МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК ТА ІНЖЕНЕРІЇ

До захисту допускається
Завідувач кафедри
_____ Скарга-Бандурова І.С.
«____»_____ 2018 р.

ДИПЛОМНИЙ ПРОЕКТ (РОБОТА) БАКАЛАВРА

ПОЯСНЮВАЛЬНА ЗАПИСКА

НА ТЕМУ:

Локальна обчислювальна мережа банківської установи

Освітньо-кваліфікаційний рівень "бакалавр"
Напрям – 6.050102 "комп'ютерна інженерія"

Керівник проекту: _____ Ларгін В.А.
(підпис) (ініціали, прізвище)

Консультант з охорони праці _____ Критська Я.О.
(підпис) (ініціали, прізвище)

Студент: _____ Любенецький Д.А.
(підпис) (ініціали, прізвище)

Група: КІ-14ад

Сєвєродонецьк 2018

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Факультет Інформаційних технологій та електроніки
Кафедра Комп'ютерних наук та інженерії
Освітньо-кваліфікаційний рівень бакалавр
Напрям підготовки 6.050102 "комп'ютерна інженерія"
(шифр і назва)

ЗАТВЕРДЖУЮ:

Завідувач кафедри _____
_____І.С. Скарга-Бандурова
«_____» _____2018р.

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

Любенецький Дмитро Андрійович
(прізвище, ім'я, по батькові)

1. Тема роботи Локальна обчислювальна мережа банківської установи
_____
_____
керівник проекту (роботи) к.т.н. Ларгін Віктор Анатолійович
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від "14 " 05 2018 р. № 117/48
2. Термін подання студентом роботи 13.06.2018
3. Вихідні дані до роботи матеріали переддипломної практики
_____
_____
_____
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Розділ 1. Аналіз предметної області; Розділ 2. Проектування локально-обчислювальної мережі банківської установи; Розділ 3. Розробка ЛОМ установи банку; Розділ 4. Охорона праці у банківській установі та безпека в надзвичайних ситуаціях. _____
_____
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
електронні плакати
_____

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
4	ст.викл. Критська Я.О.		

7. Дата видачі завдання 14.05.2018

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Огляд літератури з теми ДП і постановка задачі	14.05.18-18.05.18	
2	Дослідження матеріалів	18.05.18-25.05.18	
3	Проектування локально-обчислювальної мережі банківської установи	25.05.18-01.06.18	
4	Тестування ЛОМ	03.06.18-06.06.18	
5	Розробка розділу охорона праці	06.06.18-09.06.18	
6	Оформлення електронних плакатів	10.06.18-13.06.18	
7	Оформлення пояснювальної записки	14.06.18-16.06.18	

Студент _____ Любенецький Д.А.
(підпис) (прізвище та ініціали)

Керівник _____ Ларгін В.А.
(підпис) (прізвище та ініціали)

Р Е Ф Е Р А Т

Пояснювальна записка до дипломного проекту (роботи) бакалавра: 77с., 16 рис., 12 табл., 34 бібліографічних джерел посилань, 1 додаток.

Об'єкт розробки: локальна обчислювальна мережа банківської установи.

Мета роботи: дослідження локально-обчислювальних мереж, захисту та механізмів проектування мереж.

В проекті виконано:

1. Аналіз предметної області.
2. Проектування локальної обчислювальної мережі.
3. Реалізація локальної обчислювальної мережі.

Отримано наступні результати: розроблена нова локальна обчислювальна мережа банку ПАТ “Акцент-Банк”.

Практичне значення, галузь застосування роботи: розроблену ЛОМ банківської установи можливо використати при оновленні старої мережі.

Ключові слова: Локальна обчислювальна мережа, банк, NetEmul, захист мережі, LAN, схема мережі.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

У пояснювальній записці застосовують такі терміни з відповідними визначеннями:

ДБЖ — Джерело безперебійного живлення.

ЕОМ — Електронна обчислювальна машина.

ЛОМ — Локальна обчислювальна мережа (Local Area Networks, LAN).

МЕ — Міжмережний екран.

ПК — Персональний комп’ютер.

ПЗ — Програмне забезпечення.

ВСТУП

Актуальність дипломної роботи. Стрімкий розвиток та поширення комп’ютерних мереж і відповідного програмного забезпечення — це одна з характерних прикмет сучасного періоду розвитку інформаційного суспільства. Сьогодні найважливішим застосуванням комп’ютерів є створення мереж, що забезпечують єдиний інформаційний простір для багатьох користувачів. Особливо наочно цей процес простежується на прикладі всесвітньої комп’ютерної мережі Internet.

Локальні комп’ютерні мережі банків дозволяють не лише безпечний доступ до спільних інформаційних ресурсів, але й раціональне колективне використання дорогих програмних та апаратних засобів. Через це виникла потреба в зручному і швидкому способі передачі інформації між обчислювальними машинами, таким способом стали — локально-обчислювальні мережі.

Саме за допомогою локальних мереж можливо з найменшими зусиллями організувати роботу великої кількості комп'ютерів, вести централізоване управління, забезпечити надійну інформаційну безпеку, і антивірусний захист.

Сучасні технології передачі даних надають банкам широкі можливості по організації різних видів послуг і сервісів:

1) організація електронного документообігу й ведення загальних архівів документів;

2) організація корпоративної телефонної мережі з єдиним планом нумерації;

3) організація систем конференц-зв’язку, у тому числі відеоконференц-зв’язку;

4) побудова розподілених систем відеоспостереження з єдиним центром зберігання даних;

5) організація дистанційного доступу до файлів і серверів з базами даних;

6) підключення до мережі Інтернет з можливістю організації єдиної корпоративної політики інформаційної безпеки.

Таким чином ЛОМ — це складна система, що включає тисячі найрізноманітніших компонентів: комп'ютери різних типів, системне й прикладне програмне забезпечення, мережеві адаптери, концентратори, комутатори й маршрутизатори, кабельна система. Основне завдання полягає в тому, щоб ця громіздка система якнайкраще справлялася з обробкою потоків інформації, що циркулюють між співробітниками банку й дозволяла приймати їм своєчасні й раціональні рішення.

У даному дипломі розглядається ЛОМ банківської установи "ПАТ Акцент-Банк".

Банківська установа має 20 комп'ютерів які зв'язані у ЛОМ старого покоління, яка не відповідає сучасним нормам захисту. Ця проблема виникає через те, що мережа швидко розвивається і з'являються нові технології, краща архітектура ЛОМ та нові загрози для безпеки. Щоб уникнути цього буде спроектована і реалізована нова ЛОМ з сучасними технологіями.

Установа банку має одноповерхову будівлю. На всій території знаходяться ПК і периферійні пристрої (принтер, веб-камера, сканер та інші). Банк використовує кабелі старого типу, тому інформація переміщується в мережі дуже повільно і ненадійно, відповідно до сучасних технологій. Необхідно прокласти кабелі з новою технологією, щоб досягти максимальної швидкості передачі даних у мережі. Таким чином інформація буде поступати по мережі швидше ніж раніше, що дозволить прискорити роботу банку. Захист мережі також буде підвищено.

Об'єктом дослідження дипломної роботи є локальна обчислювальна мережа банківської установи ПАТ "Акцент-Банк".

Предметом дослідження є банківська установа і організація ЛОМ в ній.

Мета дипломної роботи є розробка актуальної ЛОМ для банківської установи, розгляд теоретичних даних та варіантів програмних комплексів для виконання задачі.

Завданнями дипломної роботи є:

1) розгляд проблем мережі ПАТ “Акцент-Банк”;
2) розгляд теоретичних основ ЛОМ;
3) аналіз поставленої задачі та пошуки її вирішення;
4) дослідження різних програмних комплексів;
5) розробка актуальної ЛОМ для банківської установи;
6) розгляд систем захисту мережі;
7) підведення підсумків виконаної роботи.

Структура дипломної роботи. Дипломна робота складається зі скорочення і умовних позначень, вступу, чотирьох розділів, висновку й переліку джерел посилань.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Розгляд теоретичних даних ЛОМ

1.1.1 Модель ISO/OSI

Міжнародна Організація зі Стандартів (International Standards Organization, ISO) розробила модель, що чітко визначає різні рівні взаємодії систем, дає їм стандартні імена й указує, яку роботу повинен робити кожний рівень. Ця модель називається моделлю взаємодії відкритих систем (Open System Interconnection, OSI) або моделлю ISO/OSI.

У моделі OSI взаємодія ділиться на сім рівнів або шарів, як показано на рис.1.1 [1]. Кожний рівень має справу з одним певним аспектом взаємодії. Таким чином, проблема взаємодії декомпозована на 7 приватних проблем, кожна з яких може бути вирішена незалежно від інших. Кожний рівень підтримує інтерфейси з рівнями, які знаходяться вище і нижче.

Модель OSI описує тільки системні засоби взаємодії, не стосуючись додатків кінцевих користувачів. Додатки реалізують свої власні протоколи взаємодії, звертаючись до системних засобів. Варто мати на увазі, що додаток може взяти на себе функції деяких верхніх рівнів моделі OSI, у такому випадку при необхідності обміну даними воно звертається прямо до системних засобів, що виконують функції нижніх рівнів, що залишилися, моделі OSI.

Кожний рівень виконує певні комунікаційні завдання й за допомогою відповідних протоколів взаємодіє із сусідніми рівнями ієрархії. Передача інформації між двома мережними пристроями здійснюється з використанням цієї ієрархії рівнів (стека) у кожному із пристроїв. Наприклад, якщо робоча станція обмінюється даними із сервером, передача інформації починається в робочій станції на Прикладному рівні. Потім формується певна інформація на більш нижніх рівнях доти, поки дані не досягнуть Фізичного рівня й не будуть по мережі передані серверу. Сервер приймає дані на Фізичному рівні свого стека й передає їх для інтерпретації більш високим рівням, поки дані не досягнуть

Прикладного рівня. Кожний рівень називається або за іменем, або за положенням в стеці (1-й рівень, 2-й рівень і т. д.).

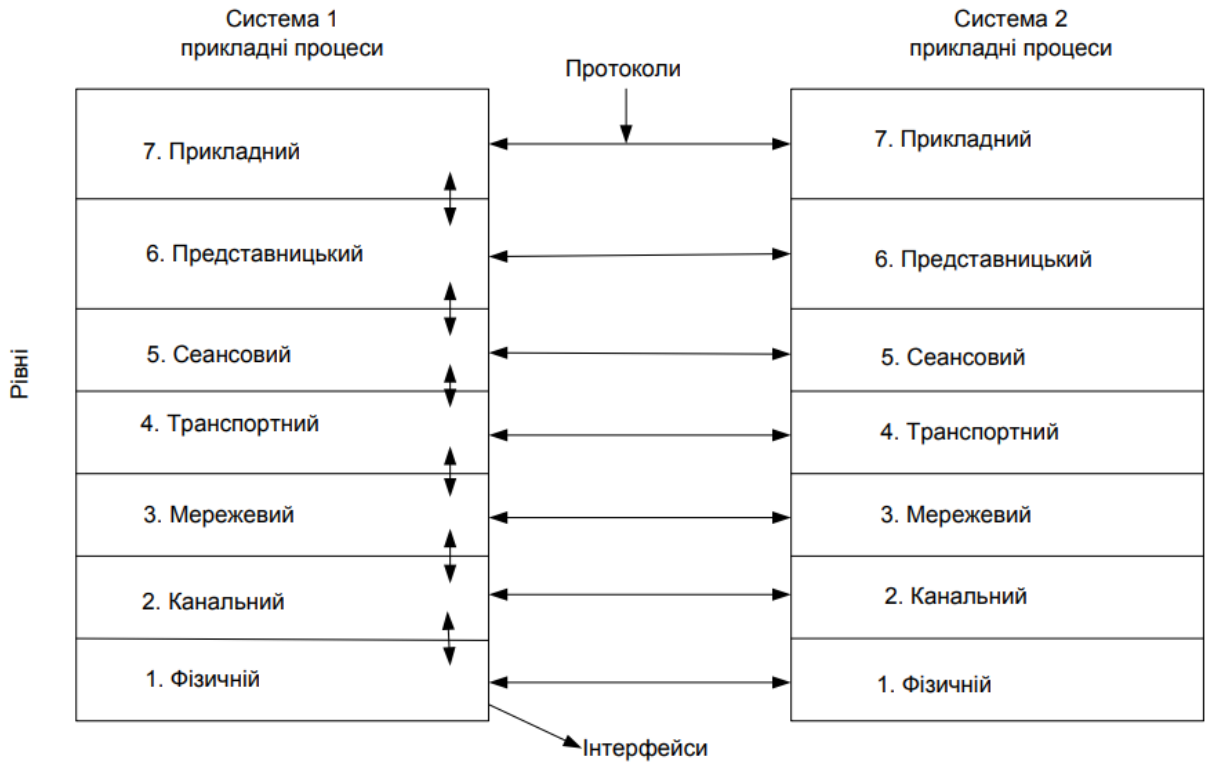

Рисунок 1.1 — Модель взаємодії відкритих систем ISO/OSI

Модель ISO/OSI визначає функції рівнів у такий спосіб:

Таблиця 1.1 — Рівні моделі OSI та їх основні функції [2]

Рівень	**Функції**
7. Прикладний рівень	Кінцевий продукт.
6. Рівень подання даних	Представлення даних.
5. Сеансовий рівень	Запуск, зупинка, відновлення передачі.
4. Транспортний рівень	Керування наскрізною доставкою даних.
3. Мережний рівень	Адреса, маршрутизатори.
2. Канальний рівень	Доступ до середовища передачі даних.
1. Фізичний рівень	Передачі даних у двійковій формі.

Фізичний рівень. Цей рівень описує: усі фізичні середовища передачі даних (кабель, оптоволокно, хвилі радіо й інших діапазонів); мережні рознімання;

топологію мережі; методи передачі й кодування сигналу; пристрій передачі даних; мережні інтерфейси;

Канальний рівень. Цей рівень кодує дані у вигляді фреймів, після чого відформатовані фрейми надходять на Фізичний рівень, де вузол, що передає, може відправити їх у комунікаційне середовище (наприклад, у кабель). Приймаючий вузол одержує фрейм від Фізичного рівня, декодує електричний сигнал, що представляє розряди даних, перетворює окремі розряди у фрейм і перевіряє наявність помилок у фреймі.

Мережний рівень. Мережний рівень аналізує адресну інформацію протоколу передачі пакетів і посилає їх по найбільш відповідному маршруту – фізичному або логічному, забезпечуючи максимальну ефективність мережі. Також цей рівень забезпечує передачу пакетів між мережами через маршрутизатори. Маршрутизатор – це пристрій, що збирає інформацію про топологію міжмережних з'єднань і на її підставі пересилає пакети мережного рівня в мережу призначення. Для того, щоб передати повідомлення від відправника, що перебуває в одній мережі, одержувачу, що перебуває в іншій мережі, потрібно зробити деяку кількість транзитних передач (hops) між мережами, щораз вибираючи відповідний маршрут. Таким чином, маршрут становить послідовність маршрутизаторів, через які проходить пакет. Проблема вибору найкращого шляху називається маршрутизацією, і її рішення є головним завданням мережного рівня. Ця проблема ускладнюється тим, що самий короткий шлях не завжди найкращий. Часто критерієм при виборі маршруту є час передачі даних по цьому маршруту; він залежить від пропускної здатності каналів зв'язку й інтенсивності трафіка, що може змінюватися із часом.

Пакети даних. У мережах та системах передачі досить рідко передача даних здійснюється окремими символами (байтами), частіше — пакетами (кадрами, фреймами) певного формату. Формати представлення даних можуть розрізнятися за наступними ознаками:

1) порядок проходження бітів і розмірність символу в бітах;

2) порядок проходження байтів;

3) подання і кодування символів;

4) структура і синтаксис файлів.

На рис. 1.2 наводиться приклад пакету даних формату IEEE 802.3, прийнятого в мережах Ethernet. Компресія або упаковка даних скорочує час передачі даних. Кодування переданої інформації забезпечує захист її від перехоплення [3].

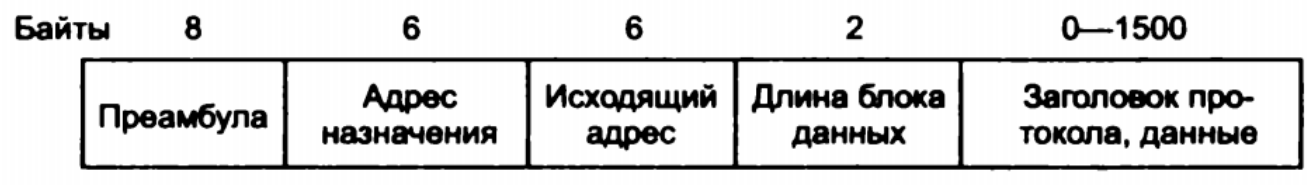

Рисунок 1.2 — Формат кадру (фрейма) IEEE 802.3

Транспортний рівень. Транспортний рівень (transport layer), подібно Канальному й Мережному рівням, виконує функції, що забезпечують надійне пересилання даних від передавального вузла до приймаючого. Наприклад, Транспортний рівень гарантує, що дані передаються й приймаються в тому самому порядку. Крім цього, після завершення пересилання приймаючий вузол може послати підтвердження (яке іноді називається квитанцією).

Сеансовий рівень. Сеансовий рівень (session layer) відповідає за встановлення й підтримку комунікаційного каналу між двома вузлами, він забезпечує черговість роботи вузлів: наприклад, визначає, який з вузлів першим починає передачу даних. Крім цього, Сеансовий рівень визначає тривалість роботи вузла на передачу, а також спосіб відновлення інформації після помилок передачі. Якщо сеанс зв'язку був помилково перерваний на більш низькому рівні, Сеансовий рівень намагається відновити передачу даних.

Рівень подання. Представницький рівень (presentation layer) управляє форматуванням даних, оскільки прикладні програми нерідко використовують різні способи подання інформації. У деякому сенсі Представницький рівень виконує функції програми перевірки синтаксису. Він гарантує, що числа й символьні рядки передаються саме в такому форматі, який зрозумілий

Представницькому рівню приймаючого вузла. Представницький рівень також відповідає за шифрування даних. Шифрування (encryption) – це процес засекречування інформації, що не дозволяє неавторизованим користувачам прочитати дані у випадку їхнього перехоплення. Наприклад, у локальній мережі може шифруватися пароль облікового запису комп'ютера, або ж номер кредитної картки може шифруватися за допомогою технології Secure Sockets Layer (SSL) (Протокол захищених сокетів) при передачі по глобальній мережі.

SSL — відповідне програмне забезпечення, як і сам протокол, в наш час широко використовується (у тому числі програмами Firefox, Safari, Internet Explorer), тому варто розглянути SSL більш детально. Отже, SSL створює захищене з'єднання між двома сокетами, що дозволяє:

1) клієнту та серверу домовитися про параметри;

2) провести аутентифікацію сервера клієнтом;

3) організувати таємне спілкування;

4) забезпечити захист цілісності даних.

SSL складається з двох субпротоколів, один з яких призначений для встановлення захищеного з'єднання, а другий — для використання цього з'єднання [4].

Прикладний рівень. Цей рівень безпосередньо управляє доступом до додатків і мережних служб. Прикладом таких служб є передача файлів, керування файлами, вилучений доступ до файлів і принтерів, керування повідомленнями електронної пошти й емуляція терміналів. Саме цей рівень програмісти використовують для зв'язку робочих станцій з мережними службами (наприклад, для надання деякій програмі послуг електронної пошти або доступу до бази даних через мережу) [5].

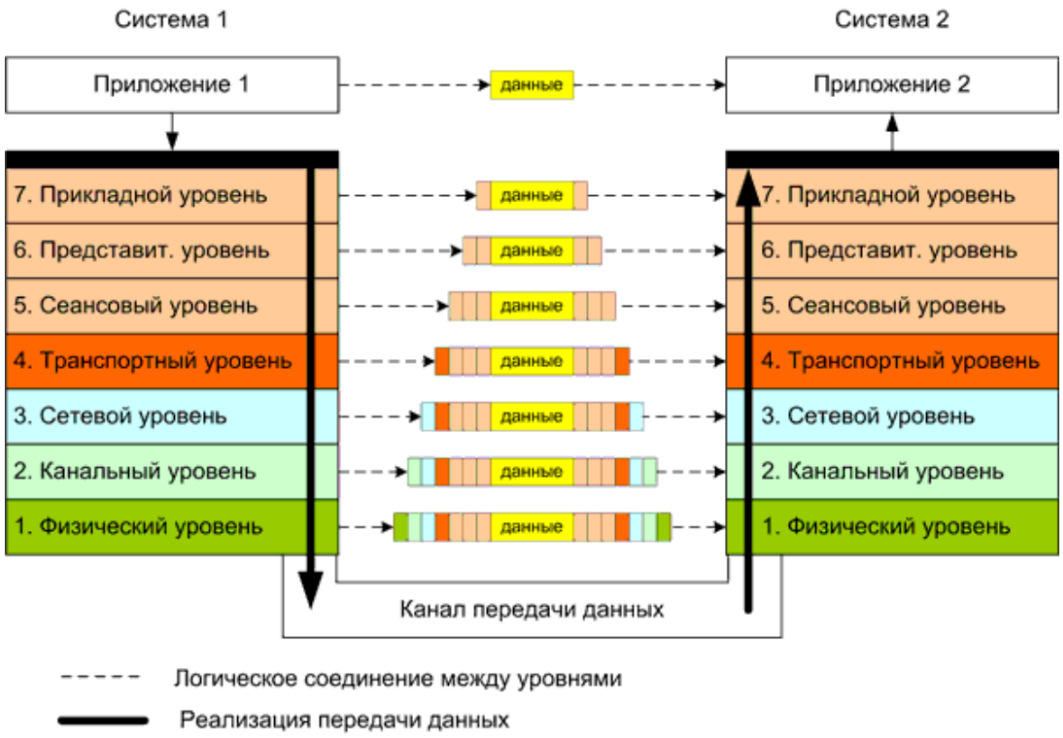

Рисунок 1.3 — Передача пакетів інформації по рівням

1.1.2 Засоби реалізації ЛОМ

Основними компонентами мережі є (рис. 1.4):

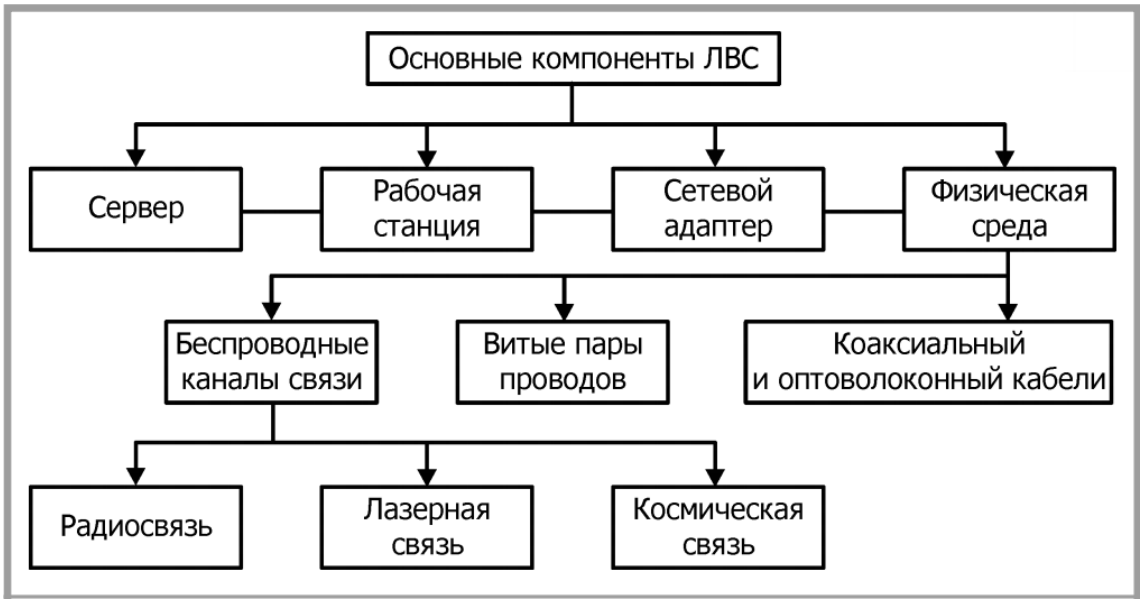

Рисунок 1.4 — Основні компоненти ЛОМ

1) фізичне середовище передачі даних (мережевий кабель);
2) робочі станції на базі комп'ютерів;
3) плати інтерфейсу середовища (мережеві адаптери);
4) сервери мережі

Розглянемо докладніше обладнання, що використовується в ЛОМ.

Мережеві адаптери (СА). Основні функції адаптерів і їх технічні характеристики визначаються підтримуваним рівнем протоколу ЛОМ у відповідності з архітектурою семирівневої еталонної моделі.

Адаптер (adapter) — пристрій або програма, призначені для узгодження параметрів вхідних і вихідних сигналів у цілях сполучення об'єктів.

Концентратори (хаби) — concentrator — пристрій або функціональний блок, у якого сумарна пропускна здатність вхідних каналів вище пропускної здатності вихідного каналу. Так як потоки вхідних даних в концентраторі більше вихідного потоку, то головним його завданням є концентрація даних. При цьому трапляються ситуації, коли кількість блоків даних, що надходить на входи концентратора, перевищує його можливості. Тоді концентратор ліквідує частину цих блоків. Ядром концентратора є процесор. Для об'єднання вхідної інформації найчастіше використовується множинний доступ з поділом часу. TDMA — Time Division Multiple Access — множинний доступ з принципом тимчасового мультиплексування каналів.

Передавачі (трансівери) і повторювачі (репітери). З допомогою цих пристроїв можна об'єднати декілька сегментів мережі з шинною технологією, збільшуючи таким чином загальну протяжність мережі.

Трансівер (прийомопередавач) – (transmitter + receiver = transceiver) – це пристрій, призначений для прийому пакетів від контролера робочих станцій і передачі їх в шину. Він також виявляє колізії в шині. Конструктивно прийомопередавач і контролер можуть об'єднуватися на одній платі або перебувати в різних вузлах. Трансівер — це частина мережевого адаптера, яка виконує наступні функції:

1) прийом і передача даних з кабелю на кабелі;

2) визначення колізій на кабелі;

3) електрична розв'язка між кабелем і іншою частиною адаптера;

4) захист кабелю від некоректної роботи адаптера.

Репітер (повторювач) (repeater) – пристрій з автономним живленням, що забезпечує передачу даних між сегментами певної довжини. Він служить для об'єднання в єдину мережу декількох сегментів кабелю і збільшення тим самим загальної довжини мережі. Повторювач приймає сигнали з одного сегмента кабелю і побітно синхронно повторює їх в іншому сегменті, покращуючи форму і потужність імпульсів, а також синхронізуючи імпульси.

Мости — це пристрої для логічної структуризації мережі. Міст (bridge) – ретрансляційна система, що з'єднує два канали передачі даних. Вони використовуються для з'єднання в основному ідентичних мереж, що мають певні фізичні відмінності на фізичному і канальному рівнях. Міст ділить розділяючи середовище передачі мережі на частини (часто звані логічними сегментами), передаючи інформацію з одного сегмента в інший тільки в тому випадку, якщо така передача дійсно необхідна, тобто якщо адреса комп'ютера призначення належить іншій підмережі. Тим самим міст ізолює трафік однієї підмережі від трафіка іншої, підвищуючи загальну продуктивність передачі даних в мережі.

Комутатор (switch) за принципом обробки кадрів нічим не відрізняється від моста. Основна його відмінність від моста полягає в тому, що він є свого роду комунікаційним мультипроцесором, оскільки кожний його порт оснащений спеціалізованим процесором, який обробляє кадри по алгоритму моста незалежно від процесорів інших портів. В перелік функцій, виконуваних комутатором локальних мереж, входять:

1) забезпечення наскрізної комутації;

2) наявність засобів маршрутизації;

3) підтримка простого протоколу управління мережею (SNMP);

4) імітація моста або маршрутизатора;

5) організація віртуальних мереж;

6) швидкісна ретрансляція блоків даних.

Шлюз (gateway) — ретрансляційна система, що забезпечує взаємодію двох інформаційних систем. Шлюзи застосовуються для різних мереж. Вони дають можливість об'єднати мережі з різними типами системного і прикладного програмного забезпечення і виконують протокольні перетворення для всіх семи рівнів моделі OSI, зокрема маршрутизацію пакетів, перетворення повідомлення з одного формату в інший або з однієї системи кодування в іншу. Шлюз (рис. 1.5) — найбільш складна ретрансляційна система, що забезпечує взаємодію двох мереж з різними наборами протоколів усіх семи рівнів. У свою чергу, набори протоколів можуть спиратися на різні типи фізичних засобів з'єднання. Штабелі протоколів і інформаційні мережі об'єднуються в єдине ціле спеціальними прикладними процесами шлюзу. Зазвичай шлюз виконує перетворення між двома протоколами. З допомогою шлюзів можна підключити ЛОМ до головного комп'ютера або до глобальної мережі.

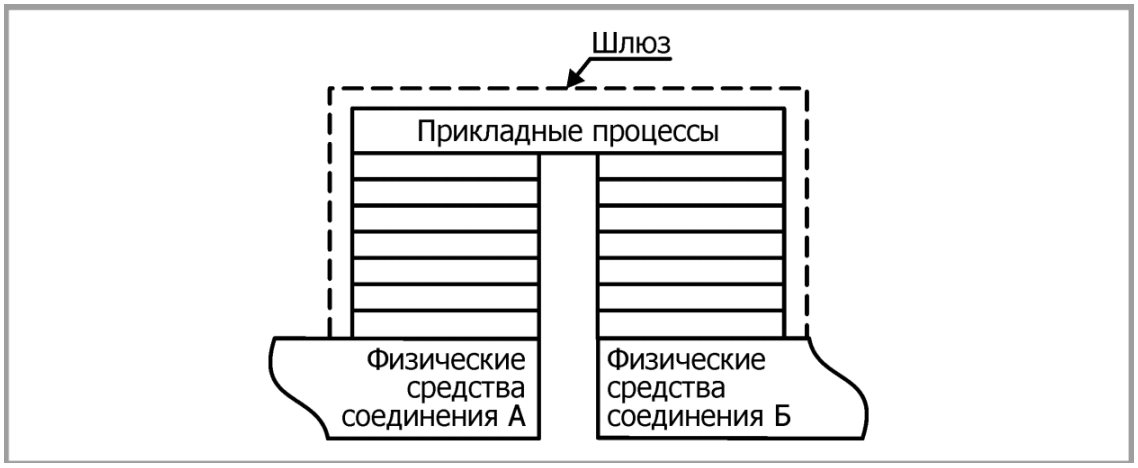

Рисунок 1.5 — Структура шлюзу

Маршрутизатор (роутер) (router) — ретрансляційна система, що з'єднує дві комунікаційні мережі або їх частини. Маршрутизатори утворять логічні сегменти за допомогою явної адресації, оскільки використовують не плоскі апаратні, а складові числові адреси. У цих адресах є поле номера мережі, так що всі комп'ютери, у яких значення цього поля однакове, належать до одного сегмента, званого в цьому випадку підмережею (subnet). Маршрутизатори більш надійно і більш ефективно, ніж мости, ізолюють трафік окремих частин мережі

один від одного. Крім локалізації трафіку, маршрутизатори виконують ще багато інших корисних функцій. Вони можуть працювати в мережі із замкнутими контурами, при цьому здійснюючи вибір найбільш раціонального маршруту з декількох можливих. Маршрутизатори забезпечують досить складний рівень сервісу: вибір найкращого маршруту передачі повідомлення, адресованого іншій мережі; управління збалансованої навантаженням у мережі шляхом рівномірного розподілу потоків даних; захист даних; буферизацію переданих даних; різні протокольні перетворення [6].

1.1.3 Канали передачі даних

Канал передачі даних являє собою фізичне середовище, у якому поширюються сигнали, і сукупність технічних пристроїв, що передають сигнали через цю фізичну середу.

Фізична середовище може бути одного з двох типів:

1) провідна;

2) бездротова.

В якості провідної середовища в комп'ютерних мережах можуть використовуватися кабелі наступних типів:

1) вита пара (неекранована, екранована);
2) коаксіальний кабель (тонкий, товстий);
3) оптоволоконний кабель.

Вита пара — це вид кабелю, який складається з двох звитих між собою ізольованих проводів або з кількох таких пар, покритих пластиковою оболонкою. Скручування провідників (з невеликою кількістю витків на одиницю довжини) проводиться з метою зменшення впливу зовнішніх електромагнітних перешкод на сигнали, які передаються, а також зменшення взаємних наведень при передачі. Основне гідність витої пари – дешевизна, основні недоліки – погана перешкодозахищеність (навіть у екранованої витої пари) і низька швидкість передачі даних.

Коаксіальний кабель складається з провідної жили, шару ізоляції, металевої обплетення і зовнішньої оболонки. Порівняно з кручений парою коаксіальний кабель володіє більш високою механічною міцністю і завадостійкістю, але його вартість набагато вище. Товстий кабель міцніше тонкого і передає сигнали на більш далеку відстань, зате тонкий кабель дешевше.

Оптоволоконний кабель є ідеальної передавальної середовищем. Він не схильний до дії електромагнітних полів, сам практично не випромінює і забезпечує найбільшу швидкість передачі інформації. Однак, порівняно з попередніми типами провідний фізичного середовища оптоволоконний кабель коштує значно дорожче і менш технологічний в експлуатації [7].

1.1.4 Типи ЛОМ

Локально-обчислювальні мережі поділяються на два типи:

1) одноранговi мережі;

2) мережі з виділеним сервером.

Одноранговi мережі (по іншому називаються робочими групами) звичайно використовуються, коли кількість ПК не перевищує 10, всі вони розташовані компактно, розширення мережі у ближній час не планується і питання захисту даних не критичні.

В одноранговій мережі всі комп'ютери рівноправні. Кожен комп'ютер функціонує і як клієнт, і як сервер. При цьому кожен користувач виконує функції адміністратора: самостійно вирішує, які ресурси на своєму комп'ютері зробити загальнодоступними в мережі.

Для з'єднання комп'ютерів в одноранговy мережу застосовується проста кабельна система. (рис. 1.6)

Перевагами одноранговоï мережі є низька вартість і висока надійність, недоліками – залежність ефективності функціонування мережі від кількості робочих станцій, складність управління мережею, складність забезпечення

захисту інформації, неможливість синхронного оновлення або зміни програмного забезпечення робочих станцій.

Рисунок 1.6 — Однорангова мережа

У мережах з виділеним сервером операційна система повинна забезпечувати захист розміщених на сервері даних від випадкового псування і несанкціонованого доступу, управляти правами користувачів і підтримувати зв'язок між всіма робочими станціями, на яких можуть бути встановлені різні ОС.

Середовища передачі даних можуть використовувати як дротові, так і бездротові канали зв'язку (рис. 1.7).

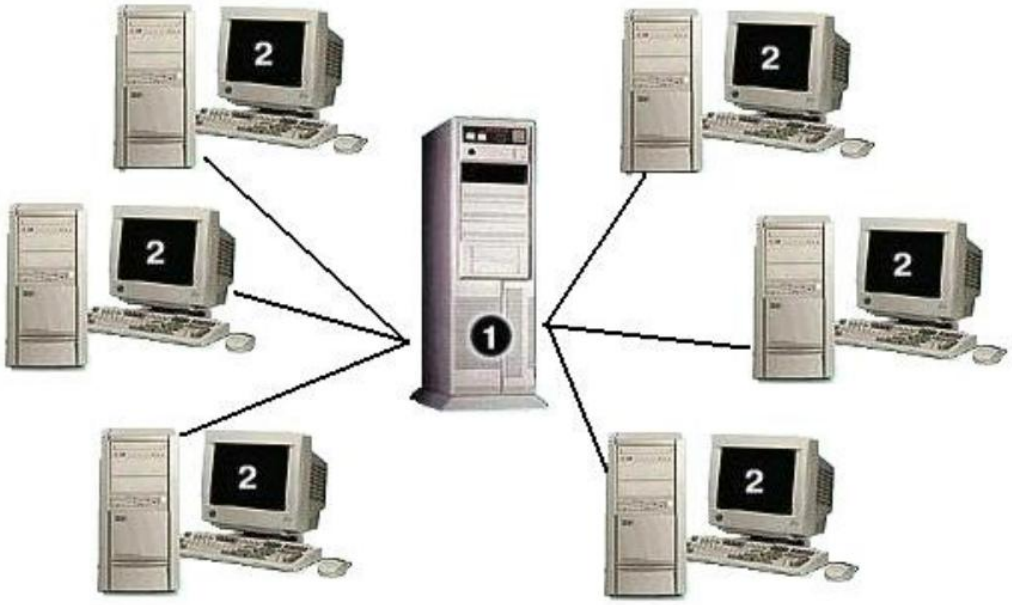

Рисунок 1.7 — Мережа з виділеним сервером

При необхідності можна збільшувати число мережевих серверів, що дозволяє ефективно обслуговувати тисячі користувачів.

Основним аргументом при виборі мережі на основі сервера є, як правило, захист даних.

Перевагами мережі з виділеним сервером є надійна система захисту інформації, висока швидкодія, відсутність обмежень на кількість робочих станцій і простота управління порівняно з одноранговими мережами. Недоліками такої мережі є висока вартість через виділення потужного комп'ютера під сервер, залежність швидкодії і надійності мережі від сервера, більш складне управління порівняно з одноранговою мережею [7].

1.1.5 Топології комп’ютерних мереж

При організації комп’ютерної мережі дуже важливим є вибір топології, тобто компонування мережевого обладнання і кабельної інфраструктури. Потрібно обрати таку топологію, яка забезпечила б надійну й ефективну роботу мережі, зручне керування потоками мережевих даних. Бажано також, щоб мережа за вартістю створення й супроводу вийшла недорогою, але в той же час, залишалися можливості для її подальшого розширення,також бажано, щоб залишилися можливості для переходу до більш швидкісних технологій зв’язку.

Існують три базові топології, на основі яких будується переважна більшість мереж: шина, зірка, кільце.

“Шина” (Bus). У цій топології усі комп’ютери з’єднуються один з одним кабелем (рис. 1.8). Послані в таку мережу дані передаються всім комп’ютерам, але обробляє їх лише той комп’ютер,апаратна MAC-адреса якого записана у кадрі як адреса одержувача.

Ця топологія дуже проста в реалізації і дешева (вимагає найменше кабелю), однак має ряд істотних недоліків:

1) Такі мережі важко розширити (збільшити число комп’ютерів у мережі та кількість сегментів окремих відрізків кабелю, що їх з’єднує).

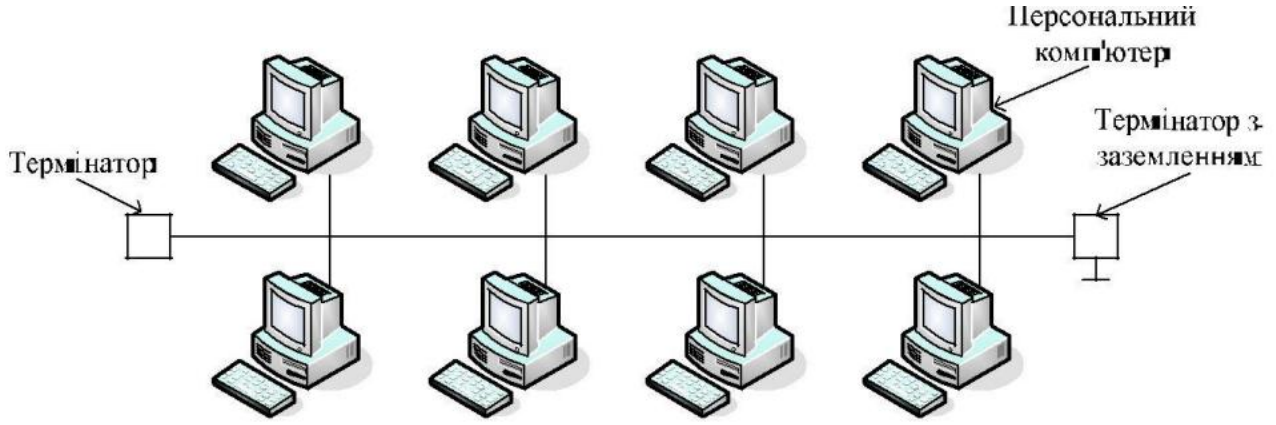

Рисунок 1.8 — Мережа з топологією “шина”

2) Оскільки шина використовується спільно, у кожний момент часу передачу може вести тільки один з комп’ютерів. Якщо передачу одночасно починають два або більше комп’ютерів, виникає викривленість сигналу (зіткнення, або колізія), що приводить до пошкодження всіх кадрів. У цьому випадку комп’ютери змушені припиняти передачу, а потім по черзі ретранслювати дані. Вплив зіткнень тим помітніший, чим вищий обсяг переданої мережею інформації та чим більше комп’ютерів, підключених до шини. Ці два фактори знижують як максимально можливу,так і загальну продуктивність мережі, сповільнюючи її роботу.

3) “Шина” є пасивною топологією – комп’ютери тільки “прослуховують” кабель і не можуть відновлювати при передачі мережею сигнали, що затухають. Щоб подовжити мережу, потрібно використовувати повторювачі (репітери), що підсилюють сигнал перед його передачею в наступний сегмент.

4) Надійність мережі з топологією “шина” низька. Коли електричний сигнал досягає кінця кабелю, він, якщо не вжити спеціальних заходів, відбивається, порушуючи роботу всього сегмента мережі. Щоб запобігти такому відбиттю сигналів, на кінцях кабелю встановлюються спеціальні резистори (термінатори), що поглинають сигнали. Якщо ж у будь-якому місці кабелю виникає обрив наприклад, при порушенні цілісності кабелю або просто при від’єднанні

конектора, — то виникають два незатерміновані сегменти, на кінцях яких сигнали починають відбиватися, і вся мережа перестає працювати.

“Кільце” (Ring). У даній топології кожний з комп’ютерів з’єднується із двома іншими так, щоб від одного він одержував інформацію, а іншому передавав її (рис. 1.9). Останній комп’ютер підключається до першого, і кільце замикається.

Переваги топології кільце:

1) Оскільки кабелі не мають вільних кінців,то термінатори тут не потрібні.

2) Кожен комп’ютер виступає в ролі повторювача, підсилюючи сигнал, що дозволяє будувати мережі великого розміру.

3) Через відсутність зіткнень топологія має високу стійкість до перевантажень, забезпечуючи при цьому ефективну роботу з великими потоками інформації, що передаються мережею.

Недоліки топології кільце:

1) Сигнал у “кільці” повинен пройти послідовно (і тільки в одному напрямку) через усі комп’ютери, кожний з яких перевіряє, чи не йому адресована інформація, тому час передачі може бути суттєвим.

2) Підключення до мережі нового комп’ютера або іншого пристрою потребує зупинки роботи всієї мережі, що порушує роботу інших комп’ютерів в мережі.

3) Вихід з ладу хоча б одного з комп’ютерів або пристрою порушує роботу всієї мережі.

4) Обрив або коротке замикання в будь-якому з кабелів кільця — робить роботу всієї мережі неможливою.

5) Щоб запобігти зупинці мережі при відмові комп’ютера або обриві кабелю, як правило, прокладають два кільця, що суттєво здорожує мережу.

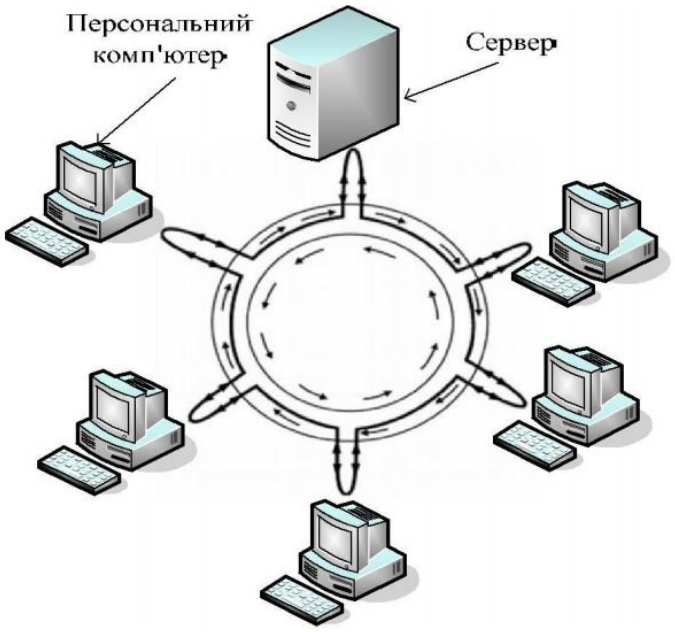

Рисунок 1.9 — Мережа з топологією “кільце”

Топологія “зірка-шина” (Star Bus). Це найпоширеніша на сьогодні топологія. Периферійні комп’ютери підключаються не до центрального комп’ютера, а до пасивного концентратора,або хабу (hub) (рис. 1.10). Останній, на відміну від центрального комп’ютера, ніяк не відповідає за керування обміном даними, а виконує ті ж функції, що й повторювач, тобто відновлює вхідні сигнали й пересилає їх усім — іншим підключеним до нього комп’ютерам і пристроям. Саме тому дана топологія, хоча фізично й виглядає як “зірка”, логічно є топологією “шина” (цей факт відображається у її назві).

Незважаючи на значні витрати кабелю, характерні для мереж типу “зірка”, ця топологія має істотні переваги перед іншими, що й обумовило її найпоширеніше застосування в сучасних мережах.

Переваги мереж типу “зірка-шина”:

1) Надійність – підключення до центрального концентратора й відключення комп’ютерів від нього ніяк не відображується на роботі іншої частини мережі; обриви кабелю впливають тільки на комп’ютери, які ним з’єднані; термінатори не потрібні.

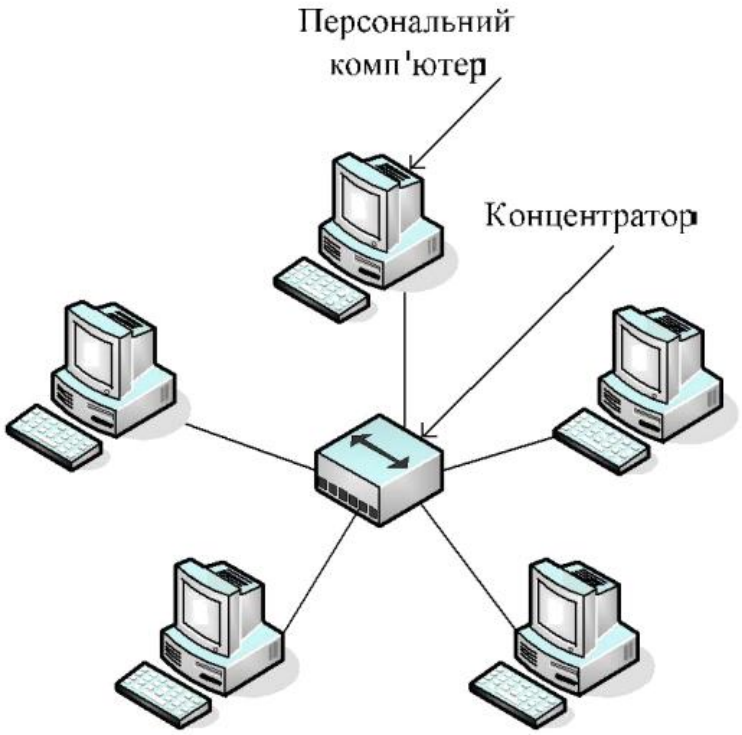

Рисунок 1.10 — Мережа з топологією “зірка-шина”

2) Легкість при обслуговуванні й усуненні проблем – усі комп’ютери й мережеві пристрої підключаються до центрального з’єднувального пристрою, що суттєво спрощує обслуговування й ремонт мережі.

3) Захищеність – концентрація точок підключення в одному місці дозволяє легко обмежити доступ до життєво важливих об’єктів мережі.

Реальні комп’ютерні мережі постійно розширюються і модернізуються. Тому майже завжди така мережа є гібридною, тобто її топологія являє собою комбінацію декількох базових топологій. Легко уявити собі гібридні топології, що є комбінацією “зірки” і “шини”, або “кільця” і “зірки”. Однак особливо слід виділити топологію **“дерево” (Tree)**, яку можна розглядати як об’єднання декількох “зірок” (рис. 1.11). Саме ця топологія на сьогодні є найбільш популярною при побудові локальних мереж [7].

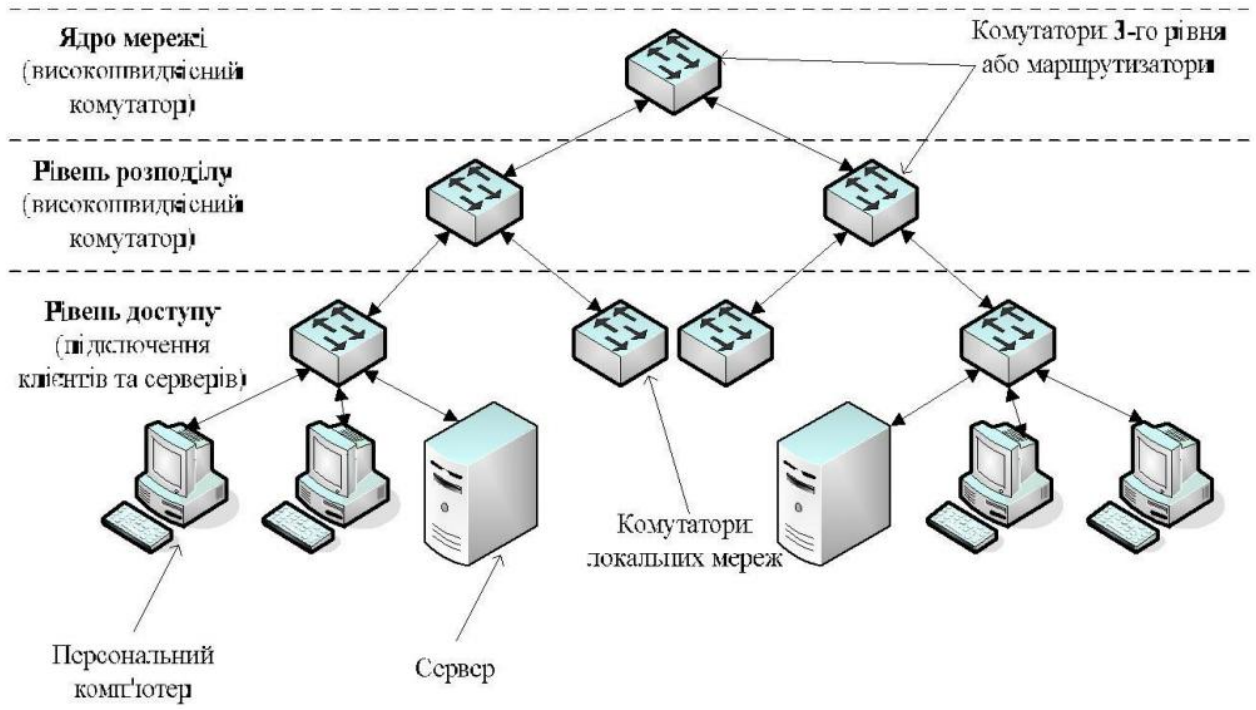

Рисунок 1.11 — Мережа з топологією “дерево”

1.1.6 Програмне забезпечення комп'ютерних мереж

Програмне забезпечення (ПЗ) комп'ютерних мереж призначене для організації колективного доступу до обчислювальних та інформаційних ресурсів мережі, а також динамічного розподілу і перерозподілу ресурсів мережі з метою підвищення оперативності обробки інформації при інтенсивному трафіку або у випадках виходу з ладу окремих апаратних компонентів мережі.

Програмне забезпечення комп'ютерних мереж включає три компоненти.

1) Загальне програмне забезпечення, утворене базовим ПЗ окремих комп'ютерів, що входять до складу мережі.

2) Спеціальне програмне забезпечення, до складу якого входять прикладні програмні засоби, що враховують специфіку предметної області при реалізації завдань користувача, наприклад завдань аналізу, прогнозу або управління.

3) Системне мережне програмне забезпечення, що являє собою комплекс програмних засобів, що підтримують і координують взаємодію всіх ресурсів комп'ютерної мережі як єдиної системи.

Особлива роль у ПЗ комп'ютерної мережі відводиться системі мережевого програмного забезпечення, функції якого реалізуються розподіленою мережевою операційною системою (ОС), що забезпечує:

1) міжпрограмний метод доступу (можливість організації зв'язку між окремими прикладними програмами комплексу, реалізованими в різних вузлах мережі);

2) доступ окремих прикладних програм до ресурсів мережі (і в першу чергу до пристроїв введення - виведення);

3) синхронізацію роботи прикладних програмних засобів в умовах їх одночасного звернення до одного і того ж обчислювального ресурсу;

4) обмін наборами даних (файлами) між ЕОМ мережі;

5) захист даних і обчислювальних ресурсів мережі від несанкціонованого доступу.

Найбільш широке поширення одержали мережеві операційні системи Windows NT, Windows XP, Server 2003, Server 2008 фірми Microsoft і NetWare фірми Novell [8].

1.1.7 Технології локальних мереж

У локальних мережах, як правило, використовується роздільне середовище передавання даних (моноканал) і основна роль відводиться протоколам фізичного та канального рівнів, оскільки ці рівні найбільше відображають специфіку локальних мереж. Мережні технології - це узгоджений набір стандартних протоколів і програмно-апаратних засобів, які їх реалізують, достатній для побудови локальної обчислювальної мережі. Мережні технології називають базовими технологіями або мережними архітектурами локальних мереж. Мережна технологія або архітектура визначає топологію і метод доступу до середовища передавання даних, кабельну систему або середовище передавання даних, формат мережних кадрів, вид кодування сигналів, швидкість передавання у локальній

мережі. У сучасних локальних обчислювальних мережах найбільше розповсюдження отримали такі технології: Ethernet, Token-Ring, ArcNet, FDDI.

Мережні технології локальних мереж IEEE802.3/Ethernet. На сьогоднішній день найбільш популярною у світі є мережна технологія IEEE802.3/Ethernet. У класичній локальній мережі Ethernet застосовується стандартний коаксіальний кабель двох видів (товстий і тонкий). Проте все більшого розповсюдження набула версія Ethernet, що використовує в якості середовища передавання витої пари, так як їх монтаж і обслуговування набагато простіше. У локальних мережах Ethernet застосовуються топології типу "шина" і типу "пасивна зірка", а метод доступу CSMA/CD.

Метод доступу, що використовується в мережах Ethernet на розділеному провідному середовищі, носить назву CSMA/CD (Carrier Sense Multiple Access with Collision Detection — прослуховування несучої частоти з множинним доступом і розпізнавання колізій). Назва методу досить добре описує його особливості.

Всі комп'ютери в мережі на розділеному середовищі мають можливість негайно (з врахуванням затримки поширення сигналу в фізичному середовищу) одержати дані, які будь-який з комп'ютерів почав передавати на загальну середу. Кажуть, що середовище, до якого підключені всі станції, працює в режимі колективного доступу (Multiply Access, MA).

Щоб одержати можливість передавати кадр, інтерфейс-відправник повинен пересвідчитися, що спільне середовище вільне. Це досягається прослуховуванням основної гармоніки сигналу, яка ще називається несучою частотою (Carrier Sense, CS) [9].

Мережні технології локальних мереж IEEE802.5/Token-Ring. Мережа Token-Ring передбачає використання роздільного середовища передавання даних, яке утворюється об'єднанням всіх вузлів в кільце. Мережа Token-Ring має зірково-кільцеву топологію (основна кільцева і зіркова додаткова топологія). Для доступу до середовища передавання даних використовується маркерний метод (детермінований маркерний метод). Стандарт підтримує виту пару (екрановану і

неекрановану) і оптоволоконний кабель. Максимальна кількість вузлів на кільці - 260, максимальна довжина кільця - 4000 м. Швидкість передавання даних до 16 Мбіт/с.

Мережні технології локальних мереж IEEE802.4/ArcNet. В якості топології локальна мережа ArcNet використовує "шину" і "пасивну зірку". Підтримує екрановану і неекрановану виту пару та оптоволоконний кабель. У мережі ArcNet для доступу до середовища передачі даних використовується метод передавання повноважень. Серед основних переваг локальної мережі ArcNet можна виділити високу надійність, низьку вартість адаптерів і гнучкість. Основним недоліком мережі є низька швидкість передачі інформації (2,5 Мбіт/с). Максимальна кількість абонентів - 255. Максимальна довжина мережі - 6000 метрів.

Мережні технології локальних мереж FDDI (Fiber Distributed Data Interface). Мережна технологія FDDI (Fiber Distributed Data Interface) - стандартизована специфікація для мережної архітектури високошвидкісного передавання даних по оптоволоконним лініям. Швидкість передавання - 100 Мбіт/с. Ця технологія багато в чому базується на архітектурі Token-Ring і використовує детермінований маркерний доступ до середовища передачі даних. Максимальна довжина кільця мережі - 100 км. Максимальна кількість абонентів мережі - 500. Мережа FDDI - високонадійна мережа, яка створюється на основі двох оптоволоконних кілець, які утворюють основний і резервний шляхи передавання даних між вузлами [10-13].

1.2 Захист комп’ютерних мереж

На даний час безпека мереж – це дуже актуальна тема інформаційних технологій. Треба відмітити, що стосовно до мережевих технологій безпека ніколи не буває абсолютно гарантованою. Забезпечення необхідного рівня безпеки передбачає застосування комплексу заходів, які направлені на захист комп’ютерів мережі та інформації, що зберігається. Якщо грамотно побудувати корпоративну мережу, але упустити питання забезпечення необхідного рівня

безпеки - нічого гарного не вийде. У найнесподіваніший момент можна втратити всю інформацію, заради доступу до якої й будувалася мережа.

Бажані властивості безпечної мережі:

1) Конфіденційність. Тільки відправник і передбачуваний одержувач повинні бути здатні розуміти вміст переданих повідомлень. Оскільки зловмисники можуть перехопити повідомлення, воно повинно бути якимось чином зашифровано так, щоб зловмисник, перехопив повідомлення, не зміг його розшифрувати.

2) Цілісність повідомлення. Відправник хоче бути впевненим, що дані при передачі не будуть змінені. Для забезпечення такої цілісності найчастіше застосовуються розширення методів перевірки контрольних сум разом з протоколами надійного транспортування та канального рівня.

3) Аутентифікація кінцевої точки. Як відправник, так і одержувач повинні бути здатні підтвердити особистість співрозмовника — переконатися, що вони спілкуються саме з тією людиною, за якого він себе видає.

4) Операційна безпека. В даний час практично у всіх організацій є комп'ютерні мережі з виходом в інтернет. Отже ці мережі потенційно схильні до вторгнення. Зловмисники можуть намагатися впроваджувати черв'яків на хости корпоративної мережі, вивідати секрети організації, трасувати конфігурації внутрішніх мереж і здійснювати DOS-атаки. Для запобігання атак на мережі організацій використовують спеціальні пристрої — брандмауер і системи виявлення вторгнень [14].

1.3 Постановка задачі

Необхідно спроектувати, оновити і реалізувати локально-обчислювальну мережу для банківської установи ПАТ “Акцент-Банк”.

Нові робочі місця ЛОМ повинні бути інтегровані в існуючу мережу і максимально використовувати наявні власні, а не орендовані ресурси.

Локальна обчислювальна мережа повинна включати наступні компоненти:

1) кабельна інформаційна підсистема з пропускною здатністю не менш 1000 Мб/с;

2) активне обладнання (комутатори, маршрутизатори);

3) система безперебійного живлення.

Кабельна інформаційна підсистема повинна будуватися у відповідності з вимогами стандарту ISO.

Загальна кількість автоматизованих робочих місць – 20.

Живлення комутаторів необхідно підключати до ДБЖ.

Вимоги до інтернету:

1) В точках, де встановлений сервер виділений необхідний статичний IP-адрес з відкритими портами. До таких точок рекомендується підключати виділену кабельну лінію (оптоволокно).

2) Для оперативної та ефективної віддаленої підтримки потрібна ширина каналу не нижче 2 Мб/с.

3) Підключення до інтернету потрібне постійне і стабільне на всіх точках.

ЛОМ повинна відповідати вимогам:

1) Продуктивність.

Характеризує час реакції; пропускну здатність; затримку передавання.

Максимальна довжина кабелю від інформаційного порту до комутаційної панелі не повинна перевищувати 20м.

Загальна довжина кабелю для локально-обчислювальної мережі банку не повинна перевищувати 250м, задля досягнення максимальної швидкості передачі даних.

2) Надійність і безпека.

Надійність відповідає за функціонування системи при раптовій відмові деяких елементів.

Шифрування інформації допомагає захистити її конфіденційність, тобто забезпечує неможливість несанкціонованого ознайомлення з нею. Необхідно зашифрувати інформацію.

Підсумкова оцінка ймовірності реалізації загрози обчислюється прямим добутком величини ймовірності кожного фактора.

Безпека — це здатність системи захистити дані від несанкціонованого доступу.

3) Розширюваність і масштабованість.

Розширюваність означає можливість порівняно легкого додання окремих елементів мережі (користувачів, комп'ютерів, додатків, служб), нарощування довжини сегментів мережі й заміни існуючої апаратури більш потужною.

В нас є 20 ЕОМ. Для того, щоб організувати ЛВС з 20 IP-адресами знадобитися маска 255.255.255.224. Але нам належить подальший поділ мережі на підмережі, а це супроводжується втратами IP-адреса при кожному діленні, тому необхідно використовувати більшу маску.

Масштабованість означає, що мережа дозволяє нарощувати кількість вузлів і довжину зв'язків у дуже широких межах, при цьому продуктивність мережі не погіршується.

4) Керованість.

Зумовлює можливість централізовано контролювати стан основних елементів мережі, виявляти й розв'язувати проблеми, що виникають при роботі мережі, виконувати аналіз продуктивності й планувати розвиток мережі [15].

Щоб досягти цього необхідно користуватися ПЗ Windows Server 2008.

Для розробки ЛОМ установи потрібно визначити програмний комплекс, який найбільш підходить для цієї задачі. У розділі другому будуть розглянуті такі програми як LanFlow, Cisco Packet Tracer та NetEmul.

Захист мережі повинен відповідати нормам:

1) Цілісність. Програмісти та фахівці повинні повною мірою забезпечити актуальність і правдивість інформації. Матеріали захищаються від будь-якого руйнування з боку і несанкціонованих змін.

Щоб досягти максимальної цілісності інформації необхідно встановити на ЕОМ операційну систему UNIX/Linux. Вона повинна блискуче справитись з цим завданням.

2) Повна конфіденційність. Проводиться максимальне забезпечення захищеності необхідної інформації, яка може піддаватися несанкціонованому доступу шахраїв.

Для цього у мережі необхідно додати антивірусний захист Kaspersky Open Space Security.

3) Доступність. Захист мереж проводиться в комплексі заходів, які допоможуть забезпечити всі необхідні можливості. Вони допомагають користувачам отримати доступ до збереженої й обробленої інформації.

У ПАТ Акцент-Банк існують банківські захищенні програми “Промінь” та “Робочий стіл працівника (web)”

4) Аутентичність. Відбувається необхідне забезпечення аутентичності суб'єктів і об'єктів, які мають доступ до певної інформації.

Висновки до розділу

У цьому розділі ми зробили аналіз предметної області, розглянули поставлену задачу, теоретичні дані комп’ютерної мережі (модель OSI, топологію мереж, архітектуру локальних мереж) і також проаналізували захист мережі. Після пройденого матеріалу ми отримали загальну інформацію стосовно розглядуваного питання.

У вступі була розглянута актуальність поставленого питання та методи його вирішення.

Ми дізналися що таке модель OSI, які вона має рівні та функції. Розглянули передачу пакетів інформації по рівням OSI. Також розібрали типи ЛОМ.

Була розглянута топологія комп’ютерних мереж, а саме різновиди: шина, кільце, зірка-шина, дерево.

Ознайомились з обладнанням, що використовується в ЛОМ. Провели знайомство з програмним забезпеченням комп'ютерних мереж.

Також були розглянуті топології локальних мереж: IEEE802.3/Ethernet, IEEE802.5/Token-Ring, IEEE802.4/ArcNet, FDDI.

Розділ закінчується інформацією щодо захисту комп’ютерних мереж, також розглянуто варіанти захисту від загроз для мереж.

На підставі всього першого розділу, ми можемо ґрунтувати подальше дослідження диплому.

2 ПРОЕКТУВАННЯ ЛОМ БАНКІВСЬКОЇ УСТАНОВИ

Проектування локальної мережі є важливим етапом, на якому визначається структура ЛОМ виходячи з числа комп'ютерів (іншого мережевого обладнання), призначення мережі, типу даних, що передаються, в межах одного або декількох рівнів мережі, з наступним вибором засобів фізичної реалізації ЛОМ:

1) обладнання;
2) тип кабелю;
3) програмне забезпечення.

Щоб спроектувати мережу банківської установи потрібен програмний комплекс, який буде відповідати всім вимогам для побудови та перевірки.

Тому запропоновано розглянути детальніше такі програмні комплекси як:

1) LanFlow;
2) Cisco Packet Tracer;
3) NetEmul.

Розібратися в зручності, надійності, повності потрібних ресурсів програм та обрати ту, яка найбільш підходить для проектування.

2.1 Розгляд програмних комплексів LanFlow, Cisco Packet Tracer та NetEmul.

Розглянемо програми для проектування мереж.

Для створення проекту необхідно обрати програмний комплекс, який буде відповідати усім вимогам і нормам. Також програма повинна вміщати в собі всі потрібні інструменти. Пропонується розглянути найкращі програмні комплекси, які включають в себе функції для проектування мереж:

1) LanFlow (рис. 2.1);

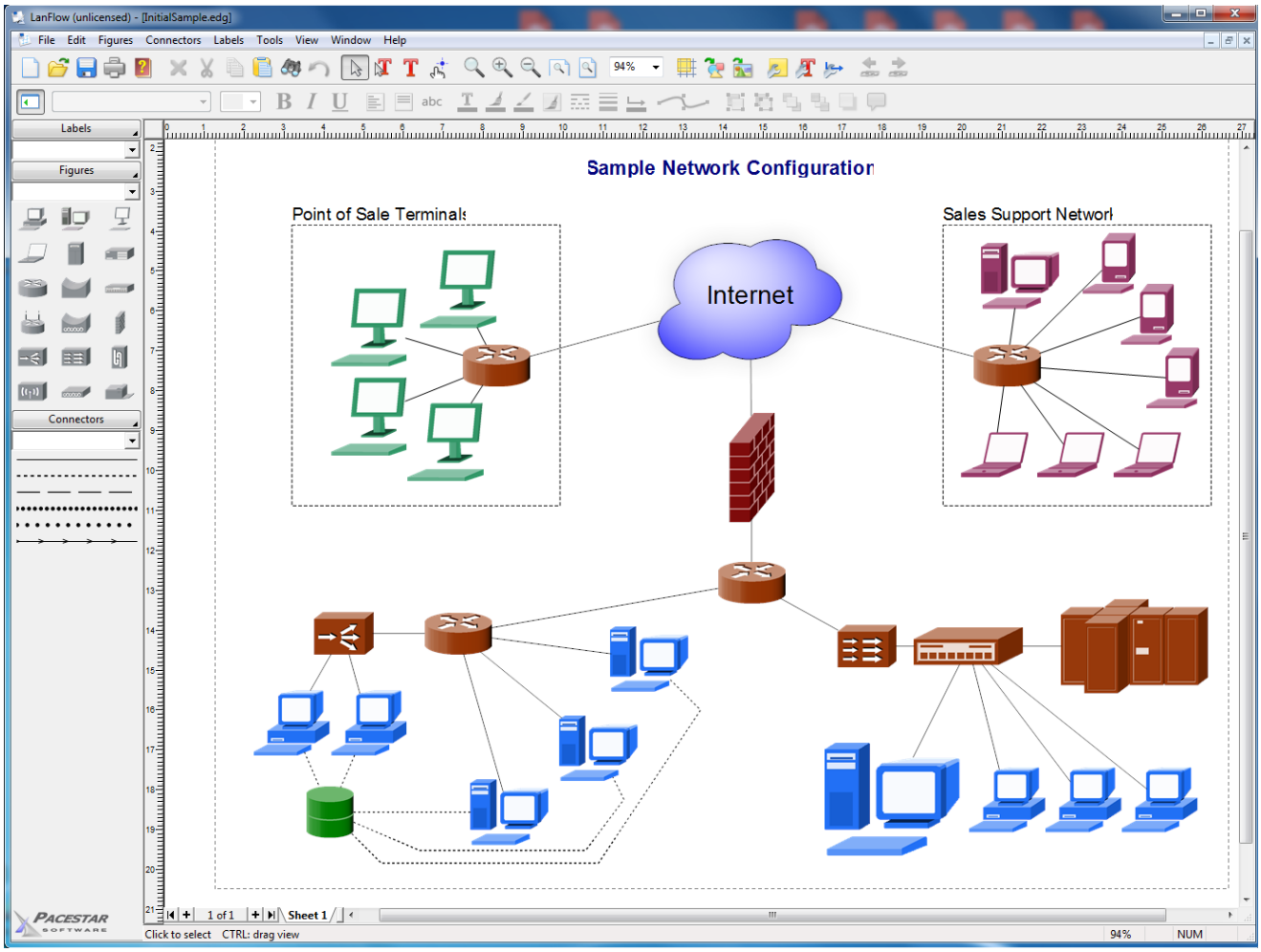

Рисунок 2.1 — Програма LanFlow

LanFlow програма для проектування і документування мереж.

Переваги системи LanFlow:

1) створення схем локальної мережі;
2) подання мережевого обладнання у вигляді 2D і 3D символів;
3) додавання кліпарта для специфіки мережі.

З недоліків можна виділити:

1) для роботи з програмою необхідні спеціалізовані знання;
2) закрита база компонентів.

2) **Cisco Packet Tracer** (рис. 2.2);

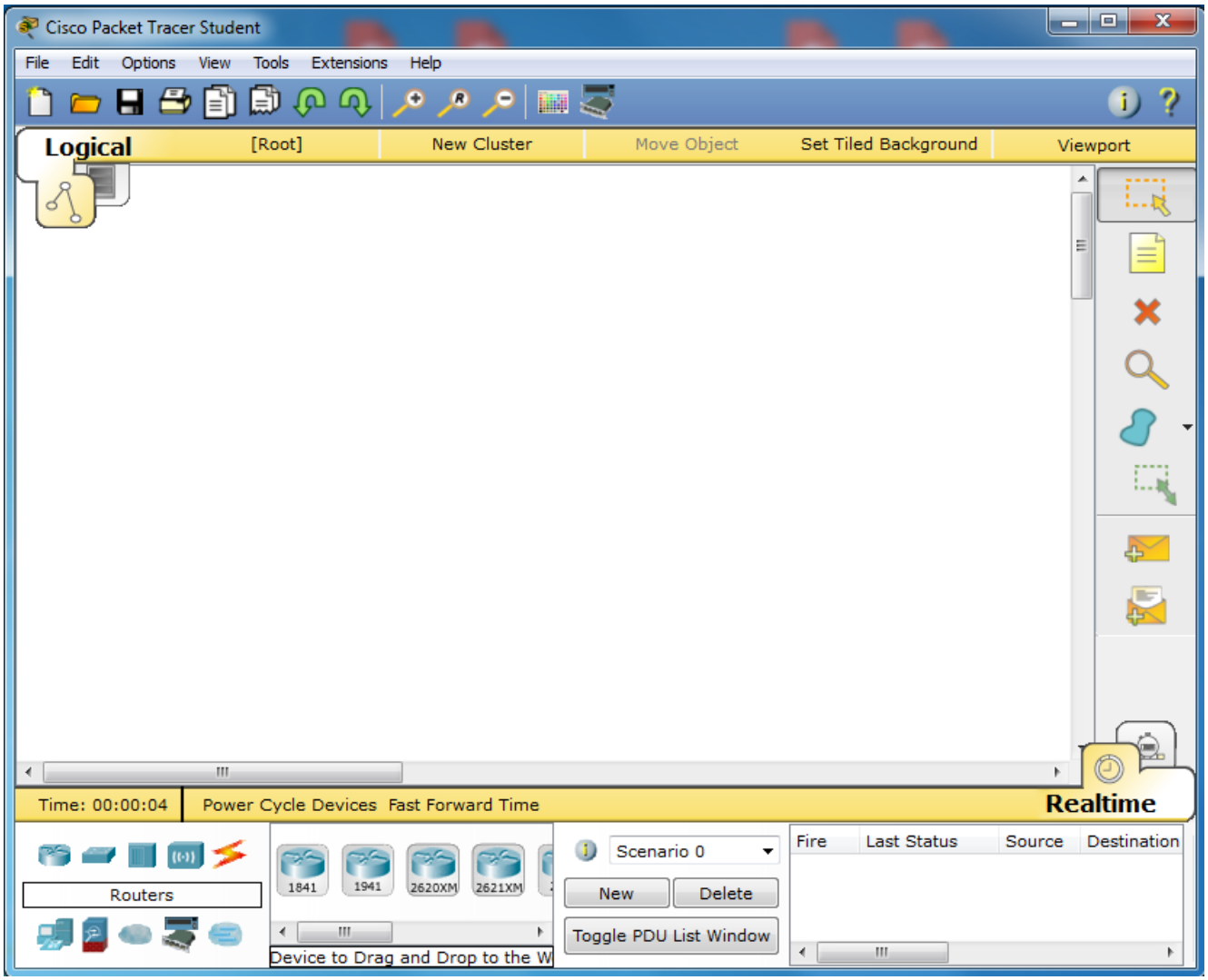

Рисунок 2.2 — Програма Cisco Packet Tracer

Історія створення засобу моделювання комп'ютерних мереж Cisco Packet Tracer відноситься до вересня 2000 року. Саме в цьому році американська транснаціональна компанія в області високих технологій Cisco Systems, що розробляє і продає мережеве обладнання, призначене для великих організацій та підприємств в сфері телекомунікацій, створює програму Cisco Packet Tracer і рекомендує її використовувати при вивченні телекомунікаційних мереж і мережевого обладнання, а також для проведення уроків з лабораторних робіт у вищих навчальних закладах, так як дана програма дозволяє наочно відображати роботу мережі, що підвищує засвоєння матеріалу учнями.

До можливостей Cisco Packet Tracer можна віднести дружелюбність,

зрозумілість і логічність графічного інтерфейсу, який сприяє кращому розумінню організації комп'ютерної мережі та принципів роботи пристроїв. Одним з найбільш цікавих переваг є можливість працювати в режимі реального часу і можливість переходити в режим симулятора (Simulation), а також бачити переміщення пакетів від пристрою до пристрою з уповільненням часу. Крім цього, Cisco Packet Tracer підтримує дві моделі побудови мереж: логічну і фізичну. Логічну схему мережі можна накласти на креслення реально існуючого будівлі або навіть міста. Крім цього багатомовність інтерфейсу програми дозволяє вивчати програму одразу на двох мовах, російською та англійською. Наявність функції Activity Wizard дозволяє мережевим інженерам створювати шаблони мереж, зберігати і використовувати в подальшій роботі.

До недоліків Cisco Packet Tracer можна віднести відсутність вбудованого в Cisco Packet Tracer функціоналу Embedded Event Manager (Вбудований менеджер подій), який дозволяє створювати сценарії для автоматизації роботи пристроїв. Так само в програмі іноді можуть виявлятися різноманітні збої, від яких можна позбутися тільки з допомогою перезапуску програми [16].

3) NetEmul (рис. 2.3).

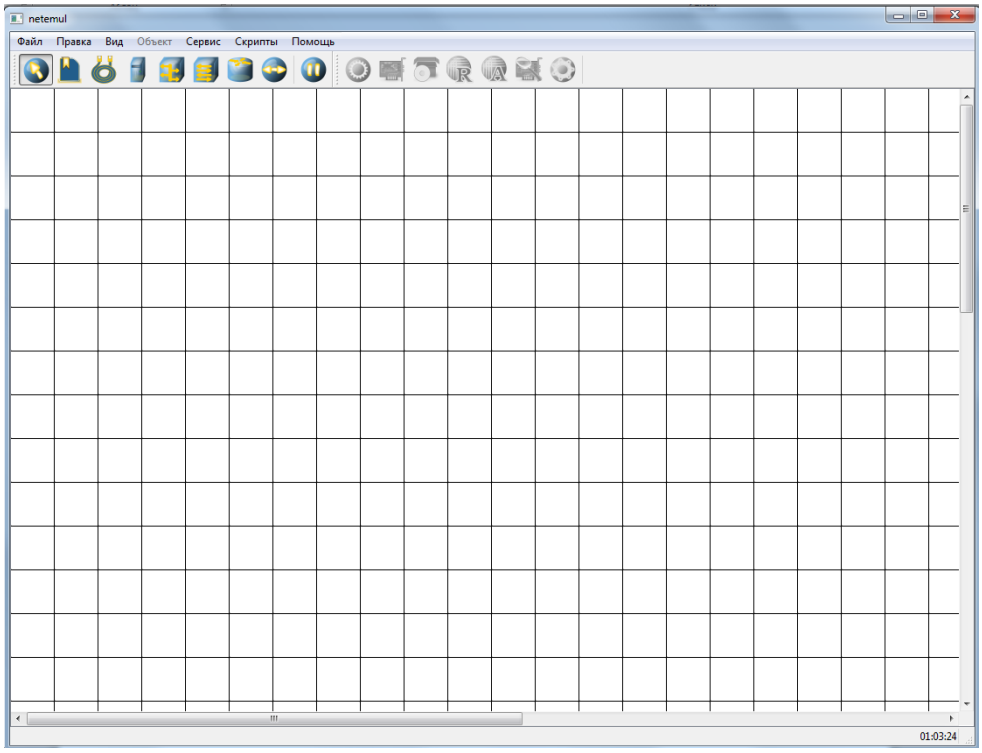

Рисунок 2.3 — Програма NetEmul

NetEmul – це безкоштовна програма емуляції комп'ютерних мереж, що дозволяє будувати і налаштовувати обчислювальні мережі. Крім того, NetEmul дає можливість наочно побачити, що відбуваються в мережі процеси, пов'язані з передачею службової інформації.

NetEmul вільно поширюється по ліцензії GPL. Також слід зазначити, що даний продукт є кросплатформним і вільно може бути використаний в операційних системах: Windows 95/98/2000 / XP, Linux, MacOS.

При розробці програми розробники щосили прагнули наблизити роботу програми до моделі роботи реальної мережі, намагаючись відобразити у програмі реальні настройки, чинники та випадковості, які відбуваються в мережі.

2.2 План розташування компонентів мережі в банківській установі

Локально-обчислювальна мережа банківської установи має 20 активних комп’ютерів (PC), з яких 15 використовуються для користування персоналу, а останні 5 в якості серверів. Також ЛОМ має 4 комутатора(switch) і один маршрутизатор(router). Було вирішено розробити мережу з топологією дерево (шина - зірка) і прокласти оптоволоконний кабель для більш швидкої передачі інформації в мережі (рис. 2.4).

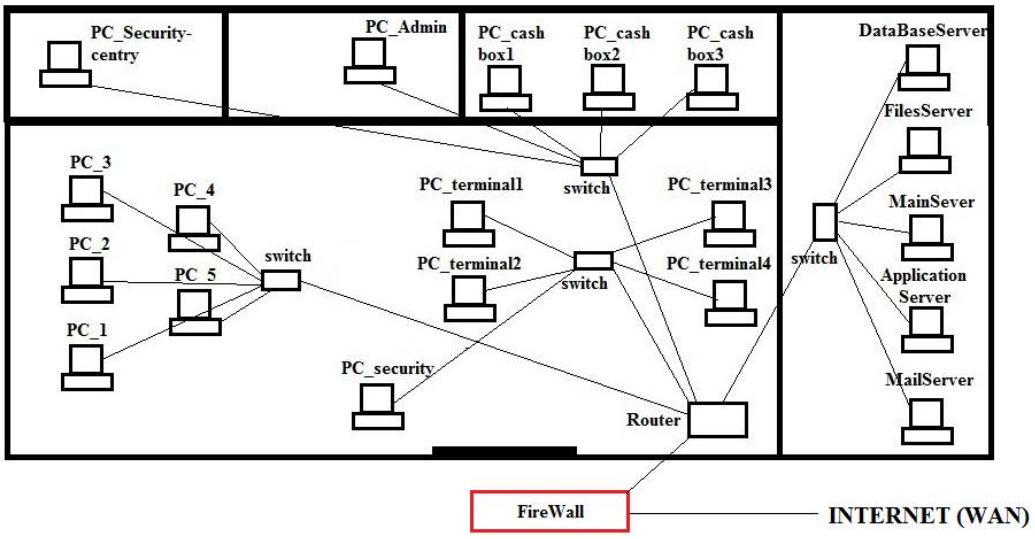

Рисунок 2.4 — Схема ЛОМ банківської установи

2.3 Захист ЛОМ установи банку

Щоб захистити ЛОМ банку необхідно дотримуватися до наступних вимог:

1) При побудові безпечної LAN слід мінімізувати кількість служб і сервісів, що надаються мережею, що використовуються клієнтами з мережі Інтернет.

2) Шифрування інформації. Шифрування інформації допомагає захистити її конфіденційність, тобто забезпечує неможливість несанкціонованого ознайомлення з нею. Шифрування — це процес перетворення відкритої інформації в закриту, зашифровану (що називається «зашифрування») і навпаки («розшифрування»). Це перетворення виконується за строгим математичним алгоритмом:

$$C = Ek_1(M) \text{— зашифрування,} \quad (2.1)$$

$$M' = Dk_2(C) \text{— розшифрування.} \quad (2.2)$$

Функція E виконує зашифрування інформації, функція D – розшифрування. У тому випадку, якщо ключ k_2 відповідає ключу k_1, застосованому при зашифровании, вдається отримати відкриту інформацію, тобто отримати відповідність $M' = M$.

При відсутності ж правильного ключа k_2 отримати вихідне повідомлення практично неможливо.

По виду відповідності ключів k_1 й k_2 алгоритми шифрування поділяються на дві категорії:

1) Симетричне шифрування: $k_1 = k_2$.

2) Асиметричне шифрування. Ключ k_1 - в даному випадку називається «відкритим», а ключ k_2 — «секретним».

Крім власне даних у перетворенні також бере участь додатковий елемент — «ключ». Ключ являє собою унікальний елемент, що дозволяє шифрувати інформацію так, що отримати відкриту інформацію з зашифрованої можна тільки певному користувачу або групі користувачів.

3) DMZ — скорочення від demilitarized zone (демілітаризована зона) — являє собою фрагмент мережі, не є повністю надійним. Сенс створення DMZ полягає в тому, щоб відгородити внутрішню систему (в даному випадку це наша захищена LAN) від доступу, який здійснюється з Інтернету. DMZ створюється за допомогою реалізації напівзахищеної мережевої зони, що досягається шляхом застосування міжмережевих екранів або маршрутизаторів зі строгими фільтрами. Потім за допомогою елементів керування мережею визначається політика, якому трафіку дозволяється проникнення в DMZ, а якому трафіку дозволено виходити за межі DMZ. Очевидно, що всі системи, доступні з зовнішнього середовища, повинні бути розміщені в демілітаризованій зоні.

4) IDS — система виявлення вторгнень. В ідеальному випадку така система лише видасть сигнал тривоги при спробі проникнення. Виявлення вторгнень допомагає при ідентифікації активних загроз за допомогою повідомлень і попереджень про те, що зловмисник здійснює збір інформації, необхідної для проведення атаки.

5) Ще одним інструментом, який ми застосуємо при проектуванні безпечної LAN, стане NAT.

NAT — це технологія трансляції однієї чи кількох адрес в інші адреси. У більшості випадків функції NAT реалізуються за допомогою міжмережевого екрану. Маршрутизатори також можуть виконувати цю функцію. Очевидно, що функція безпеки NAT реалізується завдяки тому, що приховані адреси внутрішніх систем є невидимими із зовнішньої мережі, зокрема мережі Інтернет.

6) Установка останніх оновлень строго обов'язкова.

7) На сервері, як і на робочих станціях має бути встановлене антивірусне ПЗ зі свіжими базами.

8) Файлову систему FAT32 необхідно замінити на NTFS. NTFS більш безпечна: вона дозволяє розмежувати доступ до ресурсів вашого ПК і значно ускладнить процес локального та мережного злому паролів.

9) Всі невживані сервіси бажано вимкнути. Це не тільки поліпшить продуктивність системи, але і автоматично закриє купу відкритих портів

Висновки до розділу

У цьому розділі були розглянуті 3 програми, за допомогою яких можна розробити схему ЛОМ для банківської установи. Було вирішено обрати програму NetEmul, тому що вона є найбільш легкою у ознайомленні, також вона кросплатформна. Програма дуже реалістична у проектуванні та має багатий спектр засобів для розробок мережевих систем.

Також була запропонована оновлена схема ЛОМ банківської установи ПАТ “Акцент-Банк. У ній покращені умови для передачі даних, завдяки зміні топології мережі. В ЛОМ був застосований оптоволоконний кабель, який дає кращі результати стосовно швидкості передачі даних ніж старі кабелі. Завдяки добавлення серверів, швидкість обробки даних значно зросте.

Немаловажним є захист ЛОМ. Були розглянуті важливі функції захисту мережі. Детальніше було розглянути шифрування даних, тому що це дуже важливо для банківських мереж.

Після цього розділу можна приступати до розробки самої ЛОМ у програмному комплексі NetEmul.

3 РОЗРОБКА ЛОМ УСТАНОВИ БАНКУ

3.1 Реалізація ЛОМ

Локальна обчислювальна мережа повинна об'єднати персональні комп'ютери користувачів між собою і забезпечити доступ до ресурсів, розміщених на серверах (рис. 3.1).

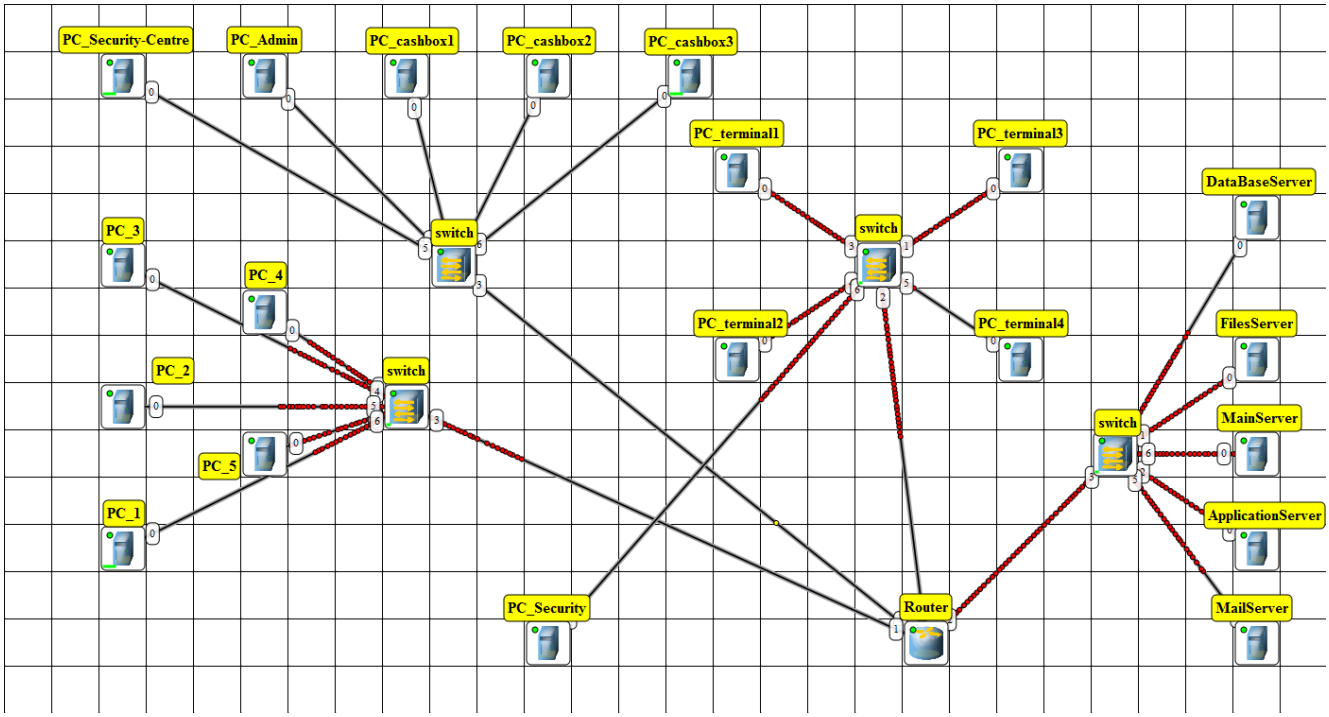

Рисунок 3.1 — схема ЛОМ Акцент-Банку в програмі NetEmul

3.2 Розрахунок загальної довжини кабелю

$$L = \left(\sum_{i}^{n} l_{k1i} + \sum_{i}^{n} l_{k2i} + \sum_{i}^{n} l_{k3i} + \sum_{i}^{n} l_{k4i} + L_{k1} + L_{k2} + L_{k3} + L_{k4} \right) \cdot 1{,}1 \qquad (3.1)$$

l_{k1i} — відстань від і-го робочого місця до комутатора №1;

l_{k2i} — відстань від і-го робочого місця до комутатора №2;

l_{k3i} — відстань від і-го робочого місця до комутатора №3;

l_{k4i} — відстань від і-го робочого місця до комутатора №4;

L_{k1} — відстань від комутатора №1 до маршрутизатора;

L_{k2} — відстань від комутатора №2 до маршрутизатора;

L_{k3} — відстань від комутатора №3 до маршрутизатора;

L_{k4} — відстань від комутатора №4 до маршрутизатора.

Таблиця 3.1 — Відстань до комутатора №1

Номер ЕОМ	**Відстань до комутатора №1, м**
1	10
2	8,2
3	5
4	4,7
5	9,5

Таблиця 3.2 — Відстань до комутатора №2

Номер ЕОМ	**Відстань до комутатора №2, м**
6	3
7	2
8	3
9	5,5
10	15,5

Таблиця 3.3 — Відстань до комутатора №3

Номер ЕОМ	**Відстань до комутатора №3, м**
11	4,5
12	4,7
13	4,9
14	4,4
15	12,6

Таблиця 3.4 — Відстань до комутатора №4

Номер ЕОМ	**Відстань до комутатора №4, м**
16	3
17	3,3
18	6,6
19	7,4
20	8

Таблиця 3.5 — Відстань до маршрутизатора

Номер комутатора	Відстань до маршрутизатора, м
1	10
2	12
3	6,6
4	14,9

Загальна довжина кабелю — $L = 169{,}3 \cdot 1{,}1 = 186{,}2 м.$

3.3 Розподіл IP-адрес для спроектованої мережі

Планування мережі

Планування мережі - це процес присвоєння IP-адреса комп'ютерам.

Виберемо IP-адресу: 205.98.42.55

Необхідно створити 4 підмережі.

Для початку необхідно перевести наявний IP-адреса у двійковий вигляд:

11001101.01100010.00101010.00110111

Тепер необхідно вибрати маску підмережі таким чином, щоб за допомогою її можна було отримати необхідну кількість IP-адрес. В нас є 20 ЕОМ. Найбільш близьке до 20 число, що дорівнює ступеню двійки - це $32 = 2^5$. Отже для того, щоб організувати ЛВС з 32 IP-адресами знадобитися маска 255.255.255.224. Але нам належить подальший поділ мережі на підмережі, а це супроводжується втратами IP-адрес при кожному діленні, тому необхідно використовувати маску, яка надасть більшу кількість IP-адрес. Такою є маска 255.255.255.192.

Переведемо маску у двійковий вигляд:

11111111.11111111.11111111.11000000.

Побітно помноживши IP-адресу і маску отримаємо адресу мережі:

11001101.01100010.00101010.00110111
*
11111111.11111111.11111111.11000000
11001101.01100010.00101010.00000000

Тобто в десятковій формі адреса мережі: 205.26.42.0.

Маска мережі, що використовується, дає 2^6 = 64 IP-адреса, то отримаємо наступний простір IP-адрес в мережі: 205.26.42.0 - 205.26.42.63.

При цьому слід враховувати, що адреса 205.26.42.0 — базовий адрес мережі (не використовується при адресації хостів, вказує тільки на мережу, тобто адресу мережі), а 205.26.42.63 — адрес бродкаста (не використовується при адресації хостів).

Тепер слід розбити наявну мережу на дві підмережі по 32 хоста.

Для цього застосуємо маску 255.255.255.224.

Отримаємо підмережі:

1-ша підмережа: 205.26.42.0 (масив IP-адрес 205.26.42.0 - 205.26.42.31; 205.26.42.0 — базовий адрес підмережі, 205.26.42.31 — адрес бродкаста в підмережі);

2-га підмережа 205.26.42.32 (масив IP-адрес 205.26.42.32 - 205.26.42.63; 205.26.42.32 — базовий адрес підмережі, 205.26.42.63 — адрес бродкаста в підмережі);

Отримані мережі розіб'ємо ще на дві підмережі:

Використовуємо маскою 255.255.255.240.

Отримаємо підмережі:

Підмережа 1.1: 205.26.42.0 (205.26.42.0 - 205.26.42.15);

Підмережа 1.2: 205.26.42.16 (205.26.42.16 - 205.26.42.31);

Підмережа 2.1: 205.26.42.32 (205.26.42.32 - 205.26.42.47);

Підмережа 2.2: 205.26.42.48 (205.26.42.48 - 205.26.42.63);

Необхідно пам'ятати, що в кожній підмережі перший IP-адрес — це базовий адресу підмережі, а останній — адреса бродкаста. Їх не можна привласнювати хостам. У підсумку, у кожній підмережі є по чотирнадцять IP-адрес, тобто всім

хостам вистачить IP-адрес, а решту можуть бути використані при подальшому розширенні мережі або для різних мережевих пристроїв.

3.4 Операційна система та прикладне ПЗ

Галузь діяльності підприємства — банківська справа. Тому необхідна така операційна система та прикладне програмне забезпечення:

1) операційна система робочих станцій: UNIX/Linux;
2) програмне забезпечення: Windows Server 2008;
3) антивірусний захист: Kaspersky Open Space Security;
4) офісний пакет програм для роботи з текстами, електронними таблицями, базами даних та ін.: LibreOffice;
5) Програма: “Промінь” та “Робочий стіл працівника (web)”

3.5 Реалізація інформаційної безпеки мережі

Загроза безпеці інформації – виникнення такого явища або події, наслідком якого можуть бути негативні впливи на інформацію: порушення фізичної цілісності, логічної структури, несанкціонована модифікація, несанкціоноване отримання, несанкціоноване розмноження.

Уразливість являє собою поєднання обставин, що дозволяє реалізувати загрозу.

Імовірність реалізації загрози обчислюється, виходячи з трьох параметрів – прямих факторів:

p_s – просторовий фактор, тобто ймовірність того, що уразливість реалізується в тому місці, де знаходиться інформація;

p_t – часовий фактор, тобто ймовірність того, що уразливість реалізується в той момент, коли інформація існує;

p_p – енергетичний фактор, ймовірність того, що енергії, для виконання уразливості буде достатньо.

Підсумкова оцінка ймовірності реалізації загрози обчислюється прямим добутком величини ймовірності кожного фактора, тобто

$$P = p_s \cdot p_t \cdot p_p \quad (3.1)$$

Таким чином, при невиконанні хоча б одного з прямих факторів, вразливість можна вважати усуненою.

Таблиця 3.6 — Загрози інформаційним ресурсам

№	Інформаційні ресурси	Виявлена загроза інформаційної безпеки	Оцінка ризику	Підсумкова оцінка, P
1	Паперові документи і знімні носії інформації	Крадіжка	$p_s = 1$ $p_t = 0,375$ $p_p = 1$	P = 0,375
		Втрата інформації	$p_s = 1$ $p_t = 1$ $p_p = 1$	P = 1
		Несанкціоноване копіювання	$p_s = 1$ $p_t = 0,4$ $p_p = 1$	P = 0,4
2	Всі інформаційні ресурси	Недостатня ефективність пожежних сповіщувачів	$p_s = 1$ $p_t = 0,5$ $p_p = 0,5$	P = 0,25
		Недбалість або злочинні дії співробітників	$p_s = 1$ $p_t = 0,375$ $p_p = 1$	P = 0,375
3	Автоматизоване робоче місце співробітників	Помилки в налаштуваннях	$p_s = 1$ $p_t = 1$ $p_p = 1$	P = 1
		Помилки користувачів	$p_s = 1$ $p_t = 1$ $p_p = 1$	P = 1
		Прослуховування внутрішнього трафіку	$p_s = 1$ $p_t = 1$ $p_p = 0,1$	P = 0,1
		Помилки в мережевих налаштуваннях	$p_s = 1$ $p_t = 1$ $p_p = 1$	P = 1
		Збої, поломки апаратури	$p_s = 1$ $p_t = 1$ $p_p = 0,3$	P = 0,3
		Вплив вірусів	$p_s = 1$ $p_t = 1$ $p_p = 1$	P = 1

Продовження таблиці 3.6

№	Інформаційні ресурси	Виявлена загроза інформаційної безпеки	Оцінка ризику	Підсумкова оцінка, Р
4	ЛОМ	Загроза доступності. Помилки в топології мережі	$p_s = 1$ $p_t = 1$ $p_p = 1$	Р = 1

В таблиці 3.6 інформаційні ресурси розбиті за групами, для кожної з яких виявлені загрози та вразливості. Загроза пожежі характерна для всіх інформаційних ресурсів.

Погрози крадіжки та несанкціонованого копіювання реалізуються при виконанні тимчасового фактора, який розраховується виходячи з тривалості робочого дня, що становить 9 годин: $P_t = 9 \div 24 = 0{,}375.$

Найвищою ймовірністю здійснення володіють загрози, вразливості яких обумовлені помилками або навмисними діями співробітників.

Ймовірність порушення роботи серверів і АРМ через недосконаліть техніки залежить від виконання енергетичного фактора та визначається на основі статистичних даних.

Вкрай висока ймовірність впливу шкідливого ПЗ, однак, наявність засобів антивірусного захисту знижує ймовірність появи цієї загрози.

У таблиці 3.7 представлені можливі методи запобігання виявлених загроз, на підставі яких розробляються організаційно-технічні заходи по захисту інформації.

Таблиця 3.7 — Методи запобігання загроз

№	Вразливість	Метод запобігання	Показник, який знижується (p_s , p_t , p_p)
1	Недбаліть або злочинні дії співробітників	Навчання персоналу та контроль	p_p
2	Недостатня ефективність пожежних сповіщувачів	Модернізація існуючої системи пожежної сигналізації	p_t , p_p
3	Прослуховування внутрішнього трафіку	Організація своєчасного оновлення, аналіз існуючих вразливостей і своєчасне їх перекриття, організація резервного копіювання даних	p_p

Продовження таблиці 3.7

№	Вразливість	Метод запобігання	Показник, який знижується (p_s , p_t , p_p)
4	Помилки в мережевих налаштуваннях	Навчання персоналу та контроль	p_p
5	Помилки користувачів	Навчання персоналу та контроль, розробка нормативно-методичної літератури, організація резервного копіювання даних	p_p
6	Збої, поломки апаратури	Проведення профілактичних перевірок стану обладнання та своєчасний ремонт, організація резервного копіювання даних	p_p
7	Вплив вірусів	Навчання персоналу та контроль, проведення профілактичних робіт	p_p
8	Загроза доступності. Помилки в топології мережі	Зміна топології мережі	p_p

З урахуванням запропонованих заходів здійснюється підбір технічних і програмно-апаратних засобів, а також розробляються нормативні документи, що регламентують порядок захисту інформації на об'єкті.

Висновки до розділу

У цьому розділі був реалізований проект ЛОМ банківської установи ПАТ “Акцент-Банк”. За допомогою програми NetEmul була створена діюча схема мережі зі всіма складовими. Вона була перевірена у програмі на наявність помилок.

Також була визначена загальна довжина кабелю для спроектованої ЛОМ — $L = 169{,}3 \cdot 1{,}1 = 186{,}2 м.$

Щоб запустити мережу — розрахували підмережі і задали ЕОМ IP-адреси та маски підмереж.

Визначити яке програмне забезпечення використовується на ЕОМ ЛОМ, які програми та антивіруси має мережа.

Розглянуті загрози інформаційним ресурсам та методи запобігання цих загроз.

4 ОХОРОНА ПРАЦІ У БАНКІВСЬКІЙ УСТАНОВІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

В даному розділі проведено аналіз потенційних небезпечних та шкідливих виробничих факторів, причин пожеж. На підставі аналізу розроблені заходи з техніки безпеки та рекомендації з пожежної профілактики. Завданням даної роботи бакалавра було розробити локально-обчислювальну мережу для банківської установи, і як результат була створена необхідна ЛОМ. За цим проектом в подальшому розроблятиметься реальна система, яка значно полегшить процес обміну інформації у мережі банку. Так як в процесі проектування використовувались електронні пристрої, то аналіз потенційно небезпечних і шкідливих виробничих чинників виконується для персонального комп'ютера на якому буде розроблятися потрібна ЛОМ.

4.1 Загальні питання з охорони праці

При роботі з обчислювальною технікою змінюються фізичні і хімічні фактори навколишнього середовища: виникає статична електрика, електромагнітне випромінювання, змінюється температура і вологість, рівень вміст кисню і озону в повітрі. Повітря забруднюється шкідливими хімічними речовинами антропогенного походження. Неправильна організація робочого місця сприяє загальному і локальній напрузі м'язів шиї, тулуба, верхніх кінцівок, викривлення хребта і розвитку остеохондрозу.

4.1.1 Правові та організаційні основи охорони праці

Основним організаційним напрямом у здійсненні управління в сфері охорони праці є усвідомлення пріоритету безпеки праці і підвищення соціальної відповідальності держави, і особистої відповідальності працівників.

Обов’язки працівників щодо додержання вимог нормативно-правових актів з охорони праці (ст. 14), відповідальність робітників всіх категорій за порушення

вимог щодо охорони праці (ст. 44) та структура організації/виробництв системи управління охорони праці визначені безпосередньо “Інструкцією на робоче місце № 12”, та іншими затвердженими власними нормативними актами з питань охорони праці (правилами, нормами, регламентами, положеннями, стандартами, інструкціями та іншими документами, обов’язковими до виконання), тобто тих, що діють на підприємстві/організації, і визначені у [18].

4.1.2 Організаційно-технічні заходи з безпеки праці

В організації проводиться навчання і перевірка знань з питань охорони праці відповідно до вимог Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці, затвердженого наказом Держнаглядохоронпраці України від 26.01.2005 N 15, зареєстрованого в Міністерстві юстиції України 15.02.2005 за N 231/10511 [19].

4.2 Аналіз стану умов праці

Робота над створенням локально-обчислювальної мережі системи проходитиме в банківській установі Акцент – банку. Для даної роботи достатньо однієї людини, для якої надано робоче місце зі стаціонарним комп’ютером.

4.2.1 Вимоги до приміщень

Геометричні розміри приміщення зазначені в таблиці 4.1

Таблиця 4.1 — Розміри приміщення

Найменування	Значення
Довжина, м	15
Ширина, м	15
Висота, м	5
Площа, $м^2$	225
Об’єм, $м^3$	1125

Згідно з [22] розмір площі для одного робочого місця оператора персонального комп’ютера має бути не менше 6 кв. м, а об’єм — не менше 20 куб. м. Отже, дане приміщення цілком відповідає зазначеним нормам.

Задля дотримання визначеного рівня мікроклімату в будівлі встановлено систему опалення та кондиціювання.

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

4.2.2 Вимоги до організації місця праці

При порівнянні відповідності характеристик робочого місця нормативним основні вимоги до організації робочого місця за [23] (табл. 4.2) і відповідними фактичними значеннями для робочого місця, констатуємо повну відповідність.

Таблиця 4.2 — Характеристики робочого місця

Найменування параметра	**Фактичне значення**	**Нормативне значення**
Висота робочої поверхні, мм	750	680 - 800
Висота простору для ніг, мм	730	не менше 600
Ширина простору для ніг, мм	660	не менше 500
Глибина простору для ніг, мм	700	не менше 650
Висота поверхні сидіння, мм	470	400 - 500
Ширина сидіння, мм	400	не менше 400
Глибина сидіння, мм	400	не менше 400
Висота поверхні спинки, мм	600	не менше 300
Ширина опорної поверхні спинки, мм	500	не менше 380
Радіус кривини спинки в горизонтальній площині, мм	400	400
Відстань від очей до екрану дисплея, мм	800	700 - 800

Робочий стіл на досліджуваному місці також містить достатньо простору для ніг. Крісло, що використовується в якості робочого сидіння, є підйомно-поворотним, має підлокітники і можливість регулювання за висотою і кутом нахилу спинки, також воно м'яке і виконане з екологічної шкіри, що дає можливість працювати у комфорті. Екран монітору знаходиться на відстані 0.8 м,

клавіатура має можливість регулювання кута нахилу 5-15°. Отже, за всіма параметрами робоче місце відповідає нормативним вимогам. Приміщення складається з одноповерхової будівлі і має об'єм 1125м^3, площу – 225м^2 . У цьому приміщенні обладнано п'ятнадцять місць праці і всі укомплектовані ПК.

Розміщення вікон забезпечує природне освітлення з коефіцієнтом природного освітлення не менше 1,5%, а загальне штучне освітлення, яке здійснюється за допомогою восьми люмінесцентних ламп, забезпечує рівень освітленості не менше 200 Лк.

У приміщенні є електрична мережа з напругою 220 В, яка створює небезпеку ураження електричним струмом. ПК та периферійні пристрої можуть бути джерелами електромагнітних випромінювань, аерозолів та шкідливих речовин.

4.2.3 Навантаження та напруженість процесу праці

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

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

4.3 Виробнича санітарія

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

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

4.3.1 Аналіз небезпечних та шкідливих факторів при виробництві виробу

Аналіз небезпечних та шкідливих виробничих факторів виконується у табличній формі (табл. 4.3). Роботу, пов'язану з ЕОП з ВДТ, у тому числі на тих, які мають робочі місця, обладнані ЕОМ з ВДТ і ПП, виконують із забезпеченням виконання [24] «Правил охорони праці під час експлуатації електронно-обчислювальних машин», які встановлюють вимоги безпеки до обладнання робочих місць, до роботи із застосуванням ЕОМ з ВДТ і ПП.

Таблиця 4.3 — Аналіз небезпечних і шкідливих виробничих факторів

Небезпечні і шкідливі виробничі фактори	**Джерела факторів (види робіт)**	**Кількісна оцінка**	**Нормативні документи**
1	2	3	4
фізичні:			
підвищена температура поверхонь обладнання	експлуатація ЕОМ, принтерів, сканерів чи/або серверного обладнання для роботи	2	[22]
підвищений рівень шуму на робочому місці	—	2	[25]
підвищений рівень електромагнітного випромінювання	—	2	[27]
підвищений рівень напруги електричної мережі	—	4	[28] [29]
підвищений рівень вібрації	—	1	[26]
підвищена або знижена вологість повітря	—	2	[22]
підвищена або знижена рухливість повітря	—	1	[22]
недостатність природного світла	порушення умов праці (вимог до приміщень)	2	[30]
недостатнє освітлення робочої зони	порушення гігієнічних параметрів виробничого середовища	3	[30]
підвищена яскравість світла	порушення умов праці (організації місця праці - налагодження моніторів)	1	[23]

Продовження таблиці 4.3

Небезпечні і шкідливі виробничі фактори	**Джерела факторів (види робіт)**	**Кількісна оцінка**	**Нормативні документи**
хімічні:			
загазованість повітря робочої зони, яка впливає на організм людини через органи дихання та надає токсичну і канцерогенну дію	від експлуатації сканерів, принтерів для роботи – O^3, оплавлення електричних і комутаційних кабелів, резисторів, конденсаторів, напівпровідникових діодів, транзисторів й інше в ЕОМ та системах кондиціювання повітря - CO, CO^2, SO^2, P^2O^5, H^2S, HCl, H, NH^3, ClF^3, F^2O^2, F^2O^3, SeO^2. SeF^6, TeF^6, $COCl^2$, SO^2F^2, інш.	3	[31] [32] [33] [34]
психофізіологічні:			
фізичні (статичне – сидіння)	порушення умов праці	2	[24] [23]

Робочі місця мають відповідати вимогам Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин, затверджених постановою Головного державного санітарного лікаря України від 10.12.98 N 7 [23]. За умов роботи з ПК виникають наступні небезпечні та шкідливі чинники: несприятливі мікрокліматичні умови, освітлення, електромагнітні випромінювання, забруднення повітря шкідливими речовинами, шум, вібрація, електричний струм, електростатичне поле, напруженість трудового процесу та інше.

4.3.2 Пожежна безпека

Небезпека розвитку пожежі на обчислювальному центрі обумовлюється застосуванням розгалужених систем електроживлення ЕОМ, вентиляції і кондиціювання. Небезпека загоряння пов'язана з особливістю комп'ютерів - із значною кількістю щільно розташованих на монтажній платі і блоках електронних вузлів і схем, електричних і комутаційних кабелів, резисторів, конденсаторів, напівпровідникових діодів і транзисторів. При відхиленні реальних умов експлуатації від розрахункових можуть виникнути пожежонебезпечні ситуації.

Кабельні лінії є найбільш пожежонебезпечним місцем. Наявність пального ізоляційного матеріалу, ймовірних джерел запалювання у вигляді електричних іскор і дуг, розгалуженість і недоступність роблять кабельні лінії місцем найбільш ймовірного виникнення і розвитку пожежі. Для зниження займистості і здатності поширювати полум'я кабелі покривають вогнезахисними покриттями. Проектом передбачено прокладати проводку: приховано, під знімною підлогою розділяючи негорючими діафрагмами, в малодоступних місцях.

Для гасіння пожеж в офісному приміщенні пропонується використовувати порошкові або вуглекислотні вогнегасники, так як вони є універсальними. Дане приміщення оснащене системою автоматичної пожежної сигналізації.

4.3.3 Електробезпека

На робочому місці виконуються наступні вимоги електробезпеки: ПК, периферійні пристрої та устаткування для обслуговування, електропроводи і кабелі за виконанням та ступенем захисту відповідають класу зони за ПУЕ (правила улаштування електроустановок), мають апаратуру захисту від струму короткого замикання та інших аварійних режимів. Лінія електромережі для живлення ПК, периферійних пристроїв і устаткування для обслуговування, виконана як окрема групова три-провідна мережа, шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів.

4.4 Гігієнічні вимоги до параметрів виробничого середовища

4.4.1 Мікроклімат

Мікроклімат робочих приміщень – це клімат внутрішнього середовища цих приміщень, що визначається діючої на організм людини з'єднанням температури, вологості, швидкості переміщення повітря. Отже оптимальні значення для

температури, відносної вологості й рухливості повітря для зазначеного робочого місця відповідають [22] і наведені в табл. 4.4:

Таблиця 4.4 — Норми мікроклімату робочої зони об’єкту

Період року	**Категорія робіт**	**Температура C^0**	**Відносна вологість %**	**Швидкість руху повітря, м/с**
Холодна	легка-1 а	22 - 24	40 – 60	0,1
Тепла	легка-1 а	23 - 25	40 – 60	0,1

Дане приміщення обладнане системами опалення, кондиціювання повітря або припливно-витяжною вентиляцією. У приміщенні на робочому місці забезпечуються оптимальні значення параметрів мікроклімату: температури, відносної вологості й рухливості повітря у відповідності до [22]. Рівні позитивних і негативних іонів у повітрі мають відповідати [22]. Для забезпечення оптимальних параметрів мікроклімату в приміщенні проводяться перерви в роботі співробітників, з метою його провітрювання.

4.4.2 Освітлення

Хороше освітлення діє тонізуюче, створює гарний настрій, покращує протікання основних процесів вищої нервової діяльності.

Природне освітлення, коли робочі місця з ПЕОМ розташовуються в один ряд по довжині приміщення на відстані 0,8 - 1,0*м* від стіни з віконними прорізами, і екрани знаходяться перпендикулярно цієї стіни. Оптимальна відстань очей до екрана відео монітора повинна становити 60-70*см*, допустиме не менше 50*см*. Розглядати інформацію ближче 50*см* не рекомендується.

Штучне освітлення створюється газорозрядними лампами. Штучне освітлення в робочому приміщенні передбачається здійснювати з використанням люмінесцентних джерел світла в світильниках загального освітлення, оскільки люмінесцентні лампи мають високу потужність (80Вт), тривалий термін служби (до 10000 годин), спектральний складом випромінюваного світла, близький до сонячного. При експлуатації ЕОМ виконується зорова робота IV розряду точності

(середня точність). При цьому нормована освітленість на робочому місці ($E_н$) рівна 200лк. Джерелом природного освітлення є сонячне світло.

У приміщенні, де розташовані ЕОМ передбачається природне бічне освітлення, рівень якого відповідає [30]. Регулярно повинен проводитися контроль освітленості, який підтверджує, що рівень освітленості задовольняє ДБН і для даного приміщення в світлий час доби достатньо природного освітлення.

Розрахунок освітлення.

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

$$S_b = \left(\frac{1}{5} \div \frac{1}{10}\right) \cdot S_n \qquad (4.1)$$

де S_b – площа віконних прорізів, *м*2 ;

S_n – площа підлоги, $м^2$.

$S_n = a \cdot b = 15 \cdot 15 = 225\ м^2$,

$S = 1/8 \cdot 225 = 28{,}125\ м^2$.

Приймаємо 14 вікон площею $S=2\ м^2$ кожне.

Для організації освітлення в темний час доби передбачається обладнати приміщення, довжина якого складає 15*м*, ширина 15*м*, світильниками ЛПО2П, оснащеними лампами типа ЛБ (дві по 80Вт) з світловим потоком 5400 лм кожна. Розрахунок штучного освітлення виробляється по коефіцієнтах використання світлового потоку, яким визначається потік, необхідний для створення заданої освітленості при загальному рівномірному освітленні. Розрахунок кількості світильників n виробляється по формулі (4.2):

$$n = \frac{E \cdot S \cdot Z \cdot K}{F \cdot U \cdot M}, \qquad (4.2)$$

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

S – освітлювана площа, $м^2$; S = 225 $м^2$;

Z – поправочний коефіцієнт світильника (Z = 1,15 для ламп розжарювання та ДРЛ; Z = 1,1 для люмінесцентних ламп) приймаємо рівним 1,1;

K – коефіцієнт запасу, що враховує зниження освітленості в процесі експлуатації – 1,5;

U – коефіцієнт використання, залежний від типу світильника, показника індексу приміщення і т.п.–0,575M – число люмінесцентних ламп в світильнику –2;

F – світловий потік лампи – 5400лм (для ЛБ-80). Підставивши числові значення у формулу (4.2), отримуємо:

$$n = \frac{300 \cdot 225 \cdot 1{,}1 \cdot 1{,}5}{5400 \cdot 0{,}575 \cdot 2} \approx 18$$

Приймаємо освітлювальну установку, яка складається з 18-х світильників, які складаються з двох люмінесцентних ламп загальною потужністю 160Вт, напругою – 220В.

4.5 Шум та вібрація, електромагнітне випромінювання

Рівень шуму, що супроводжує роботу користувачів персональних комп’ютерів (зумовлений як роботою системних блоків, клавіатури, так і друкуванням на принтерах, а також зовнішніми чинниками), коливається у межах 50–65 дБА [25]. Шум такої інтенсивності на тлі високого ступеня напруженості праці негативно впливає на функціональний стан користувачів. У залах опрацювання інформації та комп’ютерного набору рівні шуму не повинні перевищувати 65 дБА.

Для зниження шуму на шляху його поширення передбачається розміщення в приміщенні штучних поглиначів. Для зниження рівня шуму стелю або стіни вище 1.5 - 1.7 метра від підлоги повинні облицьовуватися звукопоглинальним

матеріалом з максимальним коефіцієнтом звукопоглинання в області частот 63-8000 Гц.

У приміщенні з ЕОМ коректований рівень звукової потужності не перевищує 45 дБА.

Віброізоляція можливо здійснювати за допомогою спеціальної прокладки під системний блок, який послаблює передачу вібрацій робочого столу. Вібрація на робочому місці в приміщенні, що розглядається, відповідає нормам [25].

4.6 Вентилювання

У приміщенні, де знаходяться ЕОМ, повітрообмін реалізується за допомогою природної організованої вентиляції (вентиляційні шахти), тобто при V приміщення > 40м^3 на одного працюючого допускається природна вентиляція. Цей метод забезпечує приток потрібної кількості свіжого повітря, що визначається в СНіП. Також має здійснюватися провітрювання приміщення, в залежності від погодних умов, тривалість повинна бути не менше 10 хв. Найкращий обмін повітря здійснюється при наскрізному провітрюванні.

4.7 Заходи з організації виробничого середовища та попередження виникнення надзвичайних ситуацій

Відповідно до санітарно-гігієнічних нормативів та правил експлуатації обладнання наводимо приклади деяких заходів безпеки.

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

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

1.2) дотримання заходів електробезпеки;

1.3) забезпечення оптимальних параметрів мікроклімату;

1.4) забезпечення раціонального освітлення місця праці;

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

1.6) зниження рівня шуму та вібрації;

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

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

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

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

2.4) не закривати меблями, різноманітним інвентарем вимикачі, штепсельні розетки;

2.5) не підключати одночасно декілька потужних електропристроїв до однієї розетки;

2.6) не залишати включені електроприлади без нагляду;

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

2.8) не ставити на електроприлади матеріали, які можуть під дією теплотизагорітися.

Вимоги безпеки при надзвичайних ситуаціях:

1) При раптовому припиненні подачі електричної енергії вимкнути всі пристрої ПК в такій послідовності: периферійні пристрої, ВДТ, системний блок, стабілізатор (або блок безперервного живлення). Витягнути вилки з розеток. При наявності ознак горіння (дим, запах горілого) необхідно вимкнути всі пристрої ПК, знайти місце загоряння і виконати всі можливі заходи для його ліквідації, попередивши терміново про це керівництво. У випадку виникнення пожежі

негайно попередити про це пожежну частину та керівництво, виконати усі можливі заходи по евакуації людей з приміщення і розпочати гасіння пожежі первинними засобами пожежогасіння.

2) При замиканні, перевантаженні електричного струму на електричному обладнанні, внаслідок ураження грозової блискавки та ймовірної небезпеки ураженням електричним струмом, приймають наступне:

2.1) попередження замикання здійснюється правильним вибором, монтажем експлуатації мереж;

2.2) застосування захисту схем у вигляді швидкодіючих реле, а також вимикачів, плавких запобіжників, автоматичних вимикачів.

Висновки до розділу

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

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

ВИСНОВОК

У даному дипломному проекті була реалізована ЛОМ банківської установи ПАТ “Акцент-Банк”. Метою розробки було оновлення старої мережі. Під час написання роботи була використана велика кількість джерел посилань. Завдяки цій роботі можливо побудувати швидку та захищену мережу для банку.

Під час розробки була спроектована і перевірена схема у надійному програмному комплексі.

Був розрахований метраж кабелю, для побудови мережі. Загальна довжина кабелю — $L = 169{,}3 \cdot 1{,}1 = 186{,}2$м.

Також було необхідно зробити настройку мережі. А саме розподілити IP-адреси та маски.

Результатом цього стало:

Підмережа №1: 205.26.42.0 (205.26.42.0 - 205.26.42.15);

Підмережа №2: 205.26.42.16 (205.26.42.16 - 205.26.42.31);

Підмережа №3: 205.26.42.32 (205.26.42.32 - 205.26.42.47);

Підмережа №4: 205.26.42.48 (205.26.42.48 - 205.26.42.63).

У дипломі були розглянуті загрози інформаційним ресурсам мережі та винайдені методи їх рішення.

Результатом дипломної роботи стала оновлена локальна обчислювальна мережа банківської установи. Були прокладені нові кабелі та реалізована нова топологія ЛОМ, завдяки чому покращилась продуктивність мережі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Таненбаум Э. Компьютерные сети. – СПб.: Питер, 2005. – 992 с.
2. Комп’ютерні мережі: навчальний посібник / [Абрамов В.О.]. – К.: І Київ. ун-т ім. Б. Грінченка, 2010. – 108 с.
3. Максимов Н .В., Попов И.И. М57 Компьютерные сети : учебное пособие для студентов учреждений среднего профессионального образования / Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2016. — 464 с.
4. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. — СПб.: Питер, 2012. — 960 с.
5. Комп’ютерні мережі. Загальні принципи функціонування комп’ютерних мереж. Навчальний посібник. С. В. Мінухін, С. В. Кавун, С. В. Знахур. – Харків: Вид. ХНЕУ, 2008.
6. Сергеев А. Н. Основы локальных компьютерных сетей: Учебное пособие. — СПб.: Издательство «Лань», 2016. — 184 с.
7. Чекмарев Ю. В. Локальные вычислительные сети. Издание второе, исправленное и дополненное.– М.: ДМК Пресс, 2009. – 200 с.
8. Комп’ютерні мережі. Конспект лекцій /Укл.: Зав’ялець Ю.А. – Чернівці, 2015. – 183 с.
9. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. — СПб.: Питер, 2010. — 944 с.
10. Нікітюк Л.А. Телекомунікаційні технології цифрових мереж: Навч. Посібник / за редакцією М.В. Захарченка.- Одеса: УДАЗ ім. О.С. Попова, 2000. – 60с.
11. Мережі та системи телекомунікацій: Т.1: Інформаційні мережі. Стандарти та рекомендації ЄНСМУ. Аналогові та компютерні мережі / М. В. Захарченко, Г. С. Гайворонська, А. І. Єщенко та ін. – 2000. – 304с.
12. Гостєв В.І., Ткаленко О.М. Мережні технології. – Київ, 2009 – 83с.

13. Живиця М.І., Грохольський Я.М., Шелепенко Ю.В., Наталенко П.П., Савінов О.П., Троцько О.О. Телекомунікаційні мережі з комутацією пакетів. Навчальний посібник. – К.: ВІТІ НТУУ «КПІ», 2011. – 352с.
14. Компьютерные сети : Нисходящий подход / Джеймс Куроуз, Кит Росс. — 6-е изд. — Москва : Издательство “Э”, 2016. — 912с.
15. Комп’ютерні мережі та телекомунікації: навчальний посібник / Азарова А.О., Лисак Н.В. — Вінниця: ВНТУ, 2012. — 293с.
16. Одом, У. Официальное руководство Cisco по подготовке к сертификационным экзаменам. М. : Вильямс, 2013. 720 с.
17. Комп’ютерні мережі: навчальний посібник / [Абрамов В.О.]. – К.: І Київ. ун-т ім. Б. Грінченка, 2010. – 108 с.
18. Гедике, А.И. Основы организации и функционирования компьютерных сетей: учеб.-метод. пособие [Электронный ресурс] / А.И. Гедике, Н.В. Лаходынова – Томск, 2016. – 78 с.
19. НПАОП 0.00-6.03-93 Порядок опрацювання та затвердження власником нормативних актів про охорону праці
20. НПАОП 0.00-4.12-05 Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці
21. НПАОП Б.02.005-2003 Про інструктаж, спецнавчання з питань пожежної безпеки
22. НПАОП 0.00-4.15-98 Про розробку інструкцій з охорони праці
23. ДСН 3.3.6.042-99 Санітарні норми мікроклімату виробничих
24. ДСанПіН 3.3.2.007-98 Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин
25. НПАОП 0.00-1.28-10 Правила охорони праці під час експлуатації електронно-обчислювальних машин
26. ДСН 3.3.6.037-99 Санітарні норми виробничого шуму, ультразвуку та інфразвуку
27. ДСН 3.3.6.039-99 Санітарні норми виробничої загальної та локальної вібрації

28. ГОСТ 12.1.006-84 ССБТ. Электромагнитные поля радиочастот. Общие требования безопасности. Допустимые уровни на рабочих местах и требования к проведению контроля
29. ГОСТ 12.1.030-81 ССБТ. Электробезопасность. Защитное заземление. Зануление.
30. ГОСТ 13109-97 „Электрическая энергия. Совместимость технических средств электромагнитных. Нормы качества электро-энергоснабжения общего назначения”
31. ДБН В.2.5-28:2015 Природнє і штучне освітлення
32. НПАОП 40.1-1.21-98 Правила безпечної експлуатації електроустановок споживачів
33. ДБН В.2.5-67:2013 Опалення, вентиляція та кондиціювання
34. ГОСТ 12.1.005-88 ССБТ. Общие санитарно-гигиенические требования к воздуху рабочей зоны

Додаток А

Дипломна робота - Локальна обчислювальна мережа банківської установи

Автор - Любенецький Дмитро Андрійович студент групи КІ-14ад

Керівник – к.т.н. Ларгін Віктор Анатолійович

Актуальність роботи полягає в тому, що діюча ЛОМ банківської установи застаріла та ненадійна

Мета проекту. Розробка актуальної ЛОМ для банківської установи

Задачі проекту. Необхідно спроектувати, оновити і реалізувати ЛОМ для банківської установи ПАТ “Акцент-Банк”.

2

Мережа з виділеним сервером

Оптоволоконний кабель

Топологія дерево

3

Програмне забезпечення локальної мережі

Технології локальних мереж

Захист комп’ютерних мереж

4

Були розглянуті програмні засоби

LanFlow, Cisco Packet Tracer та NetEmul.

Для вирішення завдання обрана програма NetEmul.

5

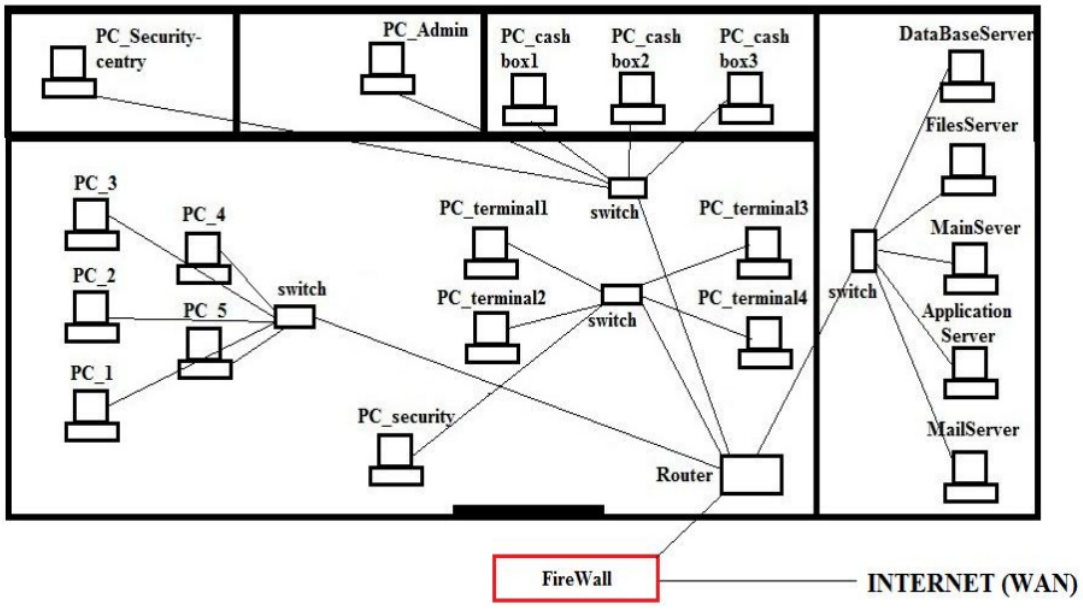

Схема ЛОМ банківської установи

6

Розрахунок загальної довжини кабелю

Розподіл IP-адрес для спроектованої мережі

Операційна система та прикладне ПЗ

Інформаційна безпека мережі

7

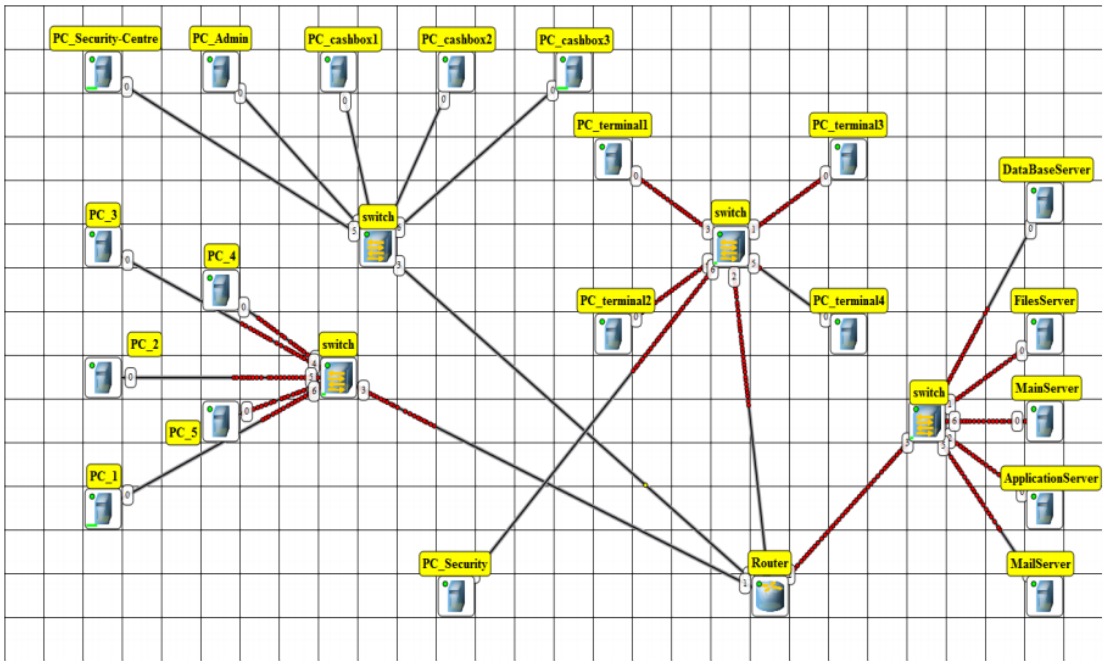

Схема ЛОМ Акцент-Банку в програмі NetEmul

8

Результатом дипломної роботи стала оновлена локальна обчислювальна мережа банківської установи.

Були прокладені структурно нові кабелі, завдяки чому поліпшилася продуктивність мережі.

Була використана краща топологія для швидкодії і надійності мережі.

Вирішено питання безпеки мережі.

9