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

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

ДИПЛОМНИЙ ПРОЕКТ (РОБОТА) БАКАЛАВРА

ПОЯСНЮВАЛЬНА ЗАПИСКА

НА ТЕМУ:

Локальна мережа фінансової установи

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

Керівник проекту:	_____ (підпис)	Рязанцев О.І.. (ініціали, прізвище)
Консультант з охорони праці:	_____ (підпис)	Критська Я.О. (ініціали, прізвище)
Студент:	_____ (підпис)	Чумаченко А. В. (ініціали, прізвище)
Група:		КІ-13бд

Сєвєродонецьк 2017

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

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

ЗАТВЕРДЖУЮ:

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

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

Чумаченко Андрія Вікторовича
(прізвище, ім'я, по батькові)

1. Тема роботи Локальна мережа фінансової установи

керівник проекту (роботи) Рязанцев Олександр Іванович, д.т.н., проф.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від " " 201_ р. № ____
2. Термін подання студентом роботи 17.06.2017
3. Вихідні дані до роботи матеріали переддипломної практики, засоби організація діяльності Лисичанської філії ВАТ КБ " Райффайзен Банк Аваль ", типові потоки інформації автоматизованих банківських систем, розміщення відділень Лисичанської філії, сучасні мережні технології, принципи організації кабельних систем, мережні налаштування операційних систем
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) АНАЛІЗ ДІЯЛЬНОСТІ УСТАНОВИ ТА ПОСТАНОВКА ЗАДАЧІ, ТЕХНІЧНІ ЗАСОБИ КОМП'ЮТЕРНИХ МЕРЕЖ, РОЗРОБЛЕННЯ РОЗПОДІЛЕНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ, ОХОРОНА ПРАЦІ 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
Охорона праці та безпека в надзвичайних ситуаціях	Критська Я.О. ас. кафедри КІ		

7. Дата видачі завдання 03.05.2017

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Ознайомлення з роботою Лисичанської	27.05 - 30.05	
	філії ВАТ КБ "Райффайзен Банк Аваль"		
2	Аналіз типових потоків інформації	01.06 - 05.06	
	АБС ВАТ КБ "Райффайзен Банк Аваль"		
3	Огляд сучасних мережних технологій	06.06 - 10.06	
4	Розробка розділу «Охорона праці та		
	Розробка розділу «Надійність»	11.06 - 13.06	
	безпека в надзвичайних ситуаціях»		
5	Оформлення пояснювальної записки та	13.06 - 16.06	
	плакатів		

Студент _____ Чумаченко А. В.
(підпис) (прізвище та ініціали)

Керівник _____ Рязанцев О.І
(підпис) (прізвище та ініціали)

Р Е Ф Е Р А Т

Пояснювальна записка до дипломного проекту: 83 с., 33 рис., 3 табл., 28 джерел, 19 електронний плакат.

Об'єкт дослідження: Лисичанська філія ВАТ КБ “РАЙФФАЙЗЕН БАНК АВАЛЬ”.

Мета роботи: розроблення розподіленої комп'ютерної мережі фінансової установи, яка працює у банківській галузі.

В проекті виконується розроблення структури комп'ютерної мережі для автоматизації діловодства, банківських і фінансових операцій, обліку клієнтів.

При розробленні локальної мережі враховані всі технологічні особливості даної установи та територіальне розташування її відділів. Структура мережі розроблялась з врахуванням топології розміщення обладнання, аналізу ймовірного розташування каналів передачі даних.

Технічні характеристики окремих підмереж та локальної мережі в цілому розраховані виходячи з інформаційних потоків і технологічних характеристик процесів управління компанією.

КОМП'ЮТЕРНА МЕРЕЖА, МЕРЕЖНА ТЕХНОЛОГІЯ, АПАРАТНЕ ЗАБЕЗПЕЧЕННЯ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, КОМУТАТОР, СЕРВЕР, БАНКІВСЬКА СИСТЕМА.

Умови одержання дипломного проекту

93400 м. Сєвєродонецьк, пр.Центральний 59«А», СНУ ім. В.Даля

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

АТМ – Automated teller machine;

OLTP – On-line Transaction Processing;

БС – банківська система;

АБС – автоматизована банківська система;

СЕП – система електронних платежів;

НЖМД – жорсткий диск;

ОС – операційна система;

ЛОМ – локальна обчислювальна мережа;

РОМ – района обчислювальна мережа;

ГОМ – глобальна обчислювальна мережа;

ГБ – головний банк;

ПК – персональний комп'ютер;

КМ – комп’ютерна мережа;

БД – база даних;

ПЗ – програмне забезпечення.

ВСТУП

В останні роки банківська система нашої країни переживає бурхливий розвиток. Незважаючи на існуючі недоліки українського законодавства, що регулює діяльність банків, ситуація неухильно змінюється на краще. Пройшли часи, коли можна було легко заробляти на спекулятивних операціях з валютою і шахрайстві. Сьогодні усе більше банків робить ставку на професіоналізм своїх співробітників і нові технології.

Важко уявити собі більш благодатний ґрунт для впровадження нових комп'ютерних технологій, ніж банківська діяльність. У принципі майже всі завдання, які виникають у ході роботи банку досить легко піддаються автоматизації. Швидка і безперебійна обробка значних потоків інформації є однієї з головних завдань будь-якої великої фінансової організації. Відповідно до цього очевидна необхідність володіння обчислювальною мережею, що дозволяє обробляти всі зростаючі інформаційні потоки. Крім того, саме банки мають достатні фінансові можливості для використання найсучаснішої техніки. Однак не слід уважати, що середній банк готовий витрачати величезні суми на комп'ютеризацію. Банк є насамперед фінансовою організацією, призначеної для одержання прибутку, тому витрати на модернізацію повинні бути порівнянні з передбачуваною користю від її проведення. Відповідно до загальносвітової практики в середньому банку витрати на комп'ютеризацію становлять не менш 17% від загального кошторису річних витрат.

Інтерес до розвитку комп'ютеризованих банківських систем визначається не бажанням отримати швидкий прибуток, а, головним чином, стратегічними інтересами. Як показує практика, інвестиції в такі проекти починають приносити прибуток лише через певний період часу, необхідний для навчання персоналу і адаптації системи до конкретних умов. Вкладаючи кошти в програмне забезпечення, комп'ютерне і телекомунікаційне обладнання та створення бази для перехід до нових обчислювальних

платформ, банки, у першу чергу, прагнуть до здешевлення і прискоренню своєї рутинної роботи та перемозі в конкурентній боротьбі.

Нові технології допомагають банкам, інвестиційним фірмам і страховим компаніям змінити взаємини із клієнтами і знайти нові засоби для здобування прибутку. Аналітики сходяться в думці, що нові технології найбільше активно впроваджують інвестиційні фірми, потім випливають банки, а самими останніми їх ухвалюють на озброєння страхові компанії.

Завдання, що стоїть перед усіма фінансовими організаціями, однакова: інтеграція успадкованих систем у розподілену архітектуру локальних мереж. Девід Стюарт, головний консультант по нових технологіях в Global Concepts, уважає, що сьогодні попит на людей, що розуміють у мережах, вище, ніж коли-або колись. На його думку, у наш час при устроєві на роботу в банк перевага віддається програмістові, а не касирові.

Банківські комп'ютерні системи на сьогоднішній день є однієї із самих галузей, що швидко розвиваються, прикладного мережного програмного забезпечення. Потрібно відзначити, що БС представляють із себе "ласий шматочок" для будь-якого виробника комп'ютерів і програмного забезпечення. Тому майже всі великі компанії розроблювачі комп'ютерної техніки пропонують на цьому ринку системи на базі своїх платформ.

У якості прикладів передових технологій, використовуваних у банківській діяльності, можна назвати бази даних на основі моделі " клієнт-сервер" (характерне використання ОС Unix і БД Oracle); засоби міжмережевої взаємодії для міжбанківських розрахунків; служби розрахунків, цілком орієнтованих на Internet, або, так звані, віртуальні банки; банківські експертно-аналітичні системи, що використовують принципи штучного інтелекту і багато чого іншого.

Об'єктом дослідження даного дипломного проекту, є локальна мережа Лисичанської філії ПАБ "Райффайзен Банк Аваль". Призначення розроблювальної мережі – об'єднання інформаційно-обчислювальних ресурсів в установі забезпечення підключення персональних комп'ютерів співробітників до корпоративної мережі.

Об'єктом безпосередньої розробки дипломного проекту є локальна обчислювальна мережа, що поєднує інформаційні та обчислювальні ресурси, розташовані в межах двох відділень Лисичанської філії банку.

1 АНАЛІЗ ДІЯЛЬНОСТІ УСТАНОВИ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Стисла характеристика фінансової установи

Сьогодні Райффайзен Банк Аваль Банк – це універсальний комерційний банк загальнонаціонального масштабу. Технологічна база для обслуговування клієнтів – це більш ніж 550 філій у різних містах України, більше 600 власних банкоматів, близько 3200 багатофункціональних POS-терміналів, а також сучасний електронний Контактний центр.

Свою діяльність комерційний банк "Райффайзен Банк Аваль" розпочав 26 жовтня 1993 року, саме в цей день Банк було зареєстровано НБУ (реєстраційний номер 205). Сьогодні банк "Райффайзен Банк Аваль" - універсальна фінансова установа, один із лідерів вітчизняного банківського ринку. "Райффайзен Банк Аваль" входить до десятки найпотужніших банків України, постійно посідає верхні рядки банківського рейтингу. 1999 рік став періодом становлення міжнародного визнання КБ "Райффайзен Банк Аваль". Банк одержав максимальні на той час оцінки за системою CAMEL (за результатами спільної перевірки фахівців НБУ і Міжнародного Валютного Фонду). Банком розпочато емісію платіжних карток VISA та увійшли до складу організацій-партнерів міжнародної системи Western Union. Банк почав роботу з новим фінансовим інструментом - облігаціями зовнішньої державної позики. У 2000 році авторитет банку за кордоном зміцнювався, як свідчення - рейтинги міжнародних рейтингових агентств Thomson Financial BankWatch і FITCH IBCA. Відкрито представництво у м. Будапешт, а угорський "Ексімбанк" встановив банку "Райффайзен Банк Аваль" ліміт для кредитування і підтвердження документарних операцій.

26 жовтня 2005 року банк "Райффайзен Банк Аваль" успішно завершив своє дебютне розміщення трьохрічних єврооблігацій у розмірі 100 млн. доларів США з найнижчим відсотковим спредом за всю історію виходу

українських приватних банків на ринок єврооблігацій. Лід-менеджерами випуску виступили великі інвестиційні банки DrKW та UBS. Єврооблігації пройшли лістинг на Швейцарській біржі з присвоєнням їм рейтингу "B1" від Moody's і "B-" від Fitch. 2006-й став роком оновлення бренду Райффайзен Банк Аваль. Позитивні зрушення відчули як постійні, так і понад 1 млн нових клієнтів Райффайзен Банк Аваль Банку. Головна їх мета - створення позитивних емоцій клієнтів та позитивних вражень від обслуговування в банку. Здобутки 2006 року сприяли поглибленню зв'язків із міжнародними фінансовими інститутами. Так, серед них - успішне повернення першого синдикованого кредиту від західних банків, взятого у 2005 році, та отримання другого синдикованого кредиту на суму понад 100 мільйонів доларів США; запуск спільно з The BanK of New York програми глобальних депозитарних розписок (GDS), тощо.

ВАТ КБ "Райффайзен Банк Аваль" активно розширяє свою регіональну мережу по всій території України. Відкрито регіональні управління в Криму, Донецьку, Вінниці, Дніпропетровську, Полтаві, Запоріжжі, Львові, Одесі, та в інших великих містах України. За станом на 31.12.2013 року банк представлений понад 700 відділеннями в різних містах України та Автономної республіки Крим. З метою представляти інтереси банку, зміцнювати партнерські відносини між підприємствами України Угорщини та Латвії, розвивати зовнішньоторговельні співробітництва між нашими країнами, працюють зарубіжні представництва банку "Райффайзен Банк Аваль" в м. Будапешт (Угорщина) та в м. Рига (Латвія).

ВАТ КБ "Райффайзен Банк Аваль" розвивається як шляхом фінансування та кредитування своїх клієнтів, так і шляхом власного укрупнення, створюючи нові філії. В 2006 році відбулося фінансування діяльності шляхом проведення дев'ятої емісії акцій банку, в результаті якої статутний капітал збільшився, і становить 490,4 млн. грн.

Лисичанська філія ВАТ КБ "Райффайзен Банк Аваль" має дві будівлі (два відділення), розташовані у центральній частині міста Лисичанськ (рис. 1.1). Цей район телефонізований місцевим вузлом зв'язку і у будівлях є

кілька працюючих телефонних пар. Безсумнівним плюсом розташування є близькість комутаційного центру ВАТ Укртелеком. Це дає можливість організувати гарний виділений канал зв'язку шляхом прокладки або оптоволоконного кабелю, або організації XDSL доступу, відстань між відділеннями складає близько 2 км.

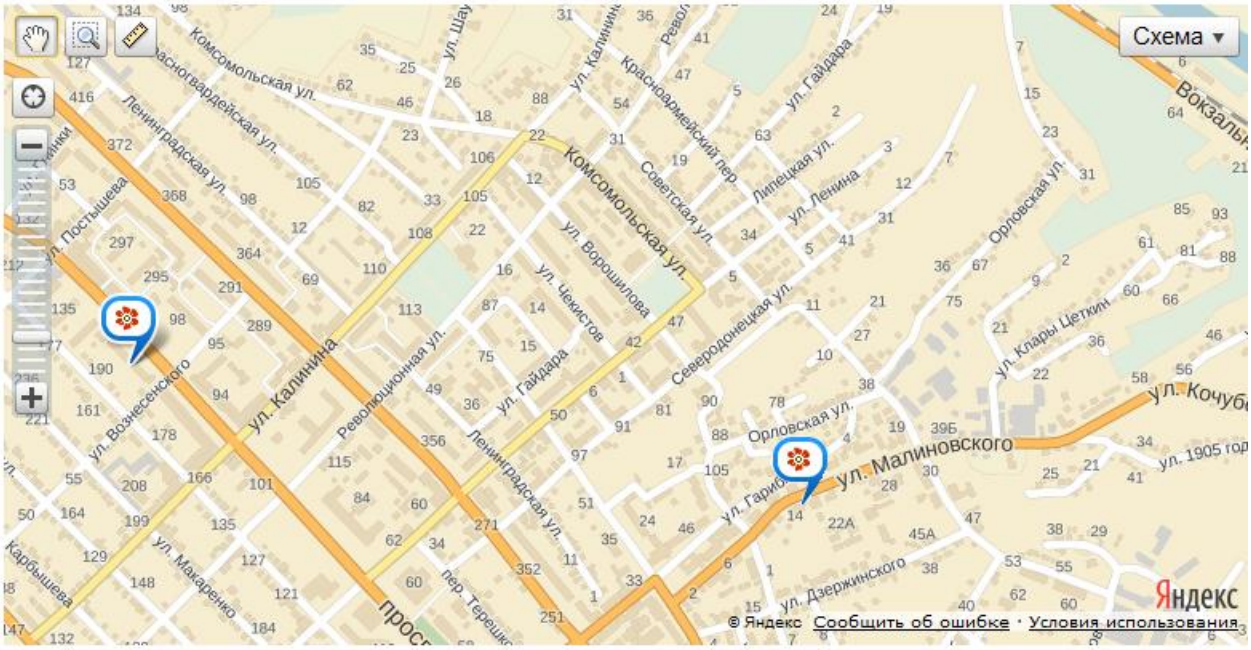

Рисунок 1.1 - Розташування будівель ВАТ КБ "Райффайзен Банк Аваль" у м.Лисичанськ

В будівлі першого відділення (рис.1.2) розташовані: каси №1, кредитний відділ №1, зала обслуговування клієнтів №1, комерційний відділ та директор.

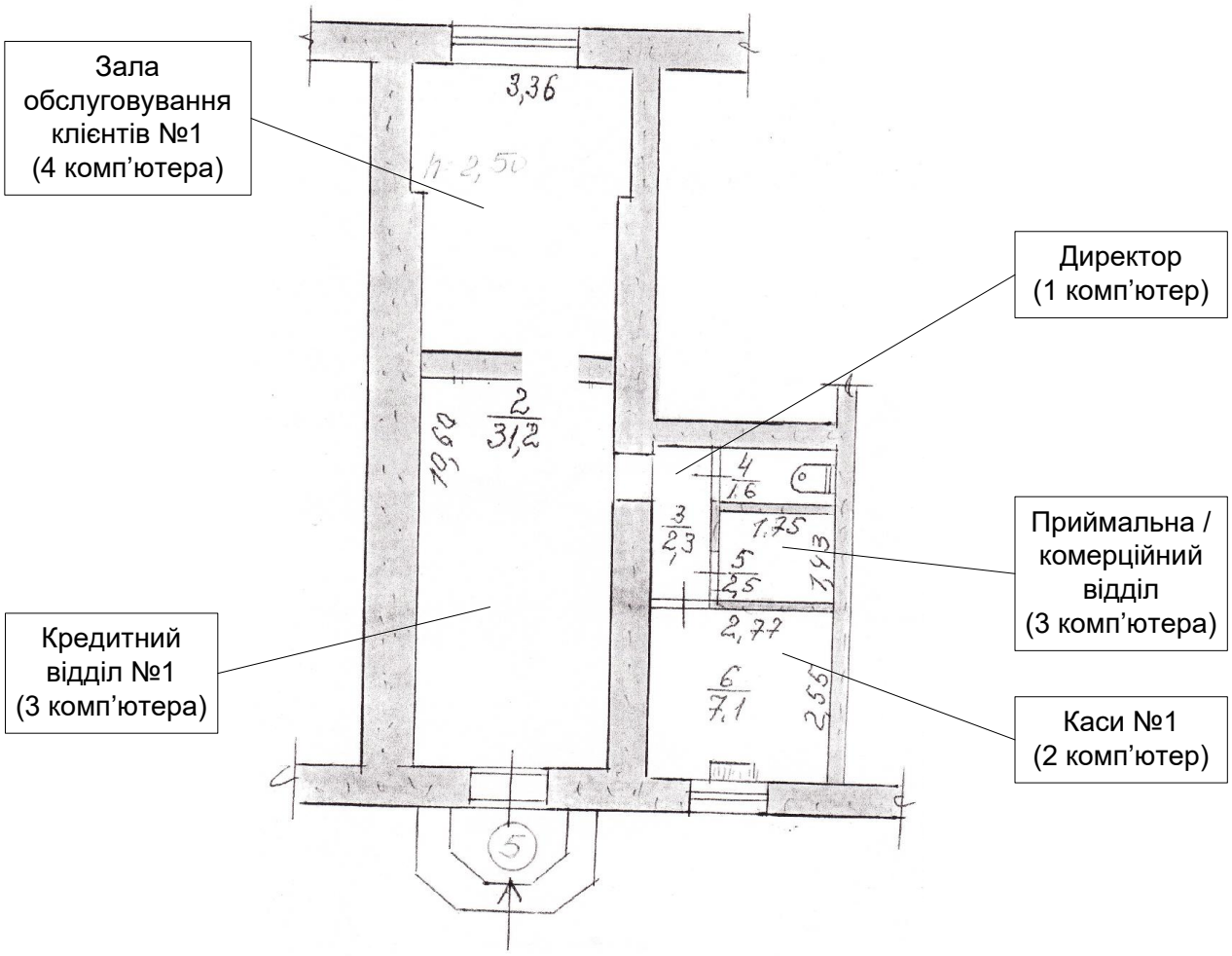

Рисунок 1.2 - План приміщень першого відділення

В будівлі другого відділення (рис.1.3) розташовані: каси №2, кредитний відділ №2, зала обслуговування клієнтів №2 та бухгалтерія.

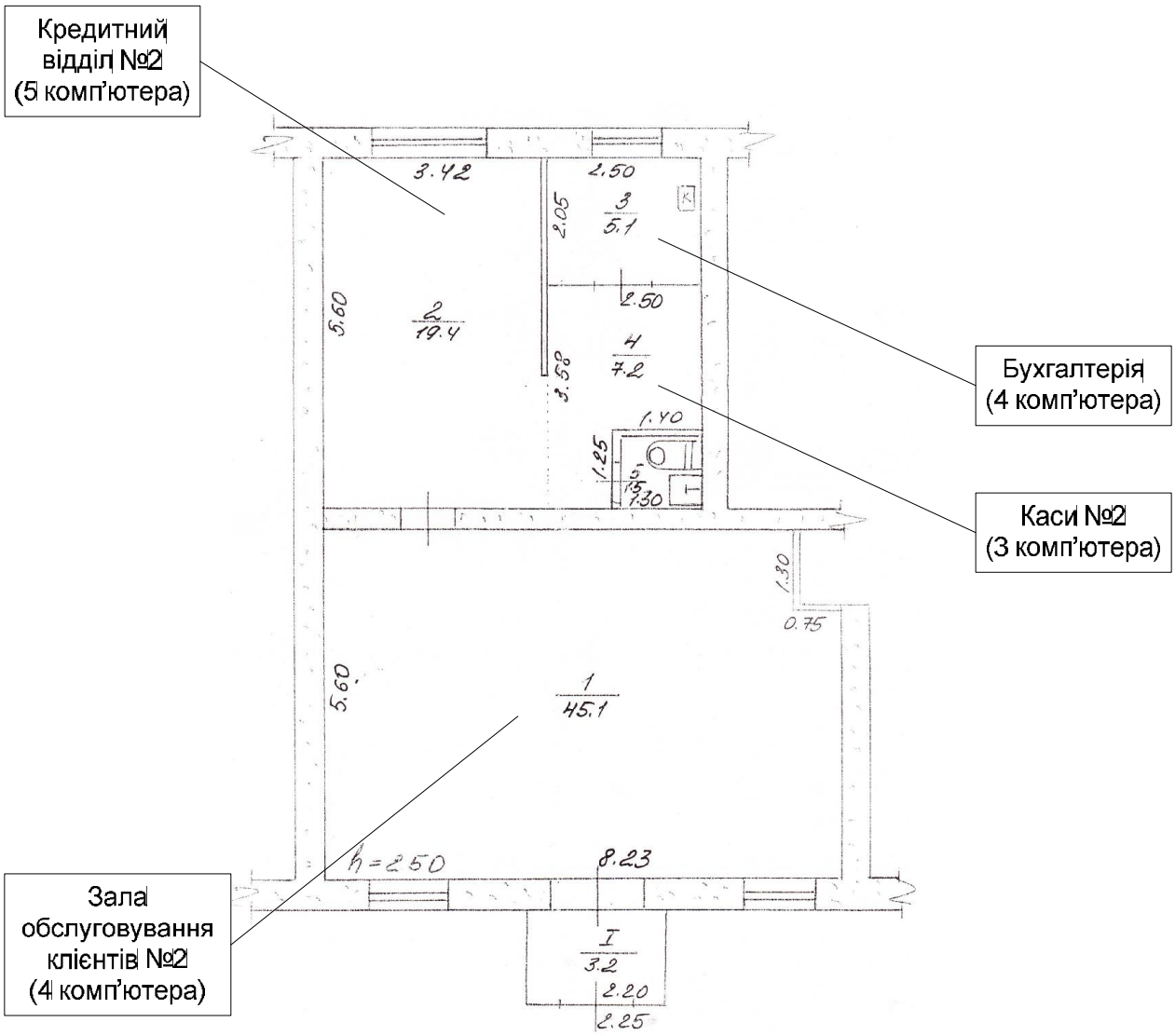

Рисунок 1.3 - План приміщень другого відділення

1.2 Типові потоки інформації АБС ВАТ КБ "Райффайзен Банк Аваль" і керування ними

Автоматизована банківська система (АБС) — це система, яка функціонує на основі ЕОМ та інших технічних засобів, що забезпечують процеси збору, реєстрації, передачі, обробки, збереження та актуалізації даних для розв'язання завдань управління банківською діяльністю. Автоматизована банківська система є інтегрованою. Інтегрована — це така

система, що побудована на загальносистемних принципах й охоплює всю сукупність банківських задач. Вона вирішує питання автоматизації комплексно з урахуванням інформаційних і функціональних зв'язків. Як будь-яка система, АБС може бути представлена у вигляді певної сукупності підсистем. До складу АБС входять забезпечуючі та функціональні підсистеми. Забезпечуючі підсистеми об'єднують в собі всі види ресурсів, необхідні для функціонування системи. До їх складу відносяться такі підсистеми: інформаційного, програмного, математичного, технічного, лінгвістичного та організаційно-правового забезпечення.

Інформаційне забезпечення — це сукупність уніфікованих форм первинних документів, систем класифікації і кодування та методів їх застосування в банківській діяльності, а також файли даних, що зберігаються у базі даних і використовуються для автоматизованого вирішення функціональних задач.

Технічне забезпечення — це комплекс технічних засобів, який включає до свого складу обчислювальну техніку та засоби збору і передачі даних для інформаційного обміну як всередині банку, так і при взаємодії з іншими банками та клієнтами.

Математичне забезпечення являє собою сукупність алгоритмів та економіко-математичних моделей, які характеризують процедури обробки даних та формування бухгалтерської і статистичної звітності.

Організаційно-правове забезпечення — це сукупність нормативно-правових документів та інструктивних і методичних матеріалів, які регламентують права й обов'язки спеціалістів та визначають технологічний порядок функціонування АБС.

Лінгвістичне забезпечення включає до свого складу мовні засоби, що використовуються в системі: мови програмування, інформаційно-пошукові мови, мови опису метаданих, мови запитів і спілкування користувачів з системою й інші мовні засоби.

Функціональні підсистеми виокремлюють, виходячи з певних ознак управління. Враховуючи багатоаспектність банківських завдань, виникає

проблема декомпозиції АБС на функціональні підсистеми. Функціональна підсистема — це певна частина загальної системи управління, яка виділена відповідно до спільності функціональних ознак управління. Основою для функціональної декомпозиції можуть бути такі характеристики: функція, період і об’єкт управління.

Автоматизована банківська система повинна забезпечувати:

– автоматизацію внутрібанківської діяльності, і насамперед внутрибанківських операцій, пов’язаних з обробкою платіжних та інших документів у тих підрозділах банківської установи, які працюють безпосередньо з клієнтами;

– автоматизацію виконання міжбанківських розрахунків та інших зовнішньобанківських операцій;

– автоматизацію фінансових операцій в межах міжнародного банківського бізнесу.

Вивчення структур різних банківських систем та проведене певне їх узагальнення дають змогу виділити такі основні функціональні підсистеми АБС (рис.1.4) :

– операційний день банку (ОДБ),

– управління кредитними ресурсами (Кредити),

– управління валютними операціями (Валютні операції),

– управління депозитами (Депозити),

– управління цінними паперами (Цінні папери),

– управління касою (Каса),

– внутрибанківський облік (Внутрішній облік),

– управління розрахунками з використанням пластикових карток (Карткові операції),

– звітність, аналіз діяльності банку (Аналіз).

АБС — це технологічна система, яка забезпечує функціонування банківської установи. Ядром АБС є підсистема ОДБ, яка інформаційно зв’язана з іншими функціональними підсистемами.

Крім внутрішніх інформаційних зв'язків, АБС характеризується великим спектром інформаційних зв'язків із зовнішнім середовищем, в ролі якого виступають клієнти банку, інші банки, фінансові та державні органи. Загальну структурну схему побудови АБС представлено на рис. 1.4.

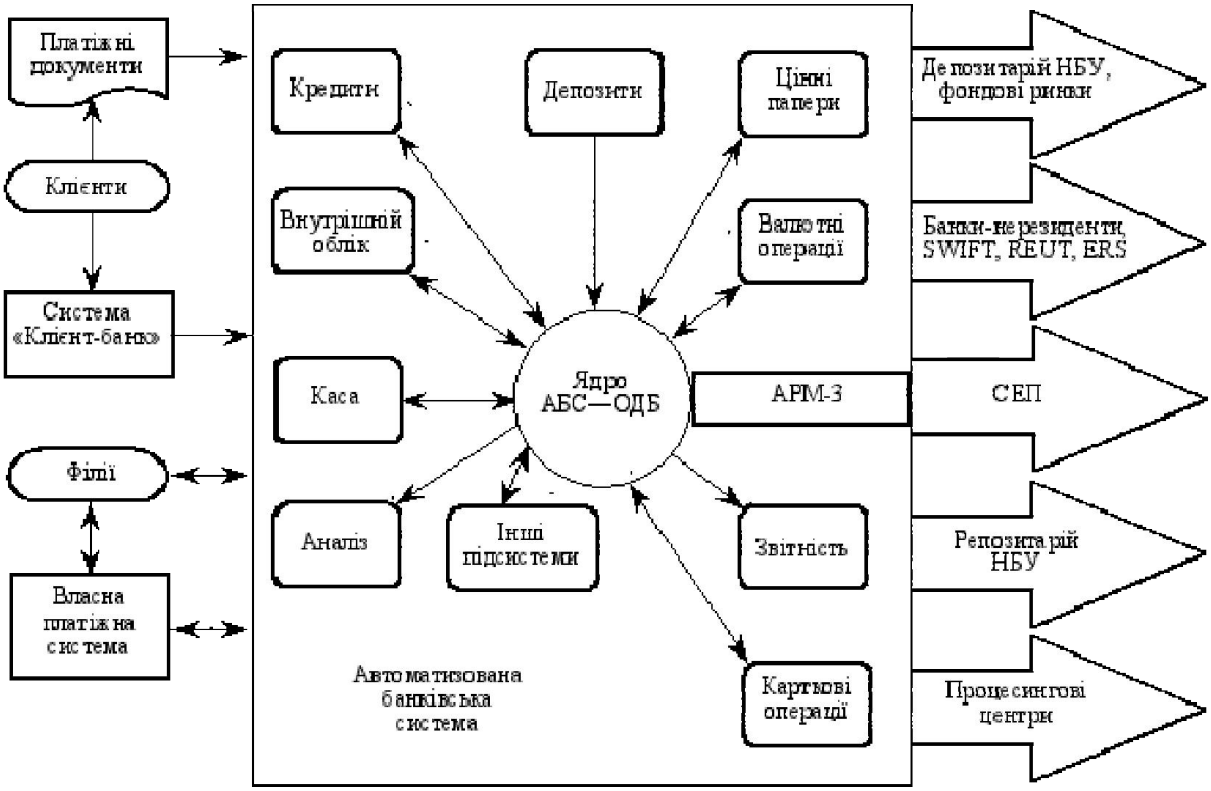

Рис.1.4 – . Структурна схема АБС

На рис.1.5 наведена апаратно-структурна реалізація АБС в багатофілійному досліджуємому ВАТ КБ "Райффайзен Банк Аваль", який у 2009 році після приходу нових закордонних інвесторів прийняв стратегію підвищення рівня захисту та сертифікованості банківських програмних продуктів, замінює автоматизовану банківську систему, засновану на засобах комплексної системи автоматизації фірми SYBASE та програмних продуктах власної розробки банку, на новітню Автоматизовану Банківську систему "БАРС-Millennium" фірми «Уніті-Барс», яка впроваджена в Національному банку України, в Державному ощадному банку України та інших великих комерційних банках України.

Автоматизована Банківська Система «Bars Millennium» [], надалі АБС, являє собою складну потужну і гнучку систему автоматизації банківських

процесів. Побудована на модульній основі, що опирається на сучасну СУБД корпорації Oracle та використовуюча інші продукти цієї корпорації, АБС дозволяє реалізувати різнопрофильні рішення для різних фінансових сфер, дозволяє зберігати і обробляти великі обсяги даних, дозволяє проводити аналіз даних будь-якої складності і глибини.

АБС являє собою 2-х рівневу архітектуру доступу до даних. Більша частина бізнес-логіки винесена на рівень схеми й процедур БД. Останнім часом все більше число завдань і нових модулів реалізується в багаторівневій архітектурі з використанням мережних технологій і серверів додатків. АБС параметризирована, що дозволяє врахувати при настроюванні індивідуальні особливості банку, оснащена гнучкою системою адміністрування й надійною системою розмежування прав і захисту даних. Багаторівневі системи фінансового візування й верифікації, роздільного доступу до фінансових ресурсів банку забезпечують надійну фінансову безпеку. АБС може взаємодіяти з більшістю сучасних криптографічних засобів захисту. АБС має відкриту систему імпорту-експорту, що дозволяє їй інтегруватися в будь-які комплексні рішення автоматизації.

Основними концепціями АБС «Bars Millennium» є:

- орієнтація на промислові сервера баз даних Oracle;
- використання архітектури « Клієнт-Сервер»;
- незалежність клієнтської частини від використовуваного сервера;
- транзакційність;
- підтримка цілісності на рівні СУБД;
- набір внутрішніх обмежень цілісності й правил зберігання даних;
- зберігання й обробка великих обсягів інформації;

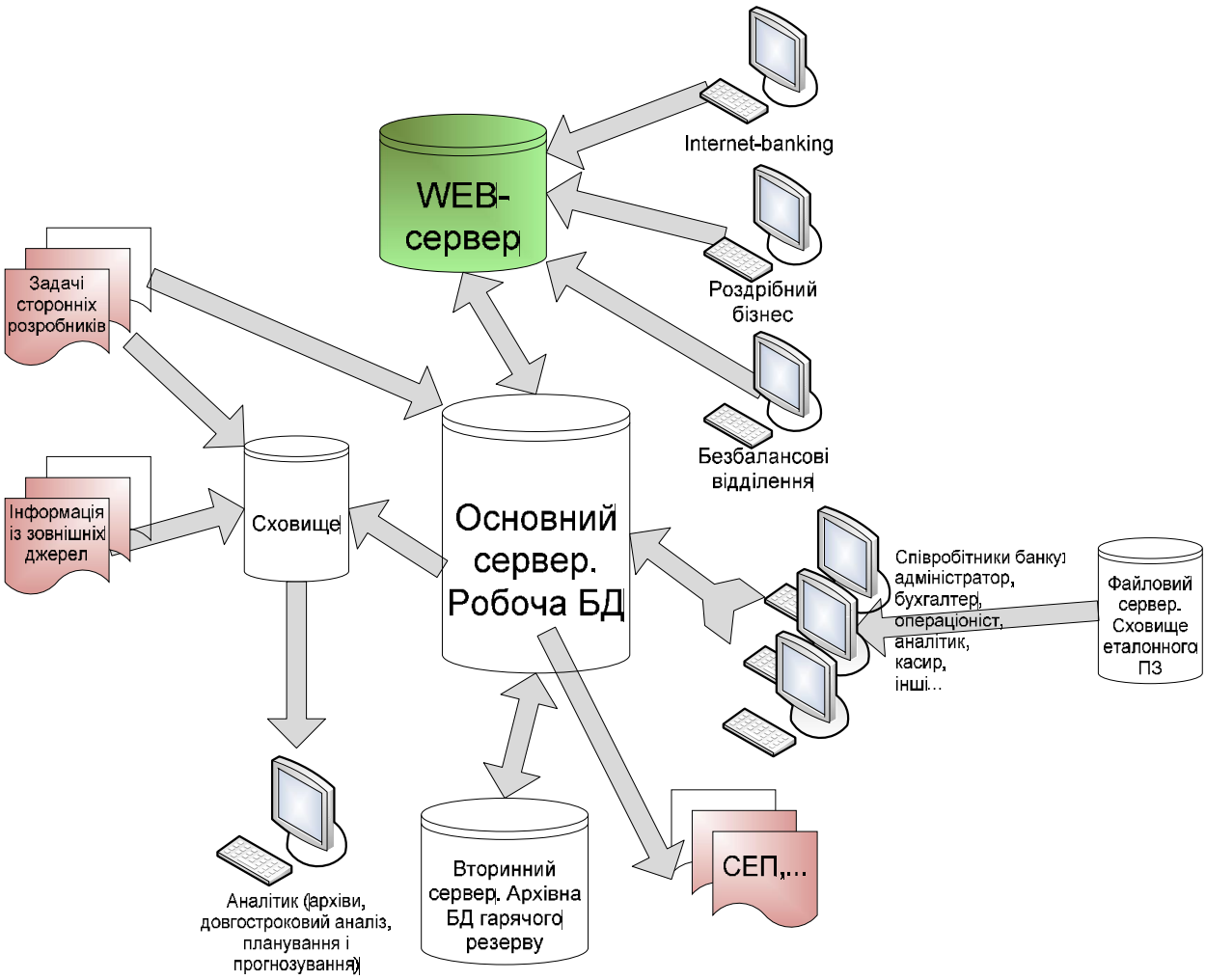

Рисунок 1.5. - Архітектура системи АБС ВАТ КБ "Райффайзен Банк Аваль"

У результаті аналізу технічних засобів використовуваних в установі і основних потоків даних передбачається побудова мережі, що складається із двох підмереж.

У першу підмережу (підмережа "Відділення №1") будуть включені робочі місця касирів каси №1, менеджерів кредитного відділу №1, менеджерів з обслуговування клієнтів №1, менеджерів комерційного відділу, а так само робоче місце секретаря і директора. Друга підмережа (підмережа "Відділення №2") об'єднає комп'ютери в бухгалтерії №2, касі №2, кредитному відділі №2, зали обслуговування клієнтів №2. Така побудова диктується розташуванням зазначених відділів в різних приміщеннях і припускає використання для кожної підмережі окремого мережного обладнання та лінії зв'язку двох підмереж.

Основне навантаження на підмережи кожного відділення виконує базова підсистема «Операційний день банку» (ОДБ). Основні функції цієї підсистеми такі:

– введення та обробка клієнтських платіжних документів;

– створення та ведення особових рахунків клієнтів та масивів нормативно-довідкової інформації;

– робота з картотеками;

– обробка особових та балансових рахунків;

– ведення аналітичного і синтетичного обліку, формування балансу за кожний банківський день та відповідних вихідних форм;

– сервісні функції: відкриття, закриття та протоколювання банківського дня, встановлення лімітів, бізнес-правил для філій банку тощо.

У структурі будь-якого ОДБ можна виокремити три типи функціональних блоків, існування яких випливає із загальної технології його роботи. Це блоки початку роботи (відкриття ОДБ), блоки роботи протягом робочого дня і блоки закінчення роботи (закриття ОДБ).

Блоки відкриття ОДБ забезпечують обробку паролей та ідентифікацію користувачів, введення дати поточного банківського робочого дня, обробку отриманих з АРМ НБУ файлів початку роботи. При цьому коригується довідник банків — учасників СЕП, визначається значення кореспондентського рахунку банку на початок робочого дня, очищуються відповідні оперативні бази даних тощо. У процесі відкриття ОДБ накопичуються відсотки за попередній день за рахунками з процентними ставками, створюються копії вхідних основних масивів стану особових та балансових рахунків на початок дня. Якщо це день початку місяця, кварталу або року, то за балансовими рахунками формуються відповідні вхідні залишки на початок періоду, обнулюються обороти за місяць, квартал або рік. Водночас для співробітників банку встановлюються повноваження стосовно допуску до особових рахунків; функції та рахунки для обробки

перерозподіляються між працівниками банку, змінюється відповідальний виконавець, котрий веде рахунок, і т. ін.

Протягом дня відповідними блоками ОДБ виконуються операції з реєстрації нових клієнтів, відкриття або закриття рахунків, забезпечення вводу первинних платіжних документів клієнтів протягом дня та їх обробки. Прийняті від клієнтів документи поділяються на «внутрішні», в яких платник і одержувач є клієнтами даного банку, та «міжбанківські», в яких одержувачем є клієнт іншого банку. На підставі першої групи документів виконуються внутрішньобанківські проведення (змінюються залишки на рахунках), а на підставі другої формуються файли типу А (початкові міжбанківські платежі для їх передання до СЕП). Проведення «оплата» виконується лише в тому разі, якщо воно не загрожує ситуацією «червоне сальдо» за одним із кореспондуючих рахунків.

Блоки закриття ОДБ забезпечують перевірку наявності балансу, формування та видачу відомостей щодо накопичених оборотів за місяць (квартал, рік), створення копій основних файлів, архівацію платіжних документів, видачу вихідних форм про обороти за день, формування, архівацію і друк виписок. Залежно від дня місяця, кварталу, року блоки закриття формують звітність для НБУ, інформацію для податкових органів та інших служб.

Крім функціональних блоків ОДБ містить і блоки ведення та друку довідково-нормативної інформації, блоки «відновлення», тобто виконання перерахунків з певного моменту часу. Розрізняють «коротке» і «довге» відновлення. Перше використовується для виправлення помилок за тими документами, які ще не відправлені до СЕП. До нього вдаються і в разі отримання «відбійної» квитанції на якийсь раніше відправлений файл А. «Довге» відновлення полягає у відтворенні ситуації на момент закриття якого-небудь минулого дня з послідовним перераховуванням усіх операцій наступних днів.

Діяльність менеджерів роботи з корпоративними клієнтами комерційного відділу передбачає взаємне використання великої кількості

загальних ресурсів: логічні диски (диски D усіх комп'ютерів відкриті для доступу по мережі), дисководи CD-ROM, мережні принтера. Передача даних між бухгалтерією і комерційним відділом проводиться досить рідко і може розглядатися окремо. Робоче місце секретаря має DSL підключення до виділеного інтернет-серверу для приймання електронної пошти і роботи в середовищі Інтернет. Менеджери роботи з корпоративними клієнтами є найбільш активними користувачами електронної пошти і ресурсів Інтернет. Це є однією із причин, по якій комп'ютер секретаря планується підключити в підмережу комерційного відділу.

Використання двох концентраторів дозволить скоротити довжину кабелів необхідних для підключення бухгалтерії, при цьому зберігши інформаційні ресурси обох відділів у тому ж складі. У результаті, зміна структури мережі не спричинить змін, що вимагають навчання або перепідготовки кінцевих користувачів. Реструктуризацію передбачається провести лише на апаратному рівні, не зачіпаючи звичного користувацького середовища.

1.3 Технічні вимоги до об'єкта розробки

1.3.1 Найменування і галузь застосування

Об'єктом розробки для даного дипломного проекту є локальна комп’ютерна мережа. Підприємством, на якому планується впровадження розробленої мережі, є відділення Лисичанської філії ВАТ КБ "Райффайзен Банк Аваль".

1.3.2 Призначення розробки

Розроблювальна мережа повинна замінити вже існуючу в відділеннях мережу і забезпечити більш високі технічні характеристики. Основним призначенням розробки є забезпечення наступних функцій:

– передача інформації з одного робочого місця на інше;

– підключення всіх користувачів до корпоративної мережі ВАТ КБ "Райффайзен Банк Аваль";

– друк документів за допомогою мережних принтерів;

– безперебійна робота підсистем АБС.

1.3.3 Вимоги до функціональних характеристик

Розроблювальна мережа повинна мати такі характеристики:

– швидкість передачі – 100 Mbps, при роботі усередині мережі;

– швидкість підключення до корпоративної мережі – не нижче 1 Mbps;

– безпека внутрімережної інформації;

– роботу всіх додатків, які використовують співробітники ВАТ КБ "Райффайзен Банк Аваль".

1.3.4 Вимоги до складу і параметрів технічних засобів

Склад розроблювальної комп'ютерної мережі Лисичанської філії ВАТ КБ "Райффайзен Банк Аваль":

– інтернет-сервер;

– середовище передачі даних (мережний кабель між двома відділеннями);
– дві локальні підмережи, до складу яких входять:
  1) комутатор;
  2) середовище передачі даних (мережний кабель зовні відділення);
  3) сервер АБС;
  4) робочі станції.

1.3.5 Вимоги до інформаційної і програмної сумісності

Операційні системи ПК користувачів повинні забезпечувати нормальне функціонування локальних додатків, додатків, що опираються на архітектуру клієнт-сервер, а також мати зручний для користувачів інтерфейс та високий рівень безпеки (рекомендується розглянути можливість переходу з Windows XP на Linux).

Операційні системи серверів АБС повинні забезпечувати нормальне функціонування всіх додатків, що використовуються у філії (у тому числі, що опираються на архітектуру клієнт-сервер), а також мати достатню стійкість і засобами безпеки (рекомендується розглянути можливість переходу з Windows Server 2008 на Linux).

Операційна система інтернет-сервера повинна бути максимально адаптована для роботи з більшою кількістю даних, орієнтована на роботу з інтернет і мати засоби забезпечення безпеки при роботі користувача з ресурсами глобальної мережі (рекомендується Linux).

2 ТЕХНІЧНІ ЗАСОБИ КОМП'ЮТЕРНИХ МЕРЕЖ

Обчислювальною мережею називається система взаємозалежних і розподілених по фіксованій території обчислювальних центрів (ОЦ) або ЕОМ, орієнтованих на комплексне використання загальносітьових ресурсів: апаратних, програмних і інформаційних. Основне призначення мережі – забезпечення зручного і надійного доступу користувачів до розподілених по площі загальносітьових ресурсів і організації колективного їхнього використання.

Локальна комп'ютерна мережа — це насамперед середовище передачі сигналів. Без середовища передачі мережі не може бути просто по визначенню, як не може бути подиху без повітря. Середовище передачі можна умовно розділити на обмежену і необмежену. Обмежене середовище — це, попросту говорячи, кабель. Як приклад необмеженого середовища можна взяти відкритий ефір, по якому передає сигнали Radioethernet.

2.1 Середовище передачі даних

У якості середовища передачі сигналів у локальних мережах, як правило, використовуються:

- коаксіальний кабель;
- кабель на основі крученому пари;
- оптоволоконний кабель.

Показники трьох типових середовищ для передачі наведені в таблиці.

Таблиця 2.1 – Характеристики мережних кабелів

Показники	Середовище передачі даних		
	Двох жильний кабель - кручена пари	Коаксіальний кабель	Оптоволоконний кабель
Ціна	Невисока	Відносно висока	Висока
Нарощування	Дуже простої	Проблематично	Простої
Захист від прослуховування	Незначна	Гарна	Висока
Проблеми із заземленням	Немає	Можливі	Немає
Сприйнятливість до перешкод	Існує	Існує	Відсутня

Аналізуючи дані таблиці можна зробити висновок, що по показникові ціна/якість, найбільш оптимальним є використання мережного кабелю типу “кручена пари” при проектуванні підмереж локальної мережі підприємства та оптоволокно при з'єднанні двох підмереж. До аналогічних виводів прийшли керівники і системний адміністратор "" при проведенні самостійного незалежного аналізу.

2.2 Топології обчислювальної мережі

Існує ряд принципів побудови ЛОМ на основі вище розглянутих компонентів. Такі принципи ще називають – топологіями.

Основні характеристики трьох найбільш типових топологій обчислювальних мереж наведені в таблиці 2.2.

Таблиця 2.2 - Основні характеристики топологій обчислювальних мереж

Характеристики	Топології обчислювальних мереж		
	Зірка	Кільце	Шина
Вартість розширення	Незначна	Середня	Середня
Приєднання абонентів	Пасивне	Активне	Пасивне
Захист від відмов	Незначна	Незначна	Висока
Розміри системи	Будь-які	Будь-які	Обмежені
Вартість підключення	Незначна	Незначна	Висока
Поведінка системи при високих навантаженнях	Гарне	Задовільне	Погане
Можливість роботи в реальному режимі часу	Дуже гарна	Гарна	Погана
Розведення кабелю	Гарна	Задовільна	Гарна
Обслуговування	Дуже гарне	Середнє	Середнє

Техніка широкополосних повідомлень дозволяє одночасно транспортувати в комунікаційному середовищі досить великий обсяг інформації.

Аналізуючи данні таблиці не можна зробити однозначний висновок про технологію побудови локальної мережі підприємства, розміри і значимість використання засобів обчислювальної техніки, порівнянні з розглянутим вищим навчальним закладом.

Компромісом наведених характеристик може служити деревоподібна структура ЛОМ (рис. 2.1). Вона утвориться в основному у вигляді комбінацій вищезгаданих топологій обчислювальних мереж. Основа дерева обчислювальної мережі (корінь) розташовується в точці, у якій збираються комунікаційні лінії інформації (гілки дерева).

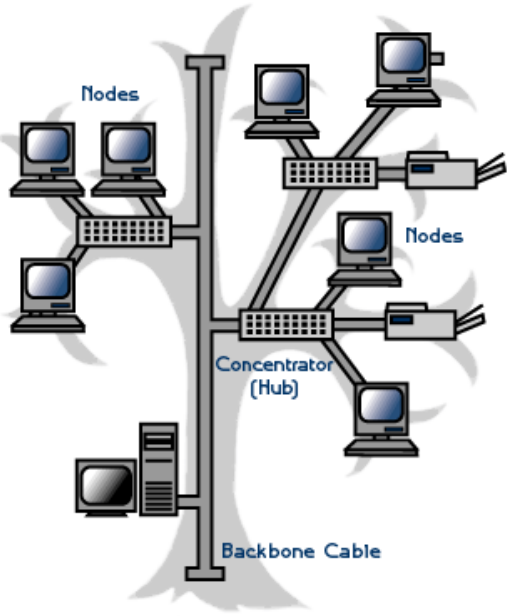

Рисунок 2.1 - Структура топології деревоподібної ЛОМ

Обчислювальні мережі з деревоподібною структурою застосовуються там, де неможливо безпосереднє застосування базових мережних структур у чистому вигляді. Для підключення великої кількості робочих станцій відповідно адаптерним платам застосовують мережні підсилювачі і/або комутатори. Комутатор, що має одночасно і функції підсилювача, називають активним концентратором.

На практиці застосовують два їхні різновиди, що забезпечують підключення відповідно восьми або шістнадцяти ліній.

Пристрій до якого можна приєднати максимум три станції, називають пасивним концентратором. Пасивний концентратор звичайно використовують як розгалужетель. Він не має потреби в підсилювачі. Передумовою для підключення пасивного концентратора є те, що можлива максимальна відстань до робочої станції не повинне перевищувати декількох десятків метрів.

Отже, виходячи з логічної організації мережі, кожну виділену групу робочих місць доцільно з'єднати за допомогою комутатора, що має мінімум два порти Gigabit Ethernet для магістрального каналу зв'язку і кілька портів 100Mbit Ethernet, причому, таких портів повинне бути трохи більше чим комп'ютерів у групі, щоб забезпечити масштабованість системи. Комутатор

для кожної групи доцільно вибрати з апаратними маршрутизаторами пакетів, щоб забезпечити автоматичне екранування груп друг від друга, за винятком дозволеного трафіку. Також замість маршрутизатора можна використовувати робочу станцію, із двома мережними адаптерами Gigabit Ethernet, але таке рішення є більше дорогим і менш гнучким, тому на практиці застосовується рідко. З метою підвищення стійкості і масштабованості системи, необхідно забезпечити резервні шляхи циркуляції потоків інформації усередині мережі. Для цієї мети всі комутатори робочих груп, крім з'єднання з єдиним центром комутації, планується з'єднати між собою магістральним каналом 1Gbit/s по топології логічного кільця.

2.3 Міжмережні технології і протоколи

Узгодження глобальних мереж між собою і з локальними здійснюється на мережному і транспортному рівнях. У цей час існує два основних підходи до формування міжмережних взаємодії:

– об'єднання мереж відповідно до міжмережного протоколу IP

– об'єднання мереж комутації пакетів (X25) відповідно до рекомендації міжнародного комітету МККТТ X75.

Основне розходження в цих підходах наступне: протокол IP відноситься до протоколів без установлення логічного з'єднання (дейтограмний), а рекомендація X75 передбачає реалізацію віртуального з'єднання (тобто каналу). Становлення корпоративних комп'ютерних мереж тісно пов'язане з мережею Internet, у рамках якої були реалізовані і апробовані основні принципи міжмережного з'єднання. З мережею Internet пов'язана і поява протоколів Internet Protocol (IP). Територіально розташовуються на мережному рівні. Погоджують транспортну і мережну служби різних комп'ютерних мереж.

Internet - велика розгалужена мережа, що містить у собі комп'ютерні вузли, розкидані по усьому світі. На сьогоднішній день це більше 120 країн миру.

Прародителькою Internet стала мережа ArpaNet, розроблена в 1969 році фірмою BBN вона об'єднала навчальні заклади, військові організації, і їхніх підрядників. Спочатку ArpaNet дозволяла тільки ввійти в систему і запускати програму на вилученому комп'ютері. Незабаром додалося:

– передача файлів;

– електронна пошта;

– розсилання, забезпечення спілкування користувачів, які цікавилися однієї і тією же галуззю науки.

Протоколи. Для того, щоб мати інформацію про поточну конфігурацію мережі, маршрутизатори обмінюються маршрутною інформацією між собою по спеціальному протоколі. Протоколи цього типу називаються протоколами обміну маршрутною інформацією (або протоколами маршрутизації). Протоколи обміну маршрутною інформацією варто відрізняти від, властиво, протоколів мережного рівня. У той час як перші несуть чисто службову інформацію, другі призначені для передачі користувальницьких даних, також, як це роблять протоколи канального рівня.

Для того, щоб доставити вилученому маршрутизатору пакет протоколу обміну маршрутною інформацією, використовується протокол мережного рівня, тому що тільки він може передати інформацію між маршрутизаторами, що перебувають у різних мережах. Пакет протоколу обміну маршрутною інформацією міститься в полі даних пакета мережного рівня, тому з погляду вкладеності пакетів протоколи маршрутизації варто віднести до більше високого рівня, чим мережний. Але функціонально вони вирішують загальне завдання з пакетами мережного рівня - доставляють кадри адресатові через різнорідну складену мережу.

За допомогою протоколів обміну маршрутною інформацією маршрутизатори становлять карту міжмережних зв'язків того або іншого

ступеня подробиці і ухвалюють рішення щодо того, якому наступному маршрутизатору потрібно передати пакет для утворення раціонального шляху.

Transmission Control Protocol/Internet Protocol (TCP/IP) - це промисловий стандарт стека протоколів, розроблений для глобальних мереж.

Стандарти TCP/IP опубліковані в серії документів, названих Request for Comment (RFC). Документи RFC описують внутрішню роботу мережі Internet. Деякі RFC описують мережні сервіси або протоколи і їхню реалізацію, у той час як інші узагальнюють умови застосування. Стандарти TCP/IP завжди публікуються у вигляді документів RFC, але не всі RFC визначають стандарти.

В цей час стік TCP/IP розповсюджений в основному в мережах з ОС UNIX, Windows, MacOS. Отже роль стека TCP/IP пояснюється наступними його властивостями:

– це найбільш завершений стандартний і в той же час популярний стік мережних протоколів, що має багаторічну історію;

– майже все більші мережі передають основну частину свого трафіка за допомогою протоколу TCP/IP;

– це метод одержання доступу до мережі Internet;

– цей стек є основою для створення intranet- корпоративної мережі, що використовує транспортні послуги Internet і гіпертекстову технологію WWW, розроблену в Internet;

– всі сучасні операційні системи підтримують стек TCP/IP;

– це гнучка технологія для з'єднання різнорідних систем як на рівні транспортних підсистем, так і на рівні прикладних сервісів;

– це стійке масштабоване міжплатформене середовище для додатків клієнт-сервер.

Протоколи TCP/IP поділяються на 4 рівні.

Самий нижній (рівень IV) відповідає фізичному І канальному рівням моделі OSI. Цей рівень у протоколах TCP/IP не регламентується, але підтримує всі популярні стандарти фізичного і канального рівня: для

локальних мереж це Ethernet, Token Ring, FDDI, Fast Ethernet, 100VG-AnyLAN, для глобальних мереж - протоколи з'єднань "точка-точка" SLIP і PPP, протоколи територіальних мереж з комутацією пакетів X.25, frame relay. Розроблена також спеціальна специфікація, що визначає використання технології ATM як транспорт канального рівня. Звичайно з появою нової технології локальних або глобальних мереж вона швидко включається в стек TCP/IP за рахунок розробки відповідного RFC, що визначає метод інкапсуляції пакетів IP у її кадри.

Наступний рівень (рівень III) - це рівень міжмережної взаємодії, що займається передачею пакетів з використанням різних транспортних технологій локальних мереж, територіальних мереж, ліній спеціального зв'язку та т.і.

Як основний протокол мережного рівня (у термінах моделі OSI) у стеці використовується протокол IP, що споконвічно проектував як протокол передачі пакетів у складених мережах, що складаються з великої кількості локальних мереж, об'єднаних як локальними, так і глобальними зв'язками. Тому протокол IP добре працює в мережах зі складною топологією, раціонально використовуючи наявність у них підсистем і ощадливо витрачаючи пропускну здатність низькошвидкових ліній зв'язку. Протокол IP є дейтаграмним протоколом, тобто він не гарантує доставку пакетів до вузла призначення, але намагається це зробити.

До рівня міжмережних взаємодії відносяться і всі протоколи, пов'язані зі складанням і модифікацією таблиць маршрутизації, такі як протоколи збору маршрутної інформації RIP (Routing Internet Protocol) і OSPF (Open Shortest Path First), а також протокол міжмережних керуючих повідомлень ICMP (Internet Control Message Protocol). Останній протокол призначений для обміну інформацією про помилки між маршрутизаторами мережі і вузлом - джерелом пакета. За допомогою спеціальних пакетів ICMP повідомляється про неможливість доставки пакета, про перевищення часу життя або тривалості складання пакета із фрагментів, про аномальні величини

параметрів, про зміну маршруту пересилання і типу обслуговування, про стан системи та т.і.

Наступний рівень (рівень II) називається основним. На цьому рівні функціонують протокол керування передачею TCP (Transmission Control Protocol) і протокол дейтаграм користувача UDP (User Datagram Protocol). Протокол TCP забезпечує надійну передачу повідомлень між вилученими прикладними процесами за рахунок утворення віртуальних з'єднань. Протокол UDP забезпечує передачу прикладних пакетів дейтаграмним способом, як і IP, і виконує тільки функції сполучної ланки між мережним протоколом і численними прикладними процесами.

Верхній рівень (рівень I) називається прикладним. За довгі роки використання в мережах різних країн і організацій стек TCP/IP нагромадив велику кількість протоколів і сервісів прикладного рівня. До них ставляться такі широко використовувані протоколи, як протокол копіювання файлів FTP, протокол емуляції термінала telnet, поштовий протокол SMTP, використовуваний в електронній пошті мережі Internet, гіпертекстові сервіси доступу до вилученої інформації, такі як WWW і багато хто інші. Зупинимося трохи докладніше на деякі з них.

Протокол пересилання файлів FTP (File Transfer Protocol) реалізує вилучений доступ до файлу. Для того, щоб забезпечити надійну передачу, FTP використовує як транспорт протокол із установленням з'єднань - TCP. Крім пересилання файлів протокол FTP пропонує і інші послуги. Так, користувачеві надається можливість інтерактивної роботи з вилученою машиною, наприклад, він може роздрукувати вміст її каталогів. Нарешті, FTP виконує аутентифікацію користувачів. Перш, ніж одержати доступ до файлу, відповідно до протоколу користувачі повинні повідомити своє ім'я і пароль. Для доступу до публічних каталогів FTP-Архівів Internet парольна аутентифікація не потрібна, і неї обходять за рахунок використання для такого доступу визначеного ім'я користувача Anonymous.

У стеці TCP/IP протокол FTP пропонує найбільш широкий набір послуг для роботи з файлами, однак він є і самим складним для програмування.

Додатки, яким не потрібні всі можливості FTP, можуть використовувати інший, більше економічний протокол - найпростіший протокол пересилання файлів TFTP (Trivial File Transfer Protocol). Цей протокол реалізує тільки передачу файлів, причому як транспорт використовується більше простій, чим TCP, протокол без установлення з'єднання - UDP.

Протокол telnet забезпечує передачу потоку байтів між процесами, а також між процесом і терміналом. Найбільше часто цей протокол використовується для емуляції термінала віддаленого комп'ютера. При використанні сервісу telnet користувач фактично управляє віддаленим комп'ютером так само, як і локальний користувач, тому такий вид доступу вимагає гарного захисту. Тому сервери telnet завжди використовують як мінімум аутентифікацію по паролі, а іноді і могутніші засоби захисту, наприклад, систему Kerberos.

Протокол SNMP (Simple Network Management Protocol) використовується для організації мережного керування. Споконвічно протокол SNMP був розроблений для вилученого контролю і керування маршрутизаторами Internet, які традиційно часто називають також шлюзами. З ростом популярності протокол SNMP стали застосовувати і для керування будь-яким комунікаційним обладнанням - концентраторами, мостами, мережними адаптерами та т.і. Проблема керування в протоколі SNMP розділяється на дві задачі.

Перша задача пов'язана з передачею інформації. Протоколи передачі керуючої інформації визначають процедуру взаємодії SNMP-Агента, що працює в керованому обладнанні, і SNMP-Монітора, що працює на комп'ютері адміністратора, що часто називають також консоллю керування. Протоколи передачі визначають формати повідомлень, якими обмінюються агенти й монітор.

Друга задача пов'язана з контрольованими змінними, що характеризують стан керованого пристрою. Стандарти регламентують, які дані повинні зберігатися і накопичуватися в пристроях, імена цих даних і синтаксис цих імен. У стандарті SNMP визначена специфікація

інформаційної бази дані керування мережею. Ця специфікація, відома як база даних MIB (Management Information Base), визначає ті елементи даних, які керований пристрій повинне зберігати, і припустимі операції над ними.

2.4 Операційні системи

Операційна система найбільшою мірою визначає вигляд всієї обчислювальної системи в цілому. Незважаючи на це, користувачі, що активно використовують обчислювальну техніку, найчастіше зазнають труднощів при спробі дати визначення операційній системі. Частково це пов'язане з тим, що ОС виконує дві по суті мало зв'язані функції: забезпечення користувачеві-програмістові зручностей за допомогою надання для нього розширеної машини і підвищення ефективності використання комп'ютера шляхом раціонального керування його ресурсами.

Операційні системи можуть різнитися особливостями реалізації внутрішніх алгоритмів керування основними ресурсами комп'ютера (процесорами, пам'яттю, пристроями), особливостями використаних методів проектування, типами апаратних платформ, галузями використання і багатьма іншими властивостями.

Розглянемо більш докладно можливості деяких мережних операційних систем і вимоги, які вони пред'являють до програмного і апаратного забезпечення пристроїв мережі.

Windows 2008 (Server), Microsoft Corp.

Відмітні риси:

– простота інтерфейсу користувача;

– доступність засобів розробки прикладних програм і підтримка прогресивних обьєктно-орієнтованих технологій

Все це привело до того, що ця операційна система може стати однієї із самих популярних мережних операційних систем.

Інтерфейс нагадує віконний інтерфейс Windows 7, інсталяція займає близько 40 хвилин. Модульна побудова системи спрощує внесення змін і перенос на інші платформи. Забезпечується захищеність підсистем від несанкціонованого доступу і від їхнього взаємного впливу (якщо зависає один процес, це не впливає на роботу інших). Є підтримка вилучених станцій - Remote Access Service (RAS).

Windows Server пред'являє більше високі вимоги до продуктивності комп'ютера в порівнянні з Linux.

Основні характеристики і вимоги до апаратного забезпечення.

- центральний процесор: 2ГГц і вище;
- мінімальний обсяг жорсткого диска: 40 Гбайт;
- мінімальний обсяг ОП на сервері: 4 Гбайт;
- мінімальний обсяг ОП РС клієнта; 2 Гбайт;
- протоколи: NetBEUI, TCP/IP, IPX/SPX, Appletalk, AsyncBEUI;
- мультипроцесорність: підтримується;
- кількість користувачів: необмежено;
- максимальний розмір файлу: необмежений;
- шифрування даних: рівень С-2;
- монітор UPS;
- керування розподіленими ресурсами мережі: домени.
- система відмовостійкості: дублювання дисків, дзеркальне відбиття дисків, RAID 5, підтримка накопичувача на магнітній стрічці, резервне копіювання таблиць домена і даних.
- стиснення даних: є.
- фрагментація блоків (Block suballocation): немає.
- файлова система клієнтів:Windows, Mac, OS/2, UNIX, Windows NT.

Операційна система Linux

Linux підтримує різні типи файлових систем для зберігання даних. Деякі файлові системи, такі як файлова система ext2fs, були створені спеціально для Linux. Цією ОС підтримуються також інші типи файлових

систем, такі як Minix-1 і Xenix. Реалізована також файлова система NTFS, що дозволяє прямо звертатися до файлів MS Windows на жорсткому диску. Підтримується також файлова система ISO 9660 CD-ROM для роботи з дисками CD-ROM.

Linux забезпечує повний набір протоколів TCP/IP для мережної роботи. Це включає драйвери пристроїв для багатьох популярних карт Ethernet, SLIP (Serial Line Internet Protocol, що забезпечують вам доступ по TCP/IP при послідовному з'єднанню), PLIP (Parallel Line Internet Protocol), PPP (Point-to-Point Protocol), NFS (Network File System), і так далі. Підтримується весь спектр клієнтів і послуг TCP/IP, таких як FTP, telnet, NNTP і SMTP. Linux забезпечує "гладкий" інтерфейс для обміну файлами між Linux і MS-DOS. Є можливість підключити розділ MS-Windows або гнучкий диск під Linux і мати прямий доступ до файлів MS Windows, як і до "рідних".

Як уже говорилося вище, даний сервер призначений для забезпечення доступу користувацьких ПК в інтернет.

Internet це всесвітня комп'ютерна мережа. На 1 жовтня 2004 року вона містила 6 898 233 комп'ютера. Темпи розвитку Internet виявилися настільки великі, що до 2010 року кількість користувачів перевищила 100 000 000.

Internet містить величезну кількість даних на які завгодно теми і надає широкий спектр послуг для одержання інформації. Особливу популярність завоював сервіс Internet, т.зв. "всесвітня павутина" WWW (World Wide Web). Для доступу до цього сервісу створений ряд програм-клієнтів, таких як Mosaic, Netscape, Opera і ін. Ці клієнти у вигляді як вільних, так і комерційних версій реалізовані для великої кількості платформ, у т.ч. Linux і MS Windows. Система WWW складається з великої кількості програм-серверів, що виконуються на машинах мережі Internet.

Спільно сервери WWW утворюють єдину розподілену базу даних мережного мультимедиа гіпертексту. Сервер наповнюється інформацією на яку-небудь тему, включаючи образи фотографій, картин і музики, звуків, мови. Далі користувач через мережу Internet за допомогою програми-браузера (browser) у себе на машині звертається до цього сервера по його

адресі в мережі. Користувач бачить вступний текст, у якому, як і має бути гіпертекстовій системі, виділені деякі ділянки тексту. Досить клацнути по виділеній ділянці мишкою і розкриється його зміст.

Linux підтримує стандарти відкритих систем. В Linux є велика кількість інструментальних пакетів, за допомогою яких реалізується прикладна система клієнт-сервер. Це СУБД, будівельники графічних інтерфейсів та ін. Ці пакети вільні, поставляються у вихідних текстах. Вони генеруються з вихідних текстів як для Linux, так і для десятків інших платформ, у т.ч. комерційних - Solaris, SCO, BSD.

X Window System (X Windows) це оконно-графічна система клієнт/сервер використовувана в Linux.

Сервер X Windows виконується на машині, де потрібно відображати інформацію. Часто до одній машині підключено один дисплей, але буває і декілька. На одній машині може працювати кілька серверів, кожний з яких обслуговує свій дисплей. Дисплей це клавіатура, мишка, планшет і т.п. у зв'язуванні з монітором або декількома моніторами (наприклад, звичайним і більшим графічним). У системах DOS і MS Windows існує підтримка протоколів TCP/IP, що дозволяє виконувати програми-клієнти, які через мережу TCP/IP взаємодіють із Linux і дозволяють завантажуватися в Linux, обмінюватися файлами, електронною поштою і новинами, монтувати файли через мережну файлову систему NFS (комерційні PCNFS, PCTCP, WATTCP, Winqvt, WINARCH, Einet winwais, вільні Winvn, WS_FTP, NCSA Telnet, NCSA Mosaic). В Linux існують відповідні програми-сервери.

В Linux є сервер Samba, який дозволяє програмам-клієнтам через протокол SMB (Session Message Block) одержати доступ до файлової системи Linux і принтеру, що працює в Linux. Це такі клієнти як Lanmanager для DOS, Windows for Workgroups, Windows NT, OS/2, Pathworks і багато інші. У пакет Samba входить і програма-клієнт, яка дозволяє одержати з Linux доступ до файлів і принтеру в Windows for Workgoups, OS/2. Протокол SMB виконується поверх протоколу TCP/IP.

Ubuntu — операційна система для робочих станцій, лептопів і серверів, є найпопулярнішим у світі дистрибутивом Linux. Серед основних цілей Ubuntu — надання сучасного і водночас стабільного програмного забезпечення для пересічного користувача із сильним акцентом на простоту встановлення і користування [1].

Ubuntu надає користувачу мінімальний набір програм загального призначення: багатовіконне стільничне середовище, засоби для перегляду Інтернету, організації електронної пошти, офісні програми з можливістю читати і записувати файли в форматі Microsoft Office, редактор зображень, програвач компакт-дисків тощо. Спеціалізоване програмне забезпечення, потрібне досвідченішим користувачам, можна отримати із відповідних репозиторіїв. Серверний варіант системи включає також засоби, потрібні для організації сервера баз даних, веб-сервера, сервера електронної пошти, тощо.

Ubuntu побудований на основі Debian GNU/Linux — іншого популярного дистрибутиву Лінукс. Спонсорується Canonical Ltd., власником якої є бізнесмен із ПАР Марк Шаттлворт. Назва дистрибутиву походить від зулуської концепції «убунту», яку можна висловити приблизно, як «людяність». Дистрибутив так названий з метою популяризації духу цієї філософії у світі програмного забезпечення. Ubuntu належить до вільного програмного забезпечення і може безкоштовно передаватись будь-якій кількості користувачів.

Офіційні підпроекти Kubuntu та Xubuntu використовують у якості основних стільничні середовища KDE та Xfce замість GNOME, який встановлюється за замовчуванням в дистрибутивах основного проекту. Інший офіційний підпроект, Edubuntu, розробляється для шкіл і використання дітьми вдома. Gobuntu є офіційним підпроектом, в якому використовується винятково вільне програмне забезпечення. Новим офіційним підпроектом є JeOS (вимовляється «Джюс»), створений для використання на віртуальних машинах.

Нові версії виходять кожні шість місяців. Кожен реліз Ubuntu підтримується оновленнями служб безпеки протягом 18 місяців. Випуски

LTS (*Long Term Support* — довгострокова підтримка), які виходять кожні два роки, підтримуються протягом трьох років для десктопів і п'яти для серверів. Останній LTS випуск, Ubuntu 14.01 LTS *(Lucid Lynx)*, датується 26-им березням 2014 року.

Враховуючи наведені властивості і можливості мережних ОС різних типів, можна дійти висновку, що найбільш потужним інструментом для контролю і керування процесами передачі інформації є Linux. Ця ОС найбільше підходить для побудови інтернет-сервера. Єдиним недоліком цієї ОС є складність взаємодії з користувачем, що не має спеціальної підготовки. Тому із цим для організації серверів баз даних будемо використовувати ОС Windows 2008. Гарна стійкість цієї ОС і великий набір інструментів контролю доступу робить її найбільш підходящої для розподілу і зберігання даних.

Отже, структура проектованої мережі така: до інтернет-серверу, керованому ОС Linux, за допомогою магістрального каналу 1Gbit/s по топології логічного кільця підключено два двадцятичотирьохпортових комутатора, до одному з них (підмережа “відділення №1”) підключено 9 машин, до другого (підмережа “відділення №2”) підключено 16 машин. У кожній підмережі організований власний сервер автоматизованої банківської системи працюючий під керуванням Ubuntu 12.04 Server Edition.

3 РОЗРОБЛЕННЯ РОЗПОДІЛЕНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ

У даному розділі дипломного проекту виконано розробку топології мережі, вибір апаратного і програмного забезпечення локальної мережі відділень Лисичанської філії ВАТ КБ "Райффайзен Банк Аваль".

3.1 Проектування мережі

3.1.1 Структура мережі та її топологія

Як уже вказувалося у технічному завданні, розроблювальна мережа розбита на дві підмережі, така побудова диктується необхідністю забезпечити роботу мережі в різних приміщеннях і скоротити довжину ліній зв'язку, але при цьому не втратити взаємозв'язок між комп'ютерами різних відділів. Ще одним важливим фактором є забезпечення основних потоків даних у підмережах обох відділень. Основні потоки даних:

– базова підсистема АБС "Операційний день банку" виконує наступні основні:

1) введення та обробка клієнтських платіжних документів;
2) створення та ведення особових рахунків клієнтів та масивів нормативно-довідкової інформації;
3) робота з картотеками;
4) обробка особових та балансових рахунків;
5) ведення аналітичного і синтетичного обліку, формування балансу за кожний банківський день та відповідних вихідних форм;
6) сервісні функції: відкриття, закриття та протоколювання банківського дня, встановлення лімітів, бізнес-правил для філій банку тощо.;

– в межах підсистеми "Управління кредитними ресурсами банку" працівники кредитного відділу банку мають можливість виконувати такі основні функції:

1) аналіз фінансового стану позичальника, визначення його кредитоспроможності та оцінка ризику при кредитуванні;
2) формування та облік кредитних договорів;
3) ведення та коригування розпоряджень на оплату кредитів;
4) ведення та коригування строкових зобов’язань на погашення кредиту;
5) ведення та коригування процентних ставок та графіків оплати процентів по кредитному договору;
6) нарахування процентів по кредиту та облік їх сплати;
7) облік та контроль погашення кредитної заборгованості;
8) аналіз кредитного портфеля, класифікація кредитів та визначення розміру резервування;

– підсистема "Управління депозитами" виконує наступні функції:

1) облік операцій з готівкою, облік безготівкових операцій;
2) облік цінних бланків;
3) нарахування відсотків за депозитними рахунками;
4) формування звітних форм щодо роботи з депозитними вкладами;

– підсистема "Каса" являє собою міні-банк, що має свій баланс, рахунки і документацію, у якій відображаються готівкові кошти. В підсистемі виконуються такі основні функції:

1) ведення довідника касових символів;
2) ведення та обробка прибуткових касових документів;
3) ведення та обробка видаткових касових документів;
4) формування та ведення касового журналу;
5) формування звітних форм з обліку роботи каси.

– підсистема «Аналіз діяльності банку» акумулює у своєму складі аналітичні задачі, які належать до класу OLAP. До основних аналітичних задач підсистеми можна віднести:

1) аналіз балансу (агрегованого та в розрізі класів, розділів, груп і балансових рахунків);
2) аналіз пасивів банку (структура пасивів, структура власних коштів, структура залучених коштів);
3) аналіз активів банку (структура активів, структура кредитного портфеля);
4) аналіз нормативів банку (ліквідність, платоспроможність, достатність капіталу тощо);
5) аналіз доходів, видатків та прибутку банку (нарахування і фактично отримані доходи, рентабельність, доходи від банківських послуг, прибутковість банку);
6) аналіз виконання фінансового плану доходів та витрат;
7) аналіз та контроль формування і використання фондів банку.

– передача даних із ПК секретаря обом підмережам. Секретар веде первинну обробку і сортування вхідних документів (пошта, електронна пошта, доручення, накази, новини ГБ та ін.), а після цього передає їх по призначенню у відповідну підмережу;

– загальний контроль за роботою установи. Директор філії має можливість контролювати дії працівників двох відділень, спостерігаючи за процесами за допомогою режиму "директор" підсистем АБС. ПК директора є клієнтом для обох серверів - і АБС-серверу та інтернет-серверу.

– підключення філії до корпоративної мережі ВАТ КБ "Райффайзен Банк Аваль" засобами мережі інтернет. Всі робочі місця обох підмереж (відділень) повинні бути забезпечені виходом у мережу інтернет через відповідний сервер.

Комп'ютери всіх користувачів мережі мають доступ до ресурсів інтернет. Підключення до глобальної мережі забезпечується за допомогою інтернет-сервера.

Сервер побудований на основі персонального комп'ютера із процесором Intel Pentium Dual-Core E5000. Сервер управляється операційною системою Linux і призначений для забезпечення і контролю доступу користувальницьких комп'ютерів в інтернет.

Однак у зв'язку з тим, що інтенсивність використання цих ресурсів відрізняється залежно від виду діяльності працівника, то для кожного з них застосовуються різні настроювання підключення. У них задаються:

- обмеження швидкості доступу;
- можливість "завантаження" блоків інформації певного типу;
- можливість користування електронною поштою;
- нормування обсягів отриманої інформації (у добу);
- доступ до FTP ресурсів і ін.

Структура розробленої локальної мережі древовідної топології відповідно до цих вимог і обмеженнями представлена на рис 3.1, 3.2.

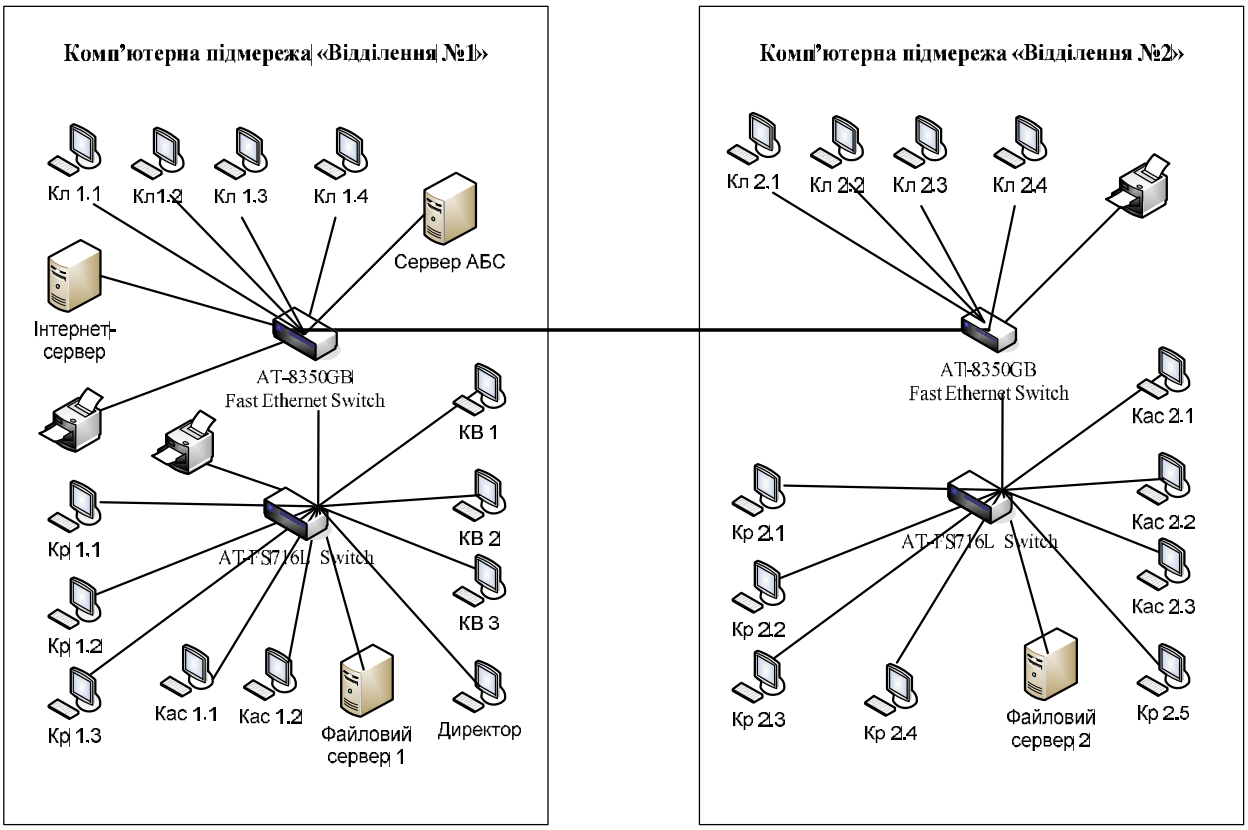

Рисунок 3.1 - Структура підмереж Лисичанської філії ВАТ КБ "Райффайзен Банк Аваль"

3.1.2 Безпека при роботі в мережі інтернет

Інформація, що зберігається на жорстких дисках комп'ютерів, має комерційний характер. Оскільки витік інформації подібного типу - явище вкрай небажане, то для забезпечення безпеки прийнятий ряд мер.

Ряд служб TCP і UDP погано забезпечують безпеку в сучасному середовищі в інтернет. При мільйонах користувачів, підключених до інтернет, недоліки в цих службах, а також легкодоступність вихідного коду і засобів для автоматизації проникнення в системи можуть зробити мережі уразливими до проникнень у них. Проте, справжній ризик при використанні Інтернету важко оцінити, і непросто сказати, наскільки уразлива мережа.

Мережі, які з'єднані з мережею інтернет, піддаються деякому ризику того, що їхні системи будуть атаковані або піддані деякому впливу з боку.

Наступні фактори можуть вплинути на рівень ризику:

– число систем у мережі;

– які служби використовуються в мережі ;

– яким образом мережа з'єднана з Інтернетом;

– профіль мережі, або наскільки відомо про її існування;

– наскільки готова організація до улагоджування інцидентів з комп'ютерною безпекою.

Для підвищення рівня безпеки найбільше часто використовують брандмауер. брандмауер - це не просто маршрутизатор, хост або група систем, які забезпечують безпека в мережі. Брандмауер - це скоріше не засіб забезпечення, а підхід до безпеки; він допомагає реалізувати політику безпеки, що визначає дозволені служби і типи доступу до них, і є реалізацією цієї політики в термінах мережної конфігурації, декількох хостів і маршрутизаторів, і інших мір захисту, таких як посилена аутентифікація замість статичних паролів. Основна мета системи брандмауера - керування доступом “до” або “з” захищаємої мережі. Він реалізує політику мережного доступу, змушуючи проходити всі з'єднання з мережею через брандмауера, де вони можуть бути проаналізовані і дозволені або відкинуті. Основною причиною використання брандмауерів є той факт, що без брандмауера системи підмережі піддаються небезпеки використання уразливих місць служб, таких NFS і NIS, або сканування і атак з боку хостів в Інтернеті.

Основними компонентами брандмауера є:

– політика мережного доступу;

– механізми посиленої аутентификации;

– фільтрація пакетів ;

– прикладні шлюзи.

Отже, політика і засоби забезпечення безпеки доступу з локальної мережі в до корпоративної мережі та інтернет (і в зворотному напряму) полягає в наступному:

– кожний користувач має унікальний пароль, по якому сервер розпізнає власника і дає доступ тільки до тих виділеним інформаційним ресурсам, що зберігаються на жорстких дисках сервера, до яких цей пароль дає доступ;

– способу, одержати доступ, до інформації локальної мережі, із зовнішньої мережі немає. Кожний користувач може одержати доступ із зовнішньої мережі тільки до тих даним, які він помістив на сервер, але тільки шляхом зазначеним вище;

– всі пакети, що вивантажуються в зовнішню мережу, контролюються програмою-сторожем, що функціонує нероздільно з ОС сервера. Її зупинка веде до руйнування всякого з'єднання із зовнішньою мережею.

Система захисту файлів платіжно-інформаційного потоку реалізована спеціальними програмно-апаратними засобами, котрі становлять комерційну таємницю та не входять до розгляду в рамках даного дипломного проекту. Маємо можливість перелічити лиш деякі з них:

– програмно-апаратна з застосуванням зовнішнього носія (таємний ключ криптосистеми) для входу в АРМ міжфілійних платежів;

– легітимність та криптозахист сформованого платіжного документа на базі 2-рівневого «електронного цифрового підпису» (ЕЦП) операторів та контроль-бухгалтера міжфілійних платежів;

– шифротрафік файлів міжфілійних платежів з застосуванням автоматичних ПЕОМ шифрошлюзів з симетричним типом шифрування потоків, направляємих через IP-мережі «Укртелекому» (VPN з IP – адресацією) чи IP-мережі Національного банку України (FOSS-MAIL – технологія)

3.2 Фізична реалізація мережі

Засоби локальної мережі Лисичанської філії ВАТ КБ "Райффайзен Банк Аваль" установлюється на перших поверхах житлових будівель, котрі переобладнані під офіси. Висота поверху становить 3.5 м, загальна товщина перекриттів дорівнює 51 см. Стіни приміщень виготовлені зі звичайної цегли і покриті штукатуркою, товщина якої становить 1 см. У ході проектування було розглянуто кілька варіантів архітектури кабельної системи, і обраний варіант як оптимальний за вартістю, так і найбільш зручний з погляду наступного адміністрування

Створювана кабельна мережа повинна забезпечити функціонування локальної мережі фінансової установи і, якщо це буде вимагатися, телефонної мережі будинку, тобто, на кожному робочому місці монтується інформаційна розетка із двома розеточними модулями, надмірність розеточних модулів забезпечить у майбутньому необхідну масштабованість і зростання системи. Внутрішня мережа телефонізації і внутрішня комп'ютерна мережа проектується як єдине ціле, як частина кабельної системи. Підсистема робочого місця складається з необхідної кількості універсальних портів RJ-45 і сполучних кабелів для підключення кінцевого мережного обладнання.

Загальне число робочих місць, визначається технічним завданням, виданим керівництвом підприємства - разом 32 робочих місць (64 універсальних портів RJ-45). Ця цифра відповідає кількості наявних на підприємстві ПЕОМ. При проектуванні кабелі ЛОМ будуть також заведені в приміщення, де в цей момент немає ПЕОМ, такі місця відзначені на схемі іншим позначенням. Це збільшить гнучкість системи до модернізацій і переміщення персоналу. Такі робочі місця будуть установлені, але не підключені до загальної кабельної мережі. Якщо буде потреба простою комутацією на кросі ці місця будуть наведені в повну працездатність. У приміщеннях, у яких розташовуються кабінети керівництва та сервісні

центри число робочих місць визначалося виходячи з необхідної кількості портів, і воно не завжди збігається з розрахунковим, тому що при розрахунку по площі в кабінетах керівництва і залах роботи з клієнтами виходить надмірна надмірність портів і розташування їх по кабінеті, тому в таких приміщеннях розетки встановлені поруч один з одним, щоб забезпечити підключення більшої кількості телекомунікаційного обладнання на одному робочому місці. Таблиця 3.1 показує кількість робочих місць мережі передачі даних в кожному відділенні.

Таблиця 3.1 - Кількість робочих місць на кожному поверсі будинку

Відділення	Кількість робочих місць	Кількість універсальних портів
Відділення №1	12	24
Відділення №2	20	40
Загальна кількість робочих місць	32	64

Розведення кабелю, розподіли робочих місць і обладнання кабельної системи знаходяться на кресленнях, прикладених до проекту.

Детальний опис кабельної системи і ЛОМ на її основі представлено нижче.

Проектована система складається з наступних підсистем:

- підсистема робочого місця;
- горизонтальна підсистема;
- вертикальна підсистема;
- підсистема керування;
- підсистема обладнання;
- зовнішня підсистема.

3.2.1 Підсистема робочого місця

Підсистема робочого місця містить у собі необхідна кількість універсальних портів на базі уніфікованих з'єднувачів RJ45 і/або оптичних з'єднувачів для підключення кінцевого обладнання.

Проектом передбачене використання наступних конфігурацій робочих місць:

- РМ - просте робоче місце, обладнається двома розетками RJ-45, двома розетками безперебійного або двома розетками стабілізованого електроживлення або їхньою комбінацією;
- РМС - робоче місце сервісного центру, обладнається чотирма розетками RJ-45, двома розетками безперебійного й двома розетками стабілізованого електроживлення;

Кількість робочих місць узято з урахуванням специфікації приміщення і задач на розміщення робочих місць. Точка установки робочого місця в процесі експлуатації може бути без особливих витрат пересунена уздовж короба. Для цієї мети необхідно залишити в кожної розетки петлю запасу кабелю близько 1м.

3.2.2 Горизонтальна підсистема

Горизонтальна підсистема забезпечує з'єднання робочих місць із комутатором. Виконана 4-х парним кабелем типу "неекранована кручена пари" категорії 5, з наступними характеристиками:

Опір	9.38 Ом/100м
Ємність	4.59 нФ/100 м на частоті 1 кГц

Усе кабельне і комутаційне обладнання, застосовуване в проекті, задовольняє вимогам 5 категорії міжнародного стандарту EIA/TIA-568A, а

також вимогам Underwriters Laboratories (UL) США по електробезпечності та технічним характеристикам.

Необхідна кількість кабелю розраховується з використанням наступного емпіричного методу. Виходячи із припущення, що робочі місця розподілені по площі, що обслуговується, рівномірно, обчислюється середня довжина (Lcp) кабельних трас по формулі:

$$Lcp = (Lmax + Lmin)/2, \quad (3.1)$$

де: Lmin і Lmax – відповідно, довжини кабельної траси від точки розміщення комутаційного обладнання до інформаційного з'єднувача найближчого і самого далекого робочого місця, полічені з урахуванням технології прокладки кабелю, усіх спусків, підйомів, поворотів і особливостей будівлі

При визначенні довжини трас необхідно додати технологічний запас величиною 10% від Lcp і запас X для процедур розведення кабелю в розподільному вузлі і інформаційному з'єднувачі; так що довжина трас L складе:

$$L = (1{,}1Lcp + X) \times N, \quad (3.2)$$

де: N – кількість розеток на поверсі

На жаль, у даному проекті цей метод розрахунків не можна застосувати через нерівномірне розташування робочих місць по площі. У деяких робочих кабінетах у наявності висока щільність робочих місць, що приведе до помилок у розрахунках кількості кабелю, тому довжина кабелю обчислюється як сума довжин відрізків кабелю від головного кросу до кожного робочого місця і до отриманої суми додаються технологічний запас і запас на розведення в робочому місці.

Кількість кабелю, необхідне для кожної будівлі.

Для першої будівлі:

L =31+34+29+28+15+15= 124м.;

Для другої будівлі

L=40+37+34+31+34+31+27+25+44+41+39+36+37+40+42+45= 518м.

Оскільки кожне робоче місце складається із двох розеток RJ-45 і, враховуючи технологічний запас кабелю і запас кабелю на розведення і можливе переміщення робочого місця, загальна довжина кабелю складе:

$L_{заг}$ = ((124+518) ×2) ×1,1= 1285,2 метри.

Відомо, що в бухті 305 метрів кабелю. Тоді для створення кабельної підсистеми необхідно 5 бухти, або метрів 1525 кабелю.

Прокладання кабелів горизонтальної підсистеми на поверхах здійснюється в пластиковому коробі, між поверхами в металевому коробі:

- вертикальний стояк – металевий короб 100х60мм;
- горизонтальна прокладка;
- пластиковий короб 100×60 мм – 1 шт на кожні 30 кабелів UTP;
- металевий короб 100х60мм – для з'єднання вертикального стояка із серверної в першої будівлі;
- спуски до робочих місць і розведення усередині кабінетів – пластиковий короб 100×40 мм.

Необхідна кількість коробів мною розраховане по робочих кресленнях і становить:

Для першої будівлі:

L_{40}=13,7+7+13+14+6+3,5+3,5+2=62 метра.

L_{60}=13,5=13,5 метрів.

Для другої будівлі:

L_{40}=14+3,5+0,5+6+8+7+5+4+11+6+4,5+2=70,5 метра.

L_{60}=9+8,7=17,7 метрів.

Загальна кількість коробів необхідна для монтажу:

L_{40}=132,5 метрів.

L_{60}=24,2 метра.

Сегменти кабелю закінчується розетками, що вбудовуються в короб, RJ-45, здатними підключати також телефонні конектори RJ-11. Для підключення обладнання робочих місць система укомплектовується патч-кордами довжиною 3 і 5м.

Комплектування комп'ютерів користувачів мережними картами даним проектом не розглядалося, тому що в наявних ПЕОМ є або інтегровані або мережні карти, що вбудовуються, які підтримують обрану топологію і швидкість передачі даних.

3.2.3 Вертикальна підсистема

Вертикальна підсистема дозволяє поєднувати в уніфіковану мережу дві будівлі. Допускає застосування мідних кручених пар і волоконо-оптичного кабелю. Забезпечує з'єднання пристроїв зв'язки і комутації комп'ютерної мережі.

У даному проекті вертикальна підсистема зведена до мінімуму. Складається з одного оптичного патч-корду SX, що з'єднує два комутатори (AT-8350GB Fast Ethernet Switch) через порт Gigabit-sx.

Вибір комутатора даного типу обумовлений наявністю порту Gigabit, високими технічними показниками, такими як довічна гарантія, високоякісна елементна база, висока перешкодозахищеність, низьке енергоспоживання, прийнятна ціна.

3.3 Розрахунки технічних характеристик ЛОМ

Для того, щоб мережа Ethernet працювала коректно, необхідно, щоб виконувалися три основні умови:

– кількість станцій у мережі не перевищує 1024.

– подвоєна затримка поширення сигналу (Path Delay Value, PDV) між двома самими вилученими друг від друга станціями мережі не перевищує 575 бітових інтервалів.

– скорочення міжкадрової відстані (Interpacket Gap Shrinkage) при проходженні послідовності кадрів через усі повторювачі не більш, ніж на 49 бітових інтервалів.

Дотримання цих вимог забезпечує коректність роботи мережі навіть у випадках, коли порушуються прості правила конфігурування, що визначають максимальну кількість повторювачів і максимальну довжину сегментів кожного типу.

Фізичний зміст обмеження затримки поширення сигналу по мережі вже пояснювався - дотримання цієї вимоги забезпечує своєчасне виявлення колізій.

Вимога на мінімальну міжкадрову відстань пов'язана з тим, що при проходженні кадру через повторювач ця відстань зменшується. Кожний пакет, прийнятий повторювачем, ресинхронизується для виключення тремтіння сигналів, накопиченого при проходженні послідовності імпульсів по кабелю і через інтерфейсні схеми. Процес ресинхронизації звичайно збільшує довжину преамбули, що зменшує міжкадровий інтервал. При проходженні кадрів через кілька повторювачів міжкадровий інтервал може зменшитися настільки, що мережним адаптерам в останньому сегменті бракуватиме часу на обробку попереднього кадру, у результаті чого кадр буде просто загублений. Тому не допускається сумарне зменшення міжкадрового інтервалу більш ніж на 49 бітових інтервалів. Величину

зменшення міжкадрової відстані при переході між сусідніми сегментами звичайно називають в англомовній літературі Segment Variability Value, SVV, а сумарну величину зменшення міжкадрового інтервалу при проходженні всіх повторювачів - Path Variability Value, PVV. Очевидно, що величина PVV дорівнює сумі SVV усіх сегментів, крім останнього.

Розрахунки PDV

Для спрощення розрахунків звичайно використовуються довідкові дані, що містять значення затримок поширення сигналів у повторювачах, прийомопередатчиках і в різних фізичних середовищах. У таблиці 3.2 наведені дані, необхідні для розрахунків значення затримки поширення сигналу PDV для всіх фізичних стандартів мереж Ethernet, узяті з довідника Technical Reference Pocket Guide (Volume 4, Number 4) компанії Bay Networks.

Таблиця 3.2 – Технічні характеристики сегментів Ethernet

Тип сегмента	База левого сегмента, біт	База проміжного сегмента, біт	База правого сегмента, біт	Затримка середовища на 1 м, біт/м	Максимальна довжина сегмента, м
10Base-5	11.8	46.5	169.5	0.0866	500
10Base-2	11.8	46.5	169.5	0.1026	185
10Base-T	15.3	42.0	165.0	0.113	100
10Base-fb	-	24.0	-	0.1	2000
10Base-fl	12.3	33.5	156.5	0.1	2000
FOIRL	7.8	29.0	152.0	0.1	1000

Лівим сегментом називається сегмент, у якому починається шлях сигналу від виходу передавача (вихід Tx) кінцевого вузла. Потім сигнал проходить через проміжні сегменти і доходить до приймача (вхід Rx) найбільш вилученого вузла найбільш вилученого сегмента, який називається правим. З кожним сегментом зв'язана постійна затримка, названа базою, яка залежить тільки від типу сегмента й від положення сегмента на шляху сигналу (лівий, проміжний або правий). Крім цього, з кожним сегментом

зв'язана затримка поширення сигналу уздовж кабелю сегмента, яка залежить від довжини сегмента й обчислюється шляхом множення часу поширення сигналу по одному метру кабелю (у бітових інтервалах) на довжину кабелю в метрах.

Загальне значення PDV дорівнює сумі базових і змінних затримок усіх сегментів мережі. Значення констант у таблиці дані з урахуванням подвоєння величини затримки при круговому обході мережі сигналом, тому подвоювати отриману суму не потрібно.

Найбільш вилученими робочими місцями є ПК економіста (розташований в комерційному відділі в першого відділення) і ПК каси (розташований на касовій залі №2 в другому відділенні). Спрощена схема сегмента мережі наведено на рис.3.2.

Лівий і правий сегменти підключені до 10Base-T, а один проміжний сегмент – до GigabitEthernet, тому значення PDV в обоє напрямки однакові.

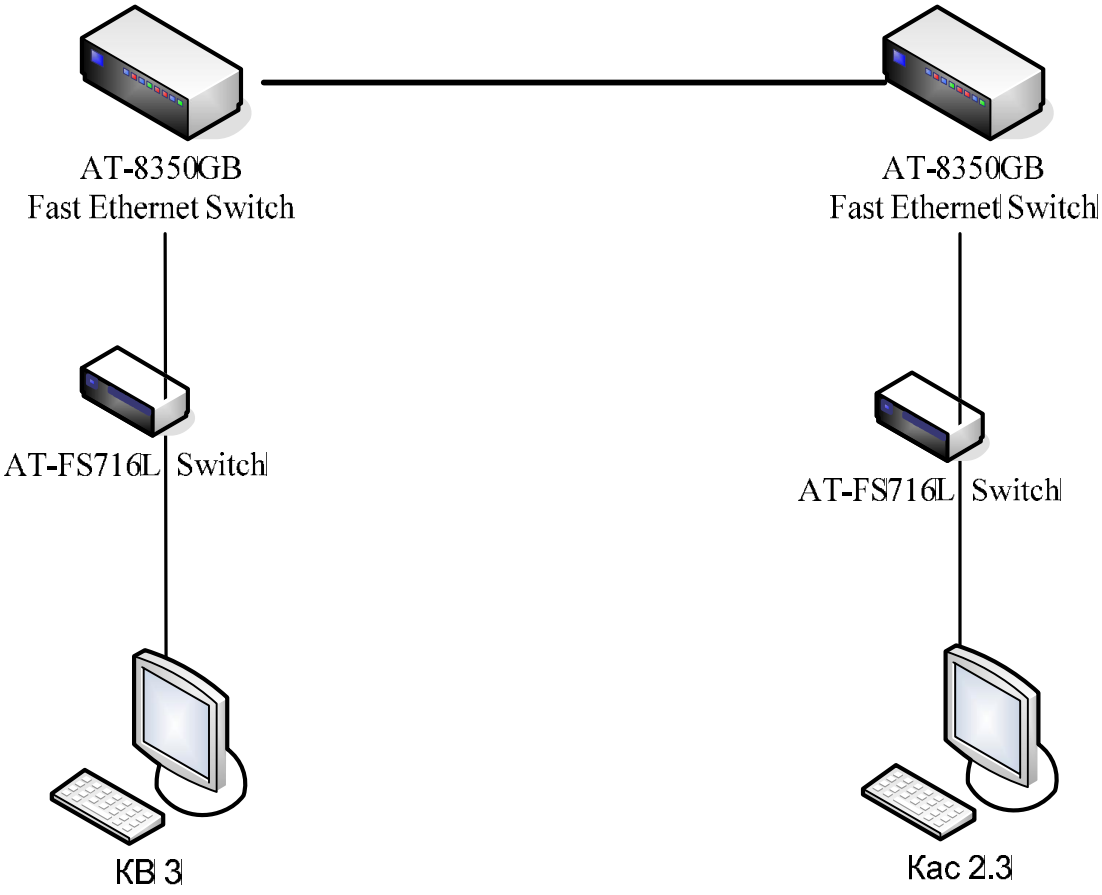

Рисунок 3.2 – Сегмент проектованої ЛОМ для розрахунків PDV

Розрахуємо значення PDV для сегмента проектованої мережі. Передбачається, що сегмент має максимальну довжину зі схожих сегментів і містить приймач/передавач сигналу на своїх кінцях. Якщо ж одним з елементів сегмента виступає ЕОМ, що містить кілька мережних адаптерів, що виконують функцію мосту ЛОМ, то в цьому випадку слід розділити сегмент на частині, виділивши окремо додатковий проміжний сегмент.

а) лівий сегмент (10Base-T): база 15,3 біт; кабель 37м * 0,113біт/м = 4,18 біт;

б) проміжний сегмент (GigabitEthernet): база 33,5 біт; кабель 7м * 0,1біт/м = 0,7 біт;

в) правий сегмент (10Base-T): база 165,0 біт; кабель 53м * 0,113біт/м = 5,99 біт;

PDV = (15,3 + 4,18) + (33,5+0,7)+ (165 + 5,99) = 224,67 біт

Сума всіх складових дає значення PDV, рівне 224,67.

Тому що значення PDV менше максимально припустимої величини 575, то проектована мережа проходить по величині максимально можливої затримки обороту сигналу до стандарту Ethernet.

Зі значення PDV слід, що, прийнявши розроблену структуру ЛОМ за остаточний варіант, ми маємо «технічний запас» по нарощуванню мережі більш ніж у два рази.

Розрахунки PVV

Для розрахунків величини зменшення міжкадрового інтервалу PVV також можна скористатися табличними значеннями (таблиця 3.3) максимальних величин зменшення міжкадрового інтервалу при проходженні повторювачів різних фізичних середовищ.

Таблиця 3.3 – Зменшення кадрового інтервалу для сегментів Ethernet

Тип сегмента	Передавальний сегмент, біт	Проміжний сегмент, біт
10Base-5 або 10Base-2	16	11
10Base-fb	-	2
10Base-fl	10.5	8
10Base-T	10.5	8

Відповідно до цих даних розрахуємо значення PVV для нашого прикладу.

а) лівий сегмент (10Base-T): 10,5 біт;

б) проміжний сегмент (GigabitEthernet): 8 біт;

в) правий сегмент (10Base-T):10,5.

PVV = 10,5+8+10,5 = 29 біт

Сума цих величин дає значення PVV, рівне 29, що менше граничного значення в 49 бітових інтервалів. Розраховане значення PVV дозволяє говорити про «технічний запас» нарощування ЛОМ.

У результаті розрахунків установлене, що спроектована корпоративна мережа (розташування комп'ютерів якої наведено на рис. 3.3-3.4) по всіх параметрах відповідає стандартам Ethernet. Крім того, розрахунковими обчисленнями доведене, що є дворазовий «технічний запас» на нарощування мережі проміжними сегментами і збільшенням числа активних приймачів/передавачів сигналів.

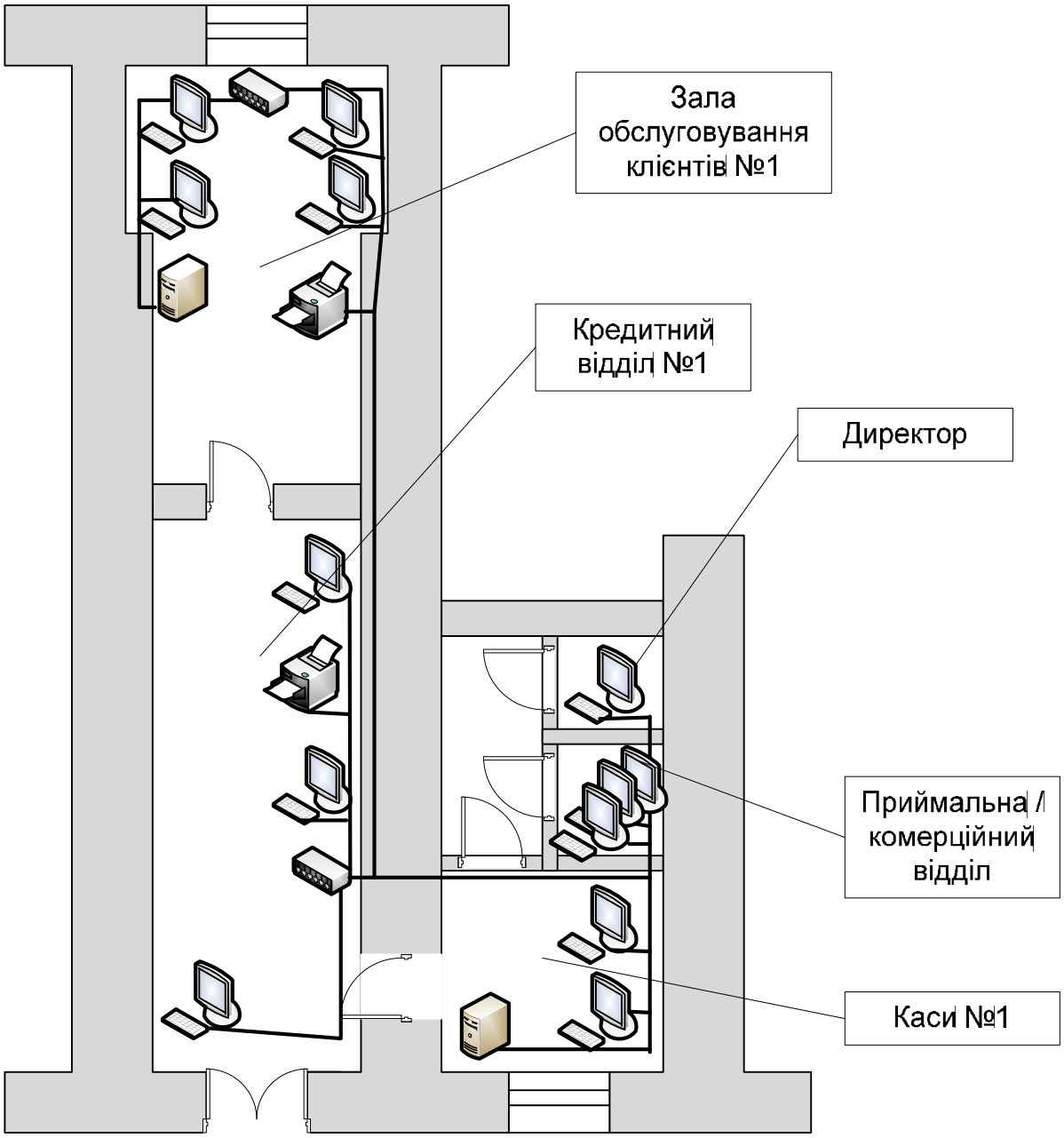

Рисунок 3.4 - Розміщення обладнання підмережі "Відділення №1"

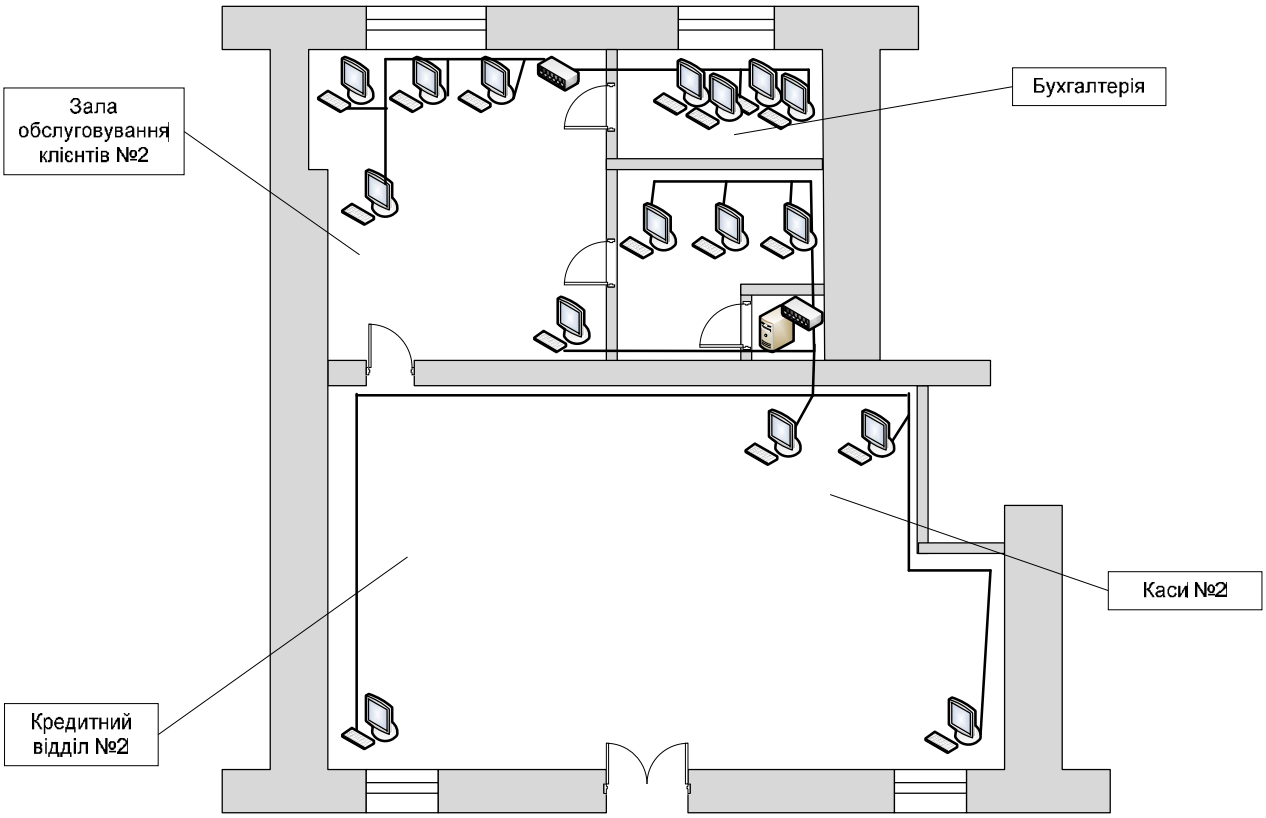

Рисунок 3.4 - Розміщення обладнання підмережі "Відділення №2"

3.4 Конфігурація мережі

Настроювання мережі зроблене таким чином, щоб не порушувати звичного робочого середовища користувачів. Оскільки впроваджувана мережа розрахована на використання вже наявних на підприємстві апаратних ресурсів, то на кожному із ПК працівників підприємства зміни торкнулися лише внутрішнього пристрою комп'ютерів і настроювання їх мережних параметрів. Індивідуальні настроювання користувачів не перетерпіли ніяких змін, відчутної для користувачів, може бути лише збільшилась швидкість передачі даних і наявність доступу в інтернет. У ході настроювання IP адреси були наведена у відповідність із настроюваннями сервера, для забезпечення користувачам необхідних параметрів доступу і безпеки, а так само для полегшення роботи мережного адміністратора.

Процедури настроювання параметрів, орієнтовані на використання середовища операційної системи Ubuntu 12.04 тому що ця операційна системи є робочою для користувачів фінансової установи.

При установці мережної карти в комп'ютер необхідно встановити драйвер – програму керуючу роботою пристрою. Драйвер, як правило, поставляється разом з пристроєм і входить у комплект поставки у вигляді файлу, записаного на компакт диск.

При першому, після установки мережної карти, запуску комп'ютера ОС визначає наявність нового (стосовно обладнання, що використовувалось раніше) пристрою і пропонує встановити драйвер (рис.3.5).

Рисунок 3.5 - Вікно встановлення драйвера пристрою

Після перезавантаження, у вікні властивостей системи (його можна викликати через властивості системи, а саме "Система - Адміністрування – Мережні параметри"), на закладці “З'єднання” з'явиться пункт типу мережного з'єднання у якому буде відображена інформація про тип пристрою (рис.3.6).

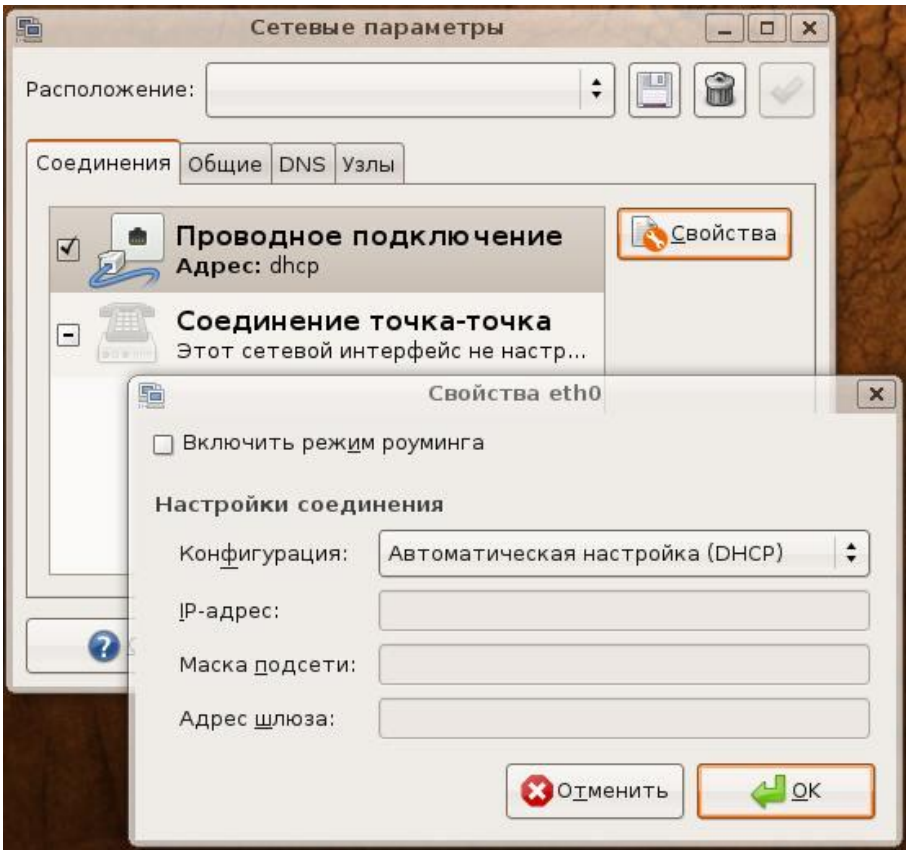

Рисунок 3.6 - Інформація про обладнання

Більш докладну інформацію про пристрій і використовуваних їм ресурсах (рис.3.7) можна отримати, двічі клацнувши по його опису в цім вікні.

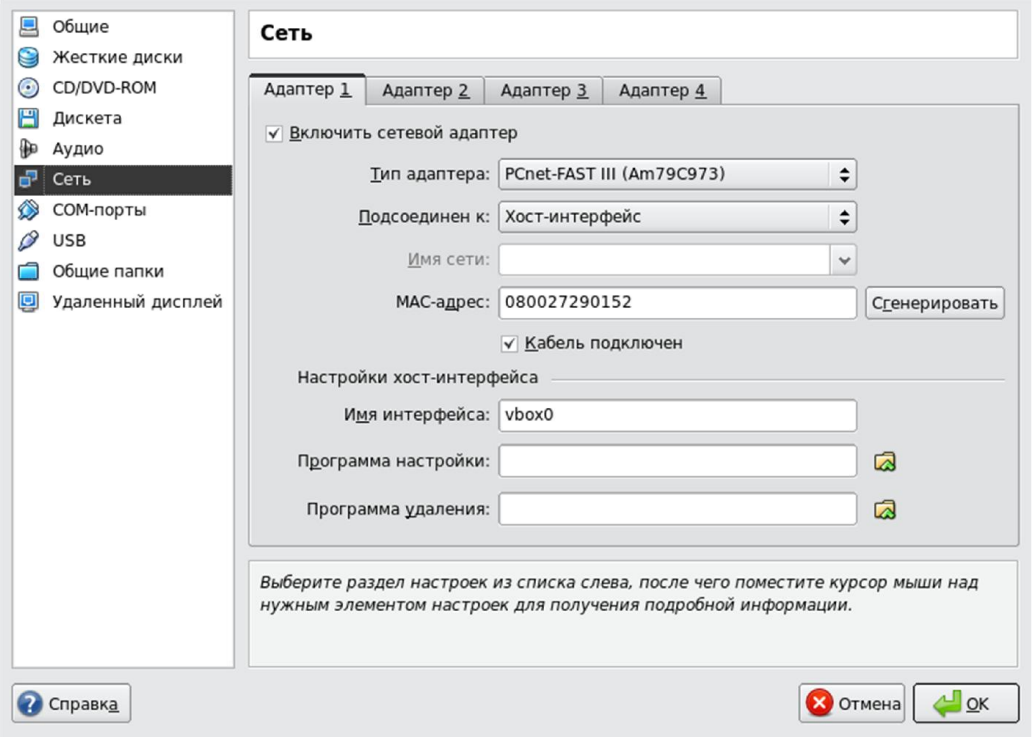

Рисунок 3.7 - Інформація про мережну карту

Після установки драйвера мережної карти, на робочому столі комп'ютера з'являється нова іконка – “мережне оточення”.

Але однієї тільки установки драйвера ще не досить, для того, щоб одержати доступ до мережних ресурсів. Для правильної роботи комп'ютера у мережі потрібно настроїти його мережні параметри. Одержати доступ до них можна, звернувшись до властивостей “мережного оточення” (рис.3.8).

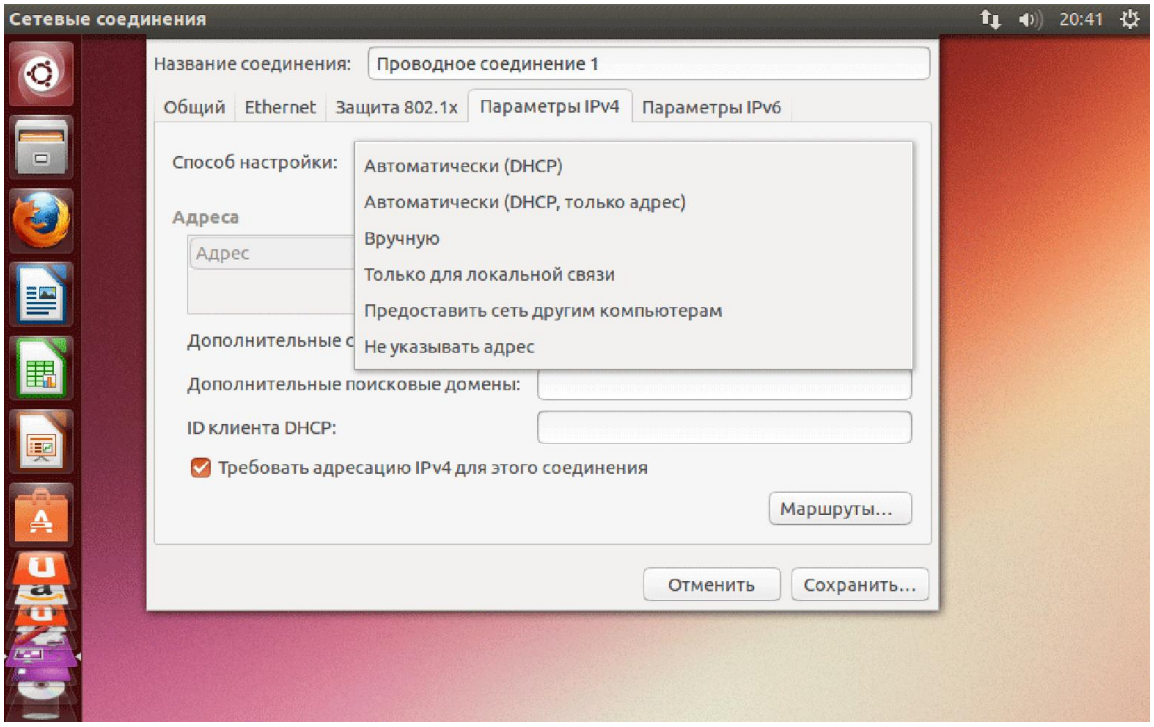

Рисунок 3.8 - Вікно налаштування мережних параметрів

Одним з найважливіших параметрів настроювання є настроювання параметрів протоколу TCP/IP (рис.3.9).

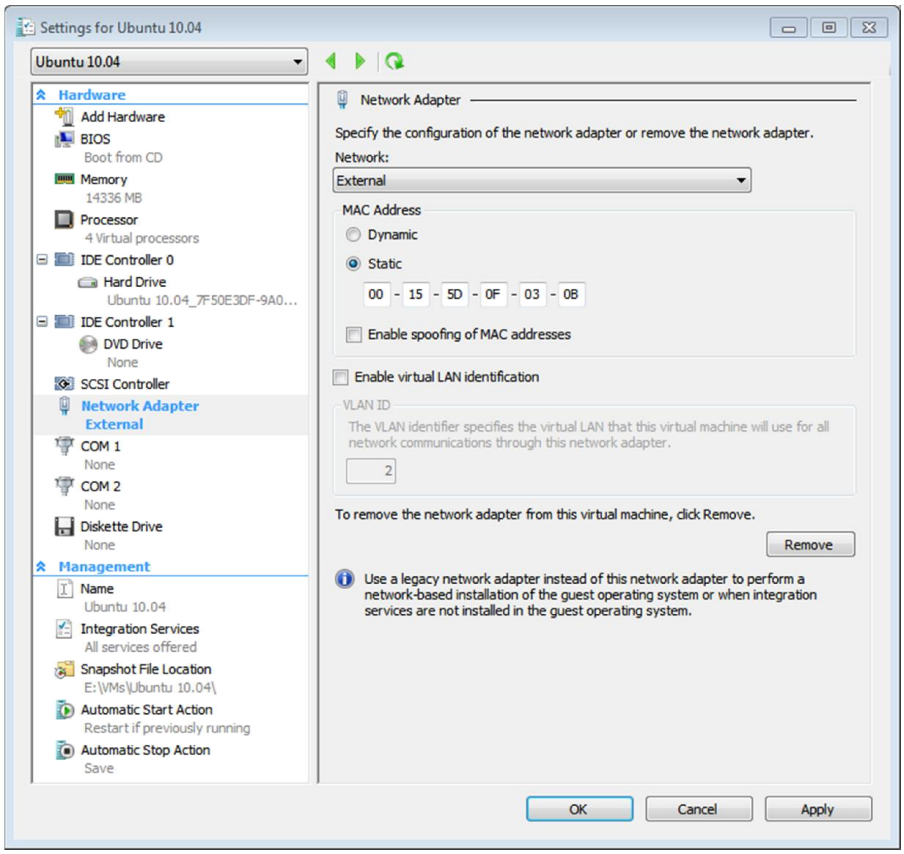

Рисунок 3.9- Вікно налаштування протоколу TCP/IP

Другий необхідний параметр – ім'я комп'ютера і ім'я “робочої групи” до якої він буде належати.

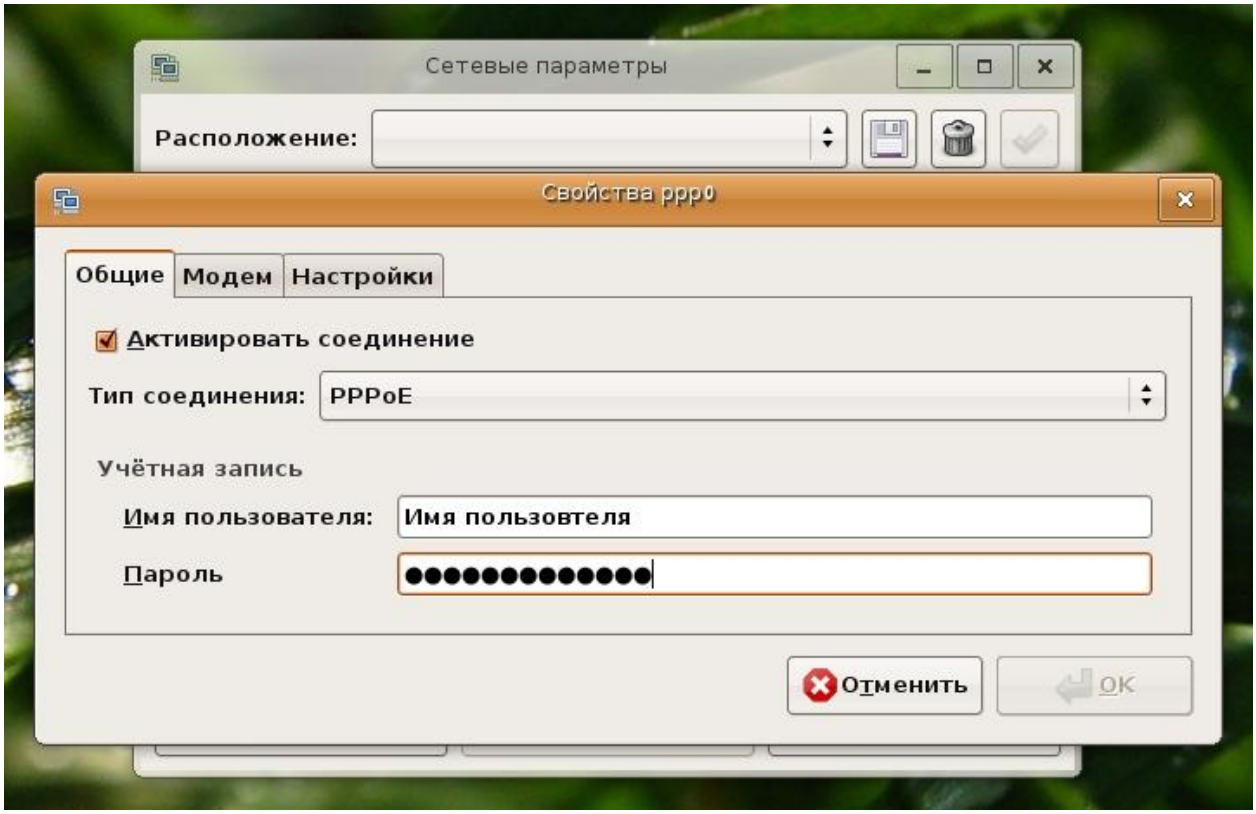

Рисунок 3.10 - Вікно налаштування імені комп'ютера та робочої групи

Подвійне клацання лівої клавіші миші на “мережному оточенні” відкриває вікно, у якому відображені всі комп'ютери, до яких є доступ з даного комп'ютера (рис.3.11).

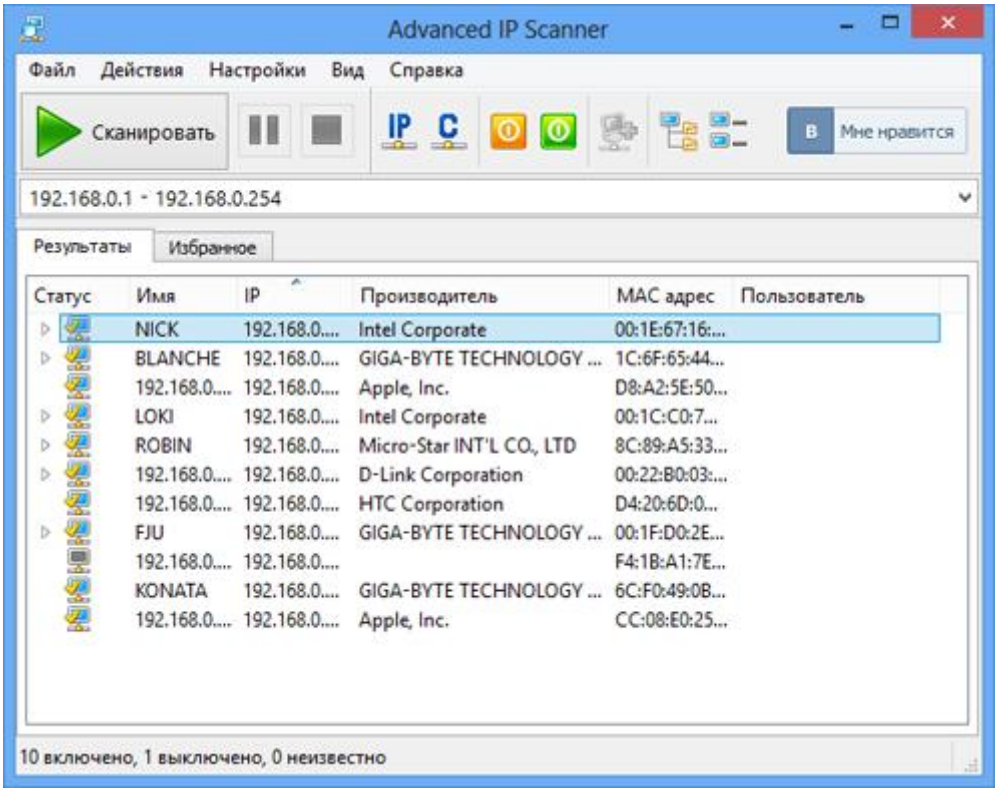

Рисунок 3.11 - Мережне оточення

Тепер комп'ютер може використовувати ресурси мережі для роботи.

Для того, щоб інші комп'ютери мережі могли використовувати ресурси даного комп'ютера, необхідно дозволити доступ до них – зробити їх мережними.

Для дозволу доступу до локальних дисків комп'ютера необхідно клацнути на значку диска правою кнопкою миші, вибрати пункт “Доступ” і у вікні, що відкрилося (рис. 3.12) вибрати бажаний режим доступу до ресурсу. Схожа процедура для дозволу доступу до принтера, приєднаного до даного комп'ютера (рис.3.13).

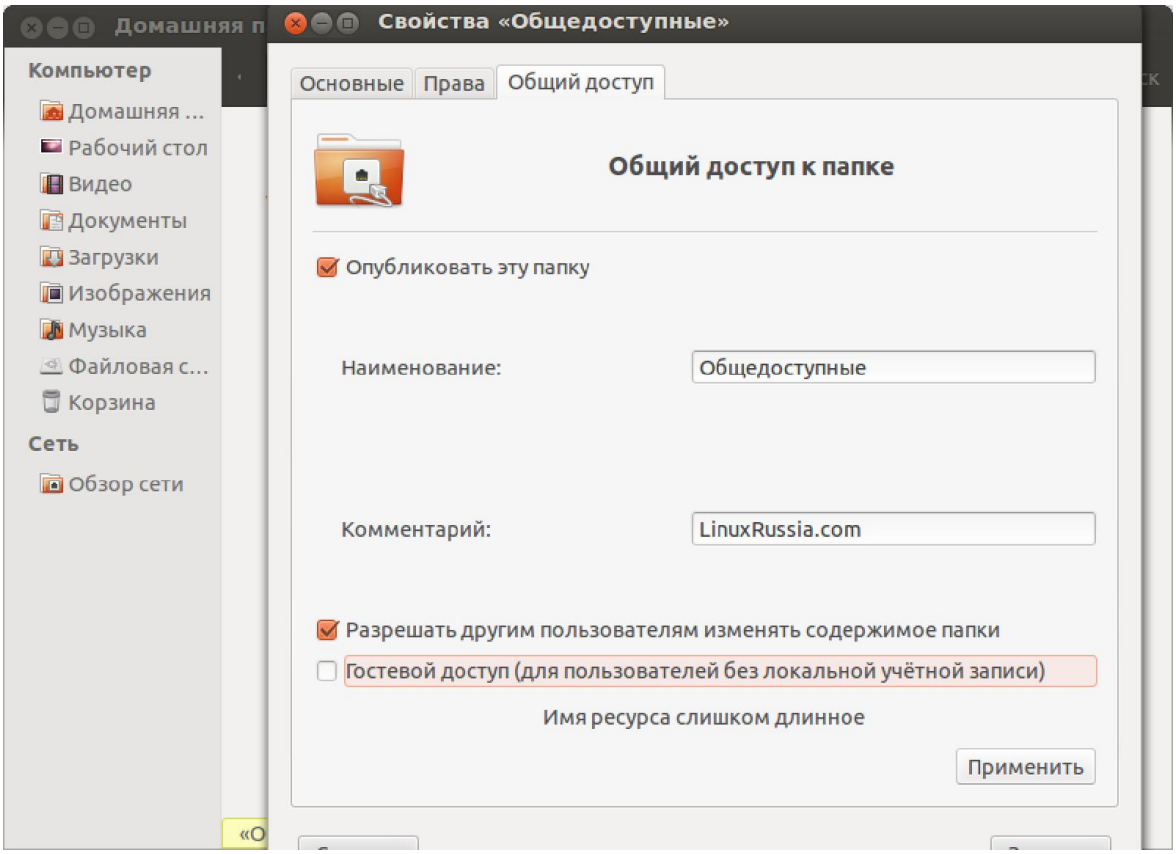

Рисунок 3.12 - Дозвіл на доступ до локального диска комп'ютера

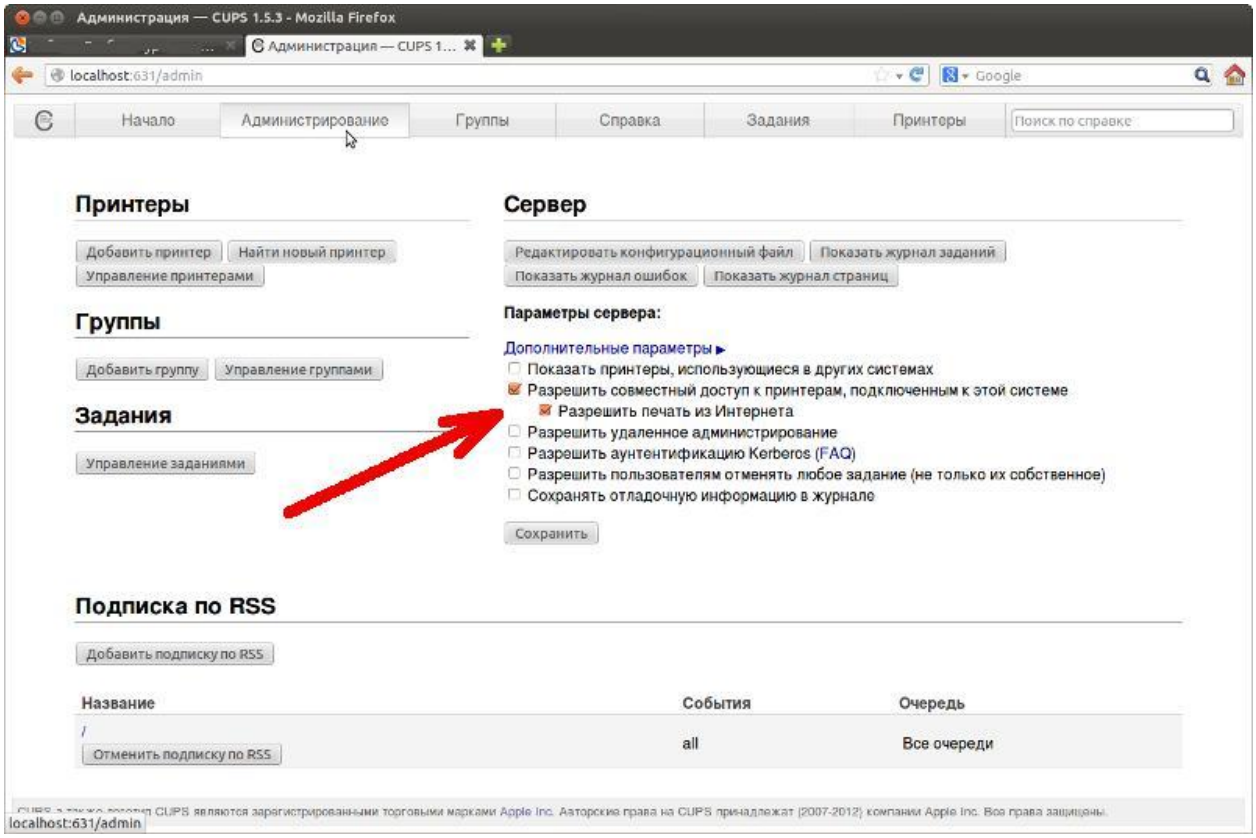

Рисунок 3.13 - Дозвіл на доступ до принтера

Результатом проектування стала ЛОМ, що має наступну структуру: в окремому приміщенні, називаному «Серверна» установлений інтернет-сервер і файл-сервер бухгалтерії. До цього сервера за допомогою кабелю на основі кручена пари підключений комутатор. Другий комутатор розташований на першому поверсі в коерційному відділі. Комутатори з'єднані кабелем Gigabit SX. Кожний з комутаторів обслуговує свою підмережу. Підмережі перебувають у різних приміщеннях і функціонально не залежать друг від друга.

До комутатора підмережі «Відділення №1» підключено 13 комп'ютерів. У цієї підмережі є три мережні принтери. До комп'ютера секретаря підключений DSL-модем для приймання електронної пошти у випадку зупинки сервера

До комутатора підмережі «Відділення №2» підключено 21 комп'ютер (20 комп'ютерів відділення і файловий сервер відділення). Ця підмережа також містить мережні принтера (2 струминних і 1 лазерний).

Керування інтернет-сервером і процесом підключення користувачів до глобальної мережі проводиться за допомогою ОС Linux.

3.5 Методи захисту інформації в мережі

Ресурси корпоративної мережі, як і будь-яка фінансова, комерційна і корпоративна інформація потребує надійного захисту. І причин тому множина: від промислового шпигунства, до мимовільній втраті інформації.

Захист апаратних ресурсів мережі попадає під адміністративно-територіальну категорію засобів захисту, тобто використання сучасних засобів захисту території та матеріальних цінностей.

Захист програмного забезпечення частково попадає під ці заходи, тобто пропускний режим, охорона території, навчання персоналу і т.д. Але разом і цим, захист ПЗ покладають на саме ПЗ. І починає подібний захист із сервера,

як самого потужного і важливого елемента інформаційного забезпечення корпоративної мережі.

Адміністрування користувачів полягає в створенні облікової інформації користувачів (визначальної ім'я користувача, приналежність користувача до різних груп користувачів, пароль користувача), а також у визначенні прав доступу користувача до ресурсів мережі - комп'ютерам, каталогам, файлам, принтерам і т.п.

Створення облікової інформації користувачів здійснюється в мережі Windows Server 2008 утилітою User Manager для локального комп'ютера та User Manager for Domains для всіх комп'ютерів домену. Права доступу до ресурсів задаються в мережі Ubuntu Server 12.04 різними засобами, залежно від типу ресурсу. Можливість використання комп'ютерів Ubuntu 12.04 у якості робочих станцій - за допомогою User Manager for Domains, доступ до локальних каталогів і файлам - за допомогою засобів IP Explorer, до вилучених поділюваних каталогів - за допомогою Server Manager, доступ до принтерів - з панелі Printers.

У мережі Ubuntu Server 12.04 можуть бути визначені наступні типи користувачів і груп користувачів:

- локальний інтерактивний користувач комп'ютера (користувач, який заведений у локальній обліковій базі даних комп'ютера, і який працює з ресурсами комп'ютера інтерактивно);
- локальний мережний користувач комп'ютера (користувач, який заведений у локальній обліковій базі даних комп'ютера, і який працює з ресурсами комп'ютера через мережу);
- локальна група комп'ютера (може створюватися на всіх комп'ютерах домену);
- локальна група домену - складається з користувачів домену;

Операції доступу - це дії об'єктів над суб'єктами. Операції можуть бути або дозволені, або заборонені, або взагалі не мати змісту для даної пари об'єкта й суб'єкта.

Уся множина операцій розділяється на підмножини, що мають особливі назви:

– дозволу (permissions) - це множина операцій, які можуть бути визначені для суб'єктів усіх типів стосовно об'єктів типу файл, каталог або принтер;

– права (user rights) - визначаються для об'єктів типу група на виконання деяких системних операцій: створення резервних копій, вимикання комп'ютера (shutdown) і т.п. Права призначаються за допомогою User Manager for Domains;

– можливості користувачів (user abilities) - визначаються для окремих користувачів на виконання дій, пов'язаних з формуванням їх операційного середовища, наприклад, зміна складу програмних груп, показуваних на екрані дисплея, включення нових іконок в Desktop, можливість використання команди Run і т.і.

Права і дозволи, що надані групі, автоматично надаються її членам, дозволяючи адміністраторові розглядати велику кількість користувачів як одиницю облікової інформації.

Можливості користувачів визначаються профілем користувача.

Можливості користувачів - визначаються для окремих користувачів на виконання нечисленних дій, що стосуються реорганізації їх операційного середовища:

– включення нових програмних одиниць у групу програм панелі User Program Manager;

– створення програмних груп User Program Manager;

– зміна складу програмних груп;

– зміна властивостей програмних одиниць (наприклад, включення в стартову групу);

– запуск програм з меню FILE в Program Manager;

– установлення з'єднань із мережним принтером, крім тих (які вже передбачені в профілі користувача).

Можливості користувача є частиною так званого профілю користувача (User Profile), який можна змінювати за допомогою утиліти User Profile Editor. Профіль поряд з описаними можливостями включає і установки середовища користувача на його робочому комп'ютері, такі як кольору, шрифти, набір програмних груп і їх склад.

Адміністратор управляє доступом користувачів до каталогів і файлам у розділах диска, відформатованих під файлову систему XFS. Розділи, відформатовані під FAT32 і HPFS, не підтримуються засобами захисту Ubuntu Server 12.04. Однак можна захистити поділювані по мережі каталоги незалежно від того, яка використовується файлова система.

Для захисту файлу або каталогу встановлюються для нього дозволи (permissions). Кожний встановлений дозвіл визначає вид доступу, який користувач або група користувачів мають стосовно даного каталогу або файлу. Наприклад, якщо встановлений дозвіл Read до файлу report14_200606.doc для групи BUHG, користувачі із цієї групи можуть переглядати дані цього файлу і його атрибути, але не можуть змінювати файл або видаляти його.

Аудит - це функція Windows 2008, що дозволяє відслідковувати діяльність користувачів, а також усі системні події в мережі. За допомогою аудита адміністратор одержує інформацію

- про виконану дію,
- про користувача, який виконав цю дію,
- про дату і часу виконання дії.

Адміністратор використовує політику аудита (Audit Policy) для вибору типів подій, які потрібно відслідковувати. Коли подія відбувається, у журнал безпеки того комп'ютера, на якому воно відбулося, додається новий запис. Журнал безпеки є тим засобом, за допомогою якого адміністратор відслідковує наступ тих типів подій, які він задав.

Політика аудита контролера домену визначає кількість і тип фіксованих подій, що відбуваються на всіх контролерах домену. На комп'ютерах Ubuntu 12.04 або Ubuntu Server 12.04, що входять у домен,

політика аудита визначає кількість і тип фіксованих подій, що відбуваються тільки на даному комп'ютері.

Адміністратор установлює політику аудита для домену для того, щоб:

– відслідковувати успішні і неуспішні події, такі як логічні входи користувачів, читання файлів, зміни в дозволах користувачів і груп, виконання мережних з'єднань і т.п.;

– виключити або мінімізувати ризик неавторизованого використання ресурсів;

– аналізувати часові тенденції, використовуючи архів журналу безпеки.

Аудит є частиною системи безпеки. Коли всі засоби безпеки відмовляють, записи в журналі виявляються єдиним джерелом інформації, на підставі якої адміністратор може зробити висновки про те, що відбулося або готується відбутися в системі.

Установлення політики аудита є привілейованою дією: користувач повинен або бути членом групи Administrators на тому комп'ютері, для якого встановлюється політика, або мати права Manage auditing and security log.

Події записуються в журнал певного комп'ютера, але можуть проглядатися з будь-якого комп'ютера мережі користувачем, який має права адміністратора на той комп'ютер, де відбулася подія.

Установка політики аудита включає два етапи:

– визначення політики аудита за допомогою панелі Audit Policy утиліти User Manager for Domains або User Manager;

– визначення каталогів, файлів і принтерів, доступ до яких необхідно відслідковувати. Для цього використовується Ubuntu Explorer або панель Printers. Спостереження за файлами і каталогами можливо тільки для файлової системи XFS.

Перегляд журналу подій здійснюється за допомогою утиліти Event Viewer (журнал Security).

Крім настроювання засобів захисту даних сервера необхідно встановити захист і на локальні даний ПК кінцевих користувачів. До

подібних заходів ставляться – установка пароля на завантаження комп'ютера засобами базової системи вводу-виводу, яка виконує початкове завантаження ПК. Далі слід використовувати пароль на вхід в Ubuntu 12.04. Якщо використовуване програмне забезпечення має у своєму складі вбудовані засоби захисту, такі як обмеження доступу і криптографічне шифрування даних, то ними не слід зневажати. Використання антивірусних і антишпигунських програм захищає комп'ютер від програмних модулів, що містять шкідливий код.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Характеристика і аналіз потенційних небезпек при роботі на ЕОМ

Експлуатовані для вирішення завдань ЕОМ має наступні характеристики:

Таблиця 4.1 – Основні технічні характеристики ПК

Показник	Значення
споживана потужність	220 Вт;
робоча напруга	220 В;
напруга джерел живлення	+12 В;- 12 В; 5 В
робоча частота	50 Гц.

Виходячи з приведених характеристик очевидно, що для оператора існує небезпека поразки електричним струмом, внаслідок недбалого поводження з комп'ютером і порушенням правил експлуатації.

Згідно ГОСТ 12.1.013-78, приміщення для ЕОМ за ступенем небезпеки ураження людини електричним струмом відносяться до приміщень без підвищеної небезпеки (немає струмопровідної підлоги, вогкості, підвищеної температури, можливості одночасного дотику до корпусів устаткування з "землею" і до струмопровідних частин).

Згідно ГОСТ12.1.005-88 тяжкість роботи персоналу, обслуговуючого ЕОМ, відноситься до категорії 1а - легкі фізичні навантаження.

Відповідно до ГОСТ 12.0.003-74 "Небезпечні і шкідливі виробничі чинники", при обслуговуванні ЕОМ мають місце фізичні і психофізичні небезпечні, а також шкідливі виробничі чинники:

– - небезпека поразки людини електричним струмом;

– - підвищена температура;

– - підвищена, або знижена рухливість повітря;

– - підвищена або знижена вологість повітря;

– - підвищений рівень електромагнітних полів в робочій зоні;

– - відсутність або нестача природного світла;

– - підвищена пульсація світлового потоку;

– - розумове перенапруження;

– - монотонність праці;

– - емоційні навантаження;

– - шумові навантаження.

4.2 Заходи з техніки безпеки

Проектом передбачаються наступні заходи, що попереджають ураження людини електричним струмом:

– - повне зняття напруги при монтажі і ремонті технічних засобів;

– - ізоляція струмоведучих частин;

– - обгороджування електроустановок;

– - заземлення електроустановок.

При роботі оператора на ЕОМ існує небезпека поразки електричним струмом, можливість отримання електротравм не лише при дотику до частин електроустаткування, але і без безпосереднього контакту з цими. Виходячи з цього передбачається захист людини у разі його дотику до корпусу машини, при замиканні однієї з фаз на корпус. Зроблено визначення струму однофазного короткого замикання і перевірку умов спрацьовування захисного апарату.

Струм однофазного короткого замикання визначається по наближеній формулі (4.1) :

$$I_k = \frac{U_Ф}{(Z_П + \frac{Z_Т}{3})} \quad (4.1)$$

де $U_Ф$ – номінальна фазна напруга мережі, В;

$Z_П$ – повний опір петлі, створений фазними і нульовими проводами;

$Z_Т$ – повний опір струму короткого замикання на корпус, Ом.

$$Z_Т/3 = 1 \text{ Ом}$$

Для провідників і жил кабелю формула (4.2.):

$$Z_{ï} = \sqrt{R_{ï}^{\ 2} + X_{ï}^{\ 2}} \quad (4.2)$$

де $R_п = R_ф + R_о$ - сумарний активний опір фазного $R_ф$ і нульового $R_о$ дротів, Ом;

$X_п$ – індуктивний опір пайки дротів, Ом.

Переріз мідного дроту S=2.5 мм:

$X_п = 0.11$ Ом;

$R_ф = 7.55$ Ом;

$R_о = 7.55$ Ом

Отже, $R_п = 7.55 + 7.55 = 15.1$ Ом

Тоді по формулі (4.2) знаходимо повний опір петлі :

$$Z_{П} = \sqrt{15{,}1^2 + 0{,}11^2} = 15{,}1 \text{ Ом}$$

Струм однофазного короткого замикання рівний:

$$I_k = 220 / (15.1 + 0.1) = 14.47 \text{ А}.$$

Дія плавкої вставки на ЕОМ забезпечується, якщо виконується співвідношення (4.3):

$$I_k >= к * I_н, \quad (4.3)$$

де $I_н$ - номінальний струм спрацьовування плавкої вставки, А (формула 4.4.);

$$I_н = P / U \quad (4.4)$$

де P = 220 Вт - споживана потужність;

U = 220 В - робоча напруга;

K = 3 - для плавких вставок.

Отже $I_н = 220 / 220 = 1$ А.

Підставимо значення у співвідношення (4.3) і отримаємо:

$$14.47 > 3*1$$

Таким чином, доведено, що апарат забезпечить спрацьовування (і захист) при збільшенні номінального струму.

4.3 Рекомендації з пожежної безпеки

Пожежі в приміщеннях, де встановлена обчислювальна техніка, представляють особливу небезпеку, оскільки зв'язані як з матеріальними

втратами, так і з відмовою засобів обчислювальної техніки, що у свою чергу спричиняє за собою порушення ходу технологічного процесу.

Пожежа може виникати при внесенні джерела запалення в горюче середовище. Горючими матеріалами в приміщенні, де розташовані ЕОМ являються:

– -поліамід - матеріал корпусу мікросхеми, горюча речовина, температура самозаймання аерогелю 420 ^{0}C

– -полівінілхлорид - ізоляційний матеріал, горюча речовина, температура займання 335 ^{o}C, температура самозаймання 530^{o}C, теплота згорання 18000 - 20700 кДж/кг;

– -склотекстоліт ДЦ - матеріал друкованих плат, важко горючий матеріал, показник горючості 1.74, не схильний до температурного самозаймання;

– -пластика кабельний No.489 - матеріал ізоляції кабелю, горючий матеріал, показник горючості більше 2.1;

– -деревина - будівельний і обробний матеріал, матеріал з якого виготовлені меблі, горючий матеріал, показник горючості більше 2.1, теплота згорання 18731 - 20853 кДж/кг, температура займання 399^{o}C, схильна до самозаймання.

Згідно ОНТП 24-86 таке приміщення відноситься до категорії "В", як пожежобезпечне. Пожежа може виникнути в наслідок утворення або внесення джерела запалення (іскри і дуги короткого замикання, порушення ізоляції, що призводить до короткого замикання, перегрівання радіодеталей внаслідок тривалого перевантаження) і внесення його в горюче середовище.

Пожежна безпека при застосуванні ЕОМ відповідно до ГОСТ 12.1.004-91 "Пожежна безпека" забезпечується:

– системою запобігання пожежам;

– системою протипожежного захисту;

– організаційно - технічними заходами.

До системи запобігання пожежі відносяться: запобігання утворенню горючого середовища і утворення в горючому середовищі джерел запалення, забезпечення пожежобезпечне устаткування.

Для запобігання утворенню в горючому середовищі джерел запалення необхідно:

– застосування устаткування, що задовольняє вимогам електростатичної іскробезпеки по ГОСТ12.1.018-91;

– унеможливлення появи іскрового розряду в горючому середовищі з енергією, рівній і вище мінімальній енергії запалення по ГОСТ12.1.004-91.

Для зниження пожежної небезпеки проектом рекомендується встановити систему автоматичної пожежної сигналізації з використанням димового сповіщувача ИДФ-1М, який розрахований для контролю площі до 100 $м^2$

Прокладення мережевого кабелю проводиться по існуючих кабельних каналах, і у важко доступних місцях (у трубах між будівлями, в стінах) кабель необхідно залити негорючим матеріалом.

Відповідно до зразкових норм первинних засобів пожежогасінні необхідно використовувати:

– ручний вогнегасник ОУ-5 - 1 шт.;

– легко - пінний вогнегасник ОВП-5 - 1 шт.

У якості організаційно - технічних заходів рекомендується проводити навчання робочого персоналу правилам пожежної безпеки.

У розділі "Охорона праці" виконаний аналіз потенційних небезпек при роботі із засобами обчислювальної техніки, розроблені заходи з техніки безпеці, заходи, що забезпечують виробничу санітарію і гігієну праці, розраховано штучне освітлення, зроблено визначення струму однофазного короткого замикання, виконані рекомендації з пожежної безпеки.

ВИСНОВКИ

При виконанні дипломного проекту була розглянута коротка характеристика комерційного банку ВАТ КБ "Райффайзен Банк Аваль" взагалі і Лисичанської філії зокрема, у роботу якої передбачається ввести ресурси корпоративної мережі. Розроблена мережа поєднує тридцять два комп'ютерів та три сервери, дозволяючи працівникам відділень користуватися загальними апаратними і програмними засобами (мережні принтера, диски, програми) і забезпечуючи доступом до корпоративної мережі і роботу з електронною поштою.

При розробці мережі, вибір програмних засобів ґрунтувався на аналізі властивостей і якостей програмних продуктів різних типів і на основі порівняння вибирався оптимальний варіант. Вибір апаратного забезпечення заснований на технічних вимогах до розробки і показниках безпеки.

У розділі “ТЕХНІЧНІ ЗАСОБИ КОМП'ЮТЕРНИХ МЕРЕЖ” наводяться порівняльні характеристики різних технологій побудови мережі (програмних і апаратних). Розділ “РОЗРОБЛЕННЯ РОЗПОДІЛЕНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ” містить інформацію про розроблену мережу і її параметрах, а так само приводиться докладний опис процедури її налаштування.

У розділі “ОХОРОНА ПРАЦІ” були проаналізовані потенційно небезпечні шкідливі виробничі фактори, що впливають на персонал при роботі з комп'ютерною технікою, і запропоновані заходи щодо техніки безпеки, виробничої санітарії й гігієні праці, рекомендації з пожежної профілактики і заходи, що забезпечують зниження впливів на навколишнє середовище.

Корпоративна мережа розроблена і впроваджена в експлуатацію у відділеннях Лисичанської філії ВАТ КБ "Райффайзен Банк Аваль" в 2017 році.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1) Кайа Соркин, Михаэль Суконник. Передача информации в современных банковских сетях // Банковские технологии, август 1996.

2) Сень А., Юшков Ю. Телекоммуникации в банковских системах // Банковские технологии, август 1996.

3) Калинин И. Финансовая информация в сети Internet // Банковские технологии, август 1996.

4) Примостка Л.О. Аналіз банківської діяльності: сучасні концепції, методи та моделі: Монографія. — К.: КНЕУ, 2002.— 316 с.

5) Офіційний сайт Асоціації банків України // WWW.AUB.COM.UA

6) Офіційний сайт ВАТ КБ “РАЙФФАЙЗЕН БАНК АВАЛЬ” // WWW.NADRA.COM.UA

7) Прангишвили И.В., Подлазов В.С., Стецюра Г.Г. Локальные микропроцессорные вычислительные сети. М.: Наука, 1984. — 176 с.

8) Флинт Д. Локальные сети ЭВМ: Пер. с англ. М.: Финансы и статистика, 1986. — 357 с.

9) А.А. Мячев, В.Н. Степанов, В.К, Щербо. Интерфейсы систем обработки данных: Справочник/ Под ред. А.А. Мячева. М.: Радио и связь, 1989. — 416 с.

10) Овчинников В.В., Рыбкин И.И. Техническая база интерфейсов локальных вычислительных сетей. М.: Радио и связь, 1989. — 272 с.

11) Дженнингс Ф. Практическая передача данных: Модемы, сети и протоколы: Пер. с англ. М.: Мир, 1989. — 272 с.

12) Блэк Ю. Сети ЭВМ: Протоколы, стандарты, интерфейсы: Пер. с англ. М.: Мир, 1990. — 506 с.

13) Игнатов В.А. Теория информации и передачи сигналов: Учебник для вузов. — 2-е изд., перераб. и доп. М.: Радио и связь, 1991. — 280 с.

14) Технологии электронных коммуникаций. Том 23. Локальные сети NETWARE. М.: «Эко-Трендз», «Электронные знания», 1992. — 156 с.

15) Фролов А.В., Фролов Г.В. Локальные сети персональных компьютеров. М.: «ДИАЛОГ-МИФИ», 1993. — 176 с.

16) Герасименко В.А. Защита информации в автоматизированных системах обработки данных: развитие, итоги, перспективы. Зарубежная радиоэлектроника, 1993, №3, с. 3—21.

17) Лапшинский А.В. Локальные сети персональных компьютеров: В 2-х ч. М.: МИФИ, 1994.

18) Нанс Б. Компьютерные сети: Пер. с англ. М.: «БИНОМ», 1996. — 400 с.

19) Spurgeon Ch. Ethernet Configuration Guidelines. Peer-to-Peer Communications, Inc., 1996. — 178 p.

20) Gigabit Ethernet. Gigabit Ethernet Alliance, 1996. — 17 p.

21) Новиков Ю.В., Карпенко Д.Г. Оптоволоконная локальная сеть персональных компьютеров типа «звезда»// Информационные технологии и системы. Hardware Software Security. Тенденции и перспективы. Сборник статей / Сост. Мельников Д.Я. М., Международная академия информатизации, 1997, с. 24—33.

22) Новиков Ю.В., Карпенко Д.Г. Комбинированный метод доступа к каналу для волоконно-оптической сети компьютеров типа «кольцо»//Электроника и информатика — 97. Вторая всероссийская научно-техническая конференция с международным участием: В 2ч. Тезисы докладов. М.:МИЭТ, 1997, с.64—65.

23) Новиков Ю.В., Карпенко Д.Г. Аппаратура локальных сетей: функции, выбор, разработка. М.: ЭКОМ, 1998.— 288 с.

24) Новиков Ю.В., Карпенко Д.Г. Волоконно-оптическая сеть персональных компьютеров типа «кольцо» //Информационные продукты, процессы и технологии. Computer-Aided Software and Hardware Engineering. М.: Технология машиностроения, 1998, с.66—73.

25) Куин Л., Рассел Р. Fast Ethernet. К.: Издательская группа BHV, 1998. — 448 с.

26) Гук М. Аппаратные средства локальных сетей. СПб.: Питер, 2001.— 576 с.

27) Ирвин Дж., Харль Д. Передача данных в сетях: инженерный подход: Пер. с англ. СПб.: БХВ-Петербург., 2003. — 448 с.

28) Хамбракен Д. Компьютерные сети: Пер. с англ. М.: ДМК Пресс, 2004. — 448 с.