (рівень доступу).

Досліджено три типи шифрування інформації: шифр Цезаря, алгоритм шифрування ГОСТ 28147-89 та RSA-алгоритм.

					ЧДТУ 201850.005 ПЗ	Арк.
						52
Змн.	Арк.	№ докум.	Підпис	Дата		



## ВИСНОВКИ

За час виконання кваліфікаційної випускної роботи розглянуті питання організації міської ділянки корпоративної банківської мережі, в даному випадку, мережі «А-банку».

Розглянуто кілька аналогів технологій корпоративних мереж. Проведено аналіз топології та технології побудови мережі. Виявлено переваги та недоліки технологій для використання їх в даному проекті. Обрано технологію ADSL, як найоптимальнішу для даної мережі.

Проведено розрахунки параметрів проектованої мережі. Розраховано пропускну здатність, навантаженість серверів та обчислено VPN-сервер. Проведені розрахунки параметрів банківської мережі свідчать про коректність вибору апаратного комунікаційного обладнання, конфігурації серверів та робочих станцій, програмного мережевого забезпечення для моделі інформаційного обміну в мережах з чергами.

Також виконано синтез мережі, проведений вибір комунікаційного устаткування, яке дозволило використати максимально всі можливості обраної технології. Запроваджено основні заходи для захисту корпоративної мережі від несанкціонованого доступу та спотворення даних.

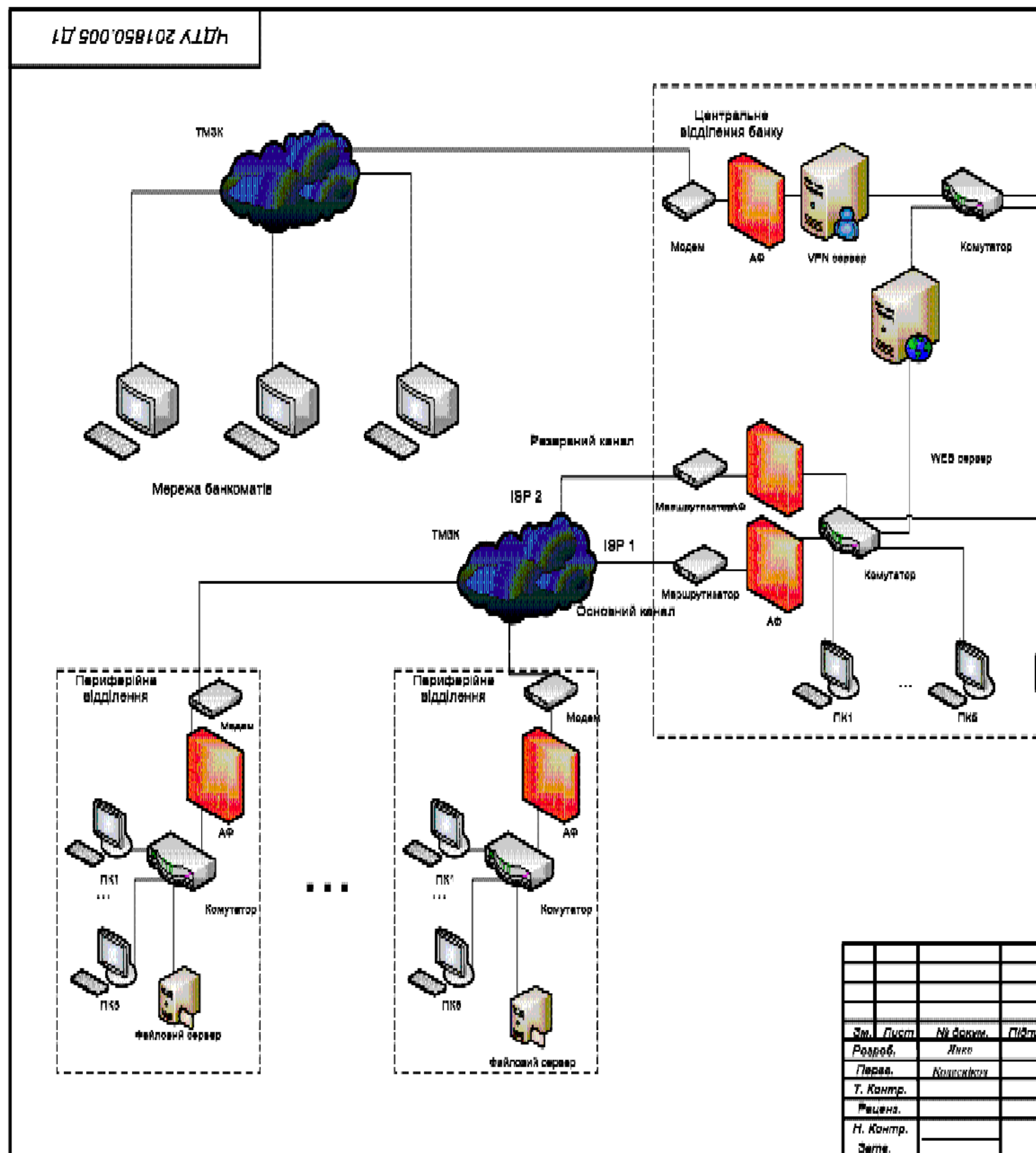
Отже, мета роботи досягнута, розрахунки підтвердили успішне виконання роботи.

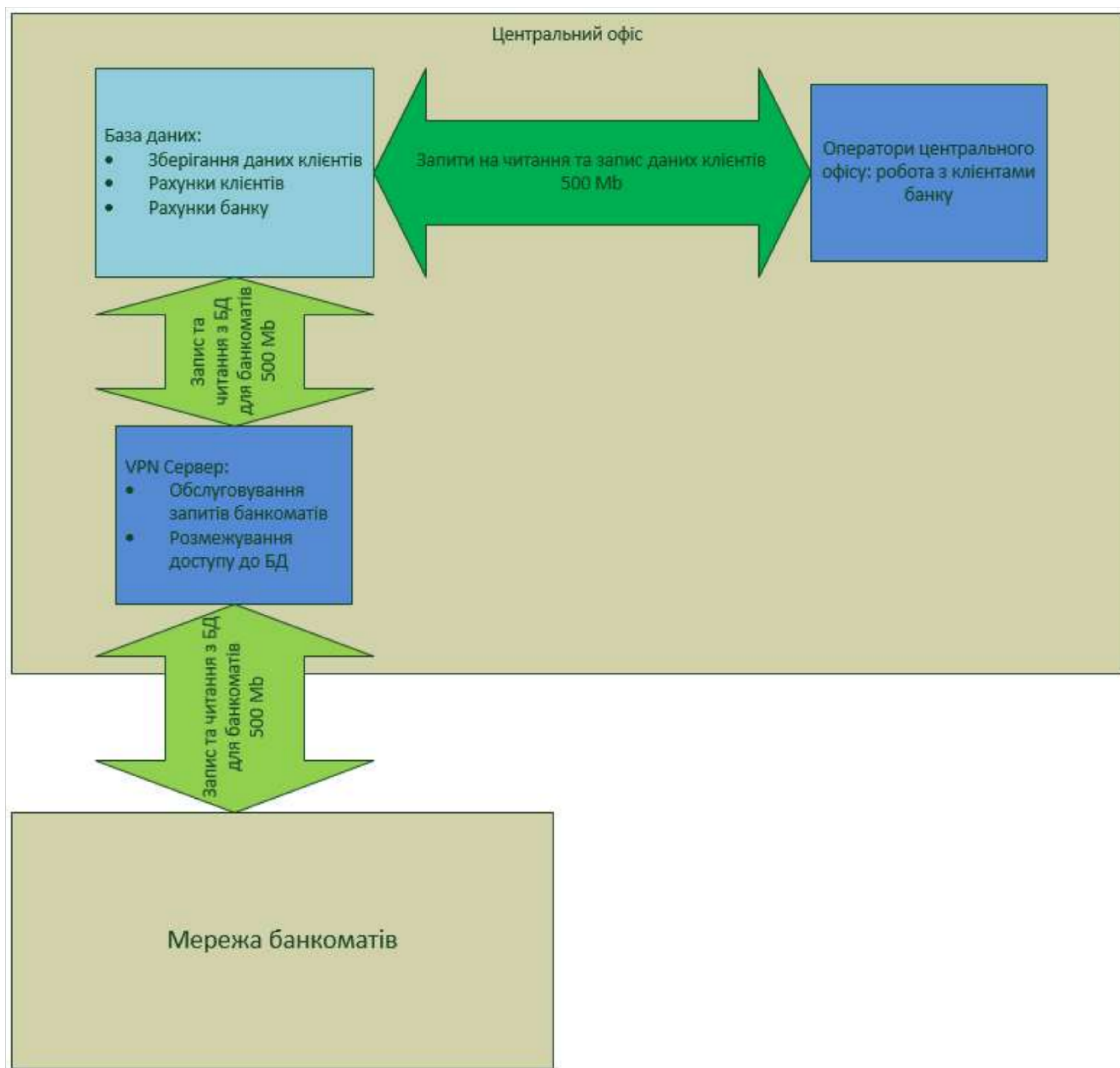
Всі вимоги ТЗ виконані у повному обсязі.

					ЧДТУ 201850.005 ПЗ	Арк.
						53
Змн.	Арк.	№ докум.	Підпис	Дата		

Формат	Зона	Поз.	Позначення	Найменування	Кіл.	Примітка	
				Документація			
A4			ЧДТУ 201850.005 ПЗ	Пояснювальна записка			
A4			ЧДТУ 201850.005 Д1	Топологія			
A4			ЧДТУ 201850.005 Д2	Схема інформаційних потоків			
A4			ЧДТУ 201850.005 Д3	Таблиця з'єднань			
A3			ЧДТУ 201850.005 Е4	Схема електрична з'єднань			
A4			ЧДТУ 201850.005 ПЕ4	Перелік елементів			
				Покупні вироби			
		1		Робоча станція Acer Aspire Z1-623	5		
		2		Модем TP-LINK TD-W8968	1		
		3		Комутатор 3COM 3C16792B-ME	2		
		4		Брандмауер D-Link DFL-260E	3		
		5		Сервер HPE ProLiant ML10 Gen9	1		
		6		Сервер Dell PowerEdge T20	2		
				Банкомат CSC/450	4		
				Матеріали			
		7		Кручена пара UTP Cat.5e		L= 124 m	
		8		Конектор RJ-45	44		
		9		Розетка RJ-45	10		
		10		Конектор RJ-11	3		
		11		Розетка RJ-11	3		
		12		Патч-корд UTP Cat.5e	5	L=2 m	
		13		Патч-корд UTP Cat.5e	4	L=4m	
		14		Шнур комутаційний RJ11-RJ11	5	L=3 m	
				Комплекти			
		15		OC Windows 10 Enterprise	5	ліцензія	
		16		MS Windows Server 2019	3	ліцензія	
				ЧДТУ 201850.005			
Зм.	Лист	№ докум.	Підпис				Дата
Розроб.	Янко Н. К..						
Перев.	Колесніков К. В.						
Реценз.							
Н.контр.	Колесніков К. В.						
Затв.	Прокопенко Т.О.						
				Міська ділянка корпоративної мережі «А-банку»	Лім.	Лист	Листів
					у		1
					ФІТІС, кафедра ІТП, група WebC-1811		







Після проведення експериментів та розрахунків, встановлено що за добу обсяг обміну інформацією складає не більше 1 Гб.

					ЧДТУ 201850.005 Д2		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.	Янко Н. К.				Міська ділянка корпоративної мережі «А-банку». Схема інформаційних потоків	Літ.	Лист
Керівник	Колесніков К. В.					у	1
Реценз.						ФІТІС, кафедра ІТП, група WEBC-1811	
Н. Контр.	Колесніков К. В.						
Затверд.	Прокопенко Т.						





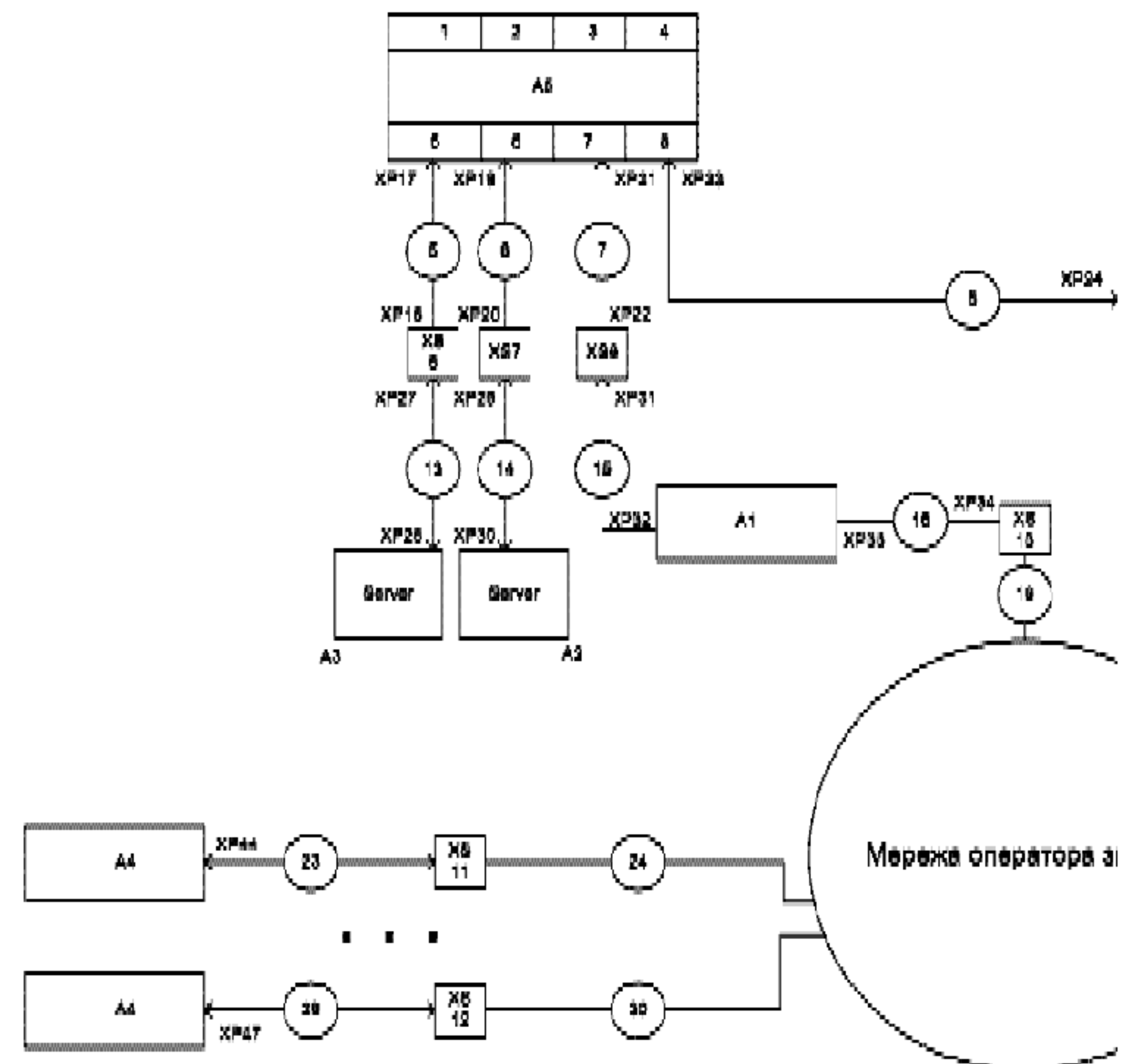




## Таблиця з'єднань

Позначка	Позначення	Дані кабелю	Кіл.	Примітки
<i>Шнури</i>				
1	Патч-корд Cat.5e	Кручена пара UTP Cat.5e	5	L=2m
2	Патч-корд Cat.5e	Кручена пара UTP Cat.5e	4	L=4m
3	Комутаційний шнур RJ11-RJ11	Телефонна лінія ТРП 2x0,5	5	L=3m
<i>Кабелі</i>				
4	UTP Cat5e	Кручена пара UTP Cat.5e	3	L=15m
5	UTP Cat5e	Кручена пара UTP Cat.5e	13	L=6m

					ЧДТУ 201850.005 ДЗ			
Зм.	Лист	№ докум.	Підпис	Дата	Міська ділянка корпоративної мережі «А-банку».	Лім.	Лист	Листів
Розроб.	Янко Н. К.					у		1
Перевір.	Колесніков К.В.							
Реценз.								
Н. Контр.	Колесніков К.В							
Затверд.	Прокопенко Т.							
					Таблиця з'єднань	ФІТІС, кафедра ІТП, Група WEBC-1811		



Зм.	Лист	№ до
Розроб.		Лн.
Перед.		Колес
Решенз.		
Н. Контр.		Колес
Затв.		Прокон



[illegible]

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Олифер В. Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 6-е изд. - СПб.: Питер, 2020. - 1010 с.: ил.;
2. Колесніков, К. В. Основи мережевих технологій: [навчальний посібник] / К. В. Колесніков, В. Ю. Шадхін; М-во освіти і науки України, Черкаський державний технологічний ун-т. – Черкаси: ЧДТУ, 2011. –343 с.
3. Бірюков М.Л., Стеклов В.К., Костік Б.Я. Транспортні мережі телекомунікацій: Системи мультимплексування: Підручник для студентів вищ. техн. закладів; за ред. В.К. Стеклова. – К.: Техніка, 2005. – 312 с.
4. Буров, Є. Комп'ютерні мережі / Є. Буров ; Пасічник В., ред. – 2-ге оновл. і доп. вид.: Львів : Бак, 2007.
5. Вишнеvский В.В. Теоретические основы проектирования компьютерных сетей . – М.: Техносфера, 2003. –512 с.
6. Молдовян В. Безопасность глобальных сетевых технологий – 2-е изд. – СПб.: БХВ-Петербург, 2003. – 368 с.: ил.
7. Сергеев А.П. Офисные локальные сети: Издательский дом «Вильямс», 2003. – 320 с.
8. Сучасні комп'ютерні технології /за ред. Швиденко М.З., Львів.: ННЦ “Інститут аграрної економіки”. – 2007. – 705 с.
9. Танненбаум Э., Уоррен Д. Компьютерные сети. 5-е изд., – СПб.: Питер, 2012, – 992 с..
10. Теоретичні основи завадостійкого кодування Частина 2: Підручник/ П. Ф. Олексенко, В. В. Коваль, Г. М. Розорінов, Г. О. Сукач. - К.: Наукова думка. - 2011. - 284 с.
11. Швиденко М.З., Матус Ю.В.. Комп'ютерні мережні технології. Навч.-метод. посібник. – Київ. – ТОВ “Авета”, - 2008.

					ЧДТУ 201850.005 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		



12. Моделі погроз цілісності інформації в мережах К. В. Колесніков  
Шнуренко Ю.Г., Андрієнко В.В. // Матеріали V-ої Міжнародної науково  
- практичної конференції "Обчислювальний інтелект-2019" Computational  
Intelligence (Results, Problems and Perspectives): Proceedings of the  
International Conference, April 15-20, 2019, Uzhorod, Ukraine;  
Міжнародний науковий симпозіум «ІНТЕЛЕКТУАЛЬНІ РІШЕННЯ»  
Ужгород , с.91-92
- 13.Офіційний сайт «А - банку» [Електронний ресурс] – Режим доступу:  
<https://a-bank.com.ua/>; дата звернення 15.04.2020
- 14.Інформаційне дослідження корпоративної мережі «Черкаського  
облавтодору» [Електронний ресурс] – Режим доступу:  
[http://studopedia.su/13\\_29379\\_InformatsIyne-doslIdzhennya-korporativnoyi-merezhI-cherkaskogo-oblavtodoru.html](http://studopedia.su/13_29379_InformatsIyne-doslIdzhennya-korporativnoyi-merezhI-cherkaskogo-oblavtodoru.html);
15. Корпоративна мережа ВАТ «Ощадбанк» [Електронний ресурс] – Режим  
доступу: [http://studopedia.su/13\\_29384\\_sintez-merezhI.html](http://studopedia.su/13_29384_sintez-merezhI.html);
16. Корпоративна мережа Черкаської облдержадміністрації [Електронний  
ресурс] – Режим доступу: [http://studopedia.su/13\\_29381\\_korporativna-merezha-cherkaskoyi-oblderzhadmInIstratsIyi.html](http://studopedia.su/13_29381_korporativna-merezha-cherkaskoyi-oblderzhadmInIstratsIyi.html);
17. Discom Network Technologies. Коммутатор 3C16792B-ME 3Com  
[Електронний ресурс] – Режим доступу:  
<http://hypercomp.ru/catalog/3com/office-connect/100/3c16792b-me/>;
18. Інтернет-магазин Rozetka. Модем TP-LINK TD-W8968 [Електронний  
ресурс] – Режим доступу:  
[http://rozetka.com.ua/ua/tp\\_link\\_td\\_w8968/p358870/](http://rozetka.com.ua/ua/tp_link_td_w8968/p358870/);
19. Інтернет-магазин Rozetka. Сервер HPE ProLiant ML10 Gen9  
[Електронний ресурс] – Режим доступу:  
[http://rozetka.com.ua/ua/hp\\_838124\\_425/p14206574/](http://rozetka.com.ua/ua/hp_838124_425/p14206574/);
20. Інтернет-магазин Rozetka. Сервер Dell PowerEdge T20 [Електронний  
ресурс] – Режим доступу:

					ЧДТУ 201850.005 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		

[http://rozetka.com.ua/ua/dell\\_t20\\_e3\\_sata/p5023661/;](http://rozetka.com.ua/ua/dell_t20_e3_sata/p5023661/)

21. Інтернет-магазин Rozetka. Робоча станція Acer Aspire Z1-623 [Електронний ресурс] – Режим доступу:

[https://hard.rozetka.com.ua/ua/acer\\_dq\\_b33me\\_002/p7391219/;](https://hard.rozetka.com.ua/ua/acer_dq_b33me_002/p7391219/)

22. Інтернет-магазин АСТІВКА.COM. Міжмережевий екран D-Link DFL-260E [Електронний ресурс] – Режим доступу:

<http://aktivka.ua/mezhsetevoj-jekran-d-link-dfl-260e.html;>

23. Зеркалов Д. В. Безпека працівника банку. Монографія. – К.: «Основа». 2014. – 765 с.

24. Методичні вказівки до виконання кваліфікаційної роботи для здобувачів освітнього ступеня "бакалавр» для студентів зі спеціальності 126 "Інформаційні системи та технології" (освітня програма «Web- технології, Web-дизайн»): / Упорядники: К. В. Колесніков, Т.О. Прокопенко – Черкаси: ЧДТУ, 2019 – 31 с.;

25. Конструктивно-технологічна побудова компонентів спеціалізованих комп'ютерних та роботехнічних систем : Колесніков К. В., Лукашенко В.М, Мусієнко М.П., Рудаков К.С.: М-во освіти і науки України, Черкас. Держ. Технол. Ун-т. –Черкаси; ЧДТУ; 2017.- 201 с.

## ПРОГРАМНІ ЗАСОБИ

1. Windows 10 Professional © Microsoft Corporation, 1983-2020;
2. Microsoft Office Word 2019 © Microsoft Corporation, 1983-2020;
3. Microsoft Office Visio 2019 © Microsoft Corporation, 1983-2020;
4. Програма для розрахунку параметрів мережі © Сахно С., 2018  
Розрахунок параметрів мережі з N серверами;
5. Google Chrome © Google Inc, 2020.

					ЧДТУ 201850.005 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		