

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
ІМЕНІ АДМІРАЛА МАКАРОВА

Навчально-науковий інститут комп'ютерних наук та управління проектами
Кафедра інформаційних управляючих систем та технологій

"Допущений до захисту"

Завідувач кафедри ІУСТ

к.т.н, доц. Михелєв І.Л.

" ____ " _____ 2024 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття ступеня вищої освіти "магістр"

(освітньо-кваліфікаційний рівень)

на тему **Дослідження технологій та проектування інформаційної мережі з системою захисту інформації на підприємстві харчової промисловості**

Виконав: студент 6 курсу, групи 6141м
напряму підготовки (спеціальності)

122 – "Комп'ютерні науки".

(шифр і назва напряму підготовки, спеціальності)

Шелест І.І.

(прізвище та ініціали)

Керівник Кроптя А.В.

(прізвище та ініціали)

м. Миколаїв – 2024 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
ІМЕНІ АДМІРАЛА МАКАРОВА

Інститут, факультет Навчально-науковий інститут комп'ютерних наук та управління проектами

Кафедра Інформаційних управляючих систем та технологій

Рівень вищої освіти другий (магістерський)

Спеціальність 122 – "Комп'ютерні науки"

Освітня програма "Комп'ютерні науки"

"ЗАТВЕРДЖУЮ"

Гарант освітньої програми

В. Ажищев

к.т.н, доц. Ажищев В.Ф.

"___" _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
на здобуття ступеня вищої освіти "магістр"

Студенту Шелесту Іллі Ігоровичу

1. Тема проекту (роботи) Дослідження технологій та проектування інформаційної мережі з системою захисту інформації на підприємстві харчової промисловості
керівник проекту (роботи) Кроптя Арсеній Володимирович,
затверджені наказом вищого навчального закладу від "08" 10 2024 року № 1055-уч.

2. Строк подання студентом проекту (роботи) 15 грудня 2024 року.

3. Вихідні дані до проекту (роботи) ДСТУ щодо обробки інформації, літературні джерела, технічна документація на існуючі аналоги систем, матеріали практики.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):

- Титульний аркуш, завдання на дипломну роботу, анотація (українською, англійською), зміст, перелік умовних означень, символів, одиниць та термінів (при необхідності).
- Вступ.
- Аналіз предметної області і постановка задачі.
- Розробка проекту автоматизованої системи.
- Реалізація проекту автоматизованої системи (технічна документація по проекту).
- Розділ з охорони праці.

- Висновки.
- Список використаної літератури.
- Додатки: загальний опис підсистеми, керівництво користувача, керівництво адміністратора, програма і методика випробувань, графічні інтерфейси, код програми.

5. Перелік графічного матеріалу

5.1 Опис діяльності об'єкта автоматизації.

5.2 Схеми функціональних зв'язків між підрозділами та функціональної структури підприємства.

5.3 Види топології локальних мереж.

5.4 Плани прокладки кабелю на підприємстві.

5.5 Система відеоспостереження.

5.6 Аналіз надійності роботи мережі.

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
1.	Кроптя А.В.	05.09.2023	22.12.2023
2.	Кроптя А.В.	23.12.2023	15.06.2024
3.	Кроптя А.В.	15.06.2024	25.09.2024
4.	Кроптя А.В.	25.09.2024	14.11.2024
5.	Гурець Н.В.	25.09.2024	14.11.2024
6.	Гурець Н.В.	25.09.2024	14.11.2024

7. Дата видачі завдання 05 вересня 2024 р.

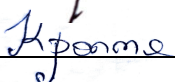
КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1.	Вивчення і опис предметної області	22.12.2024	
2.	Розробка концепції ІС	15.03.2024	
3.	Розробка проектних рішень по ІС	15.06.2024	
4.	Реалізація проекту, розробка робочої документації	25.09.2024	
5.	Вирішення питань з охорони праці	14.11.2024	
6.	Виконання графічної частини роботи	14.11.2024	
7.	Оформлення пояснювальної записки	14.11.2024	
8.	Подання роботи на кафедральний захист	16.11.2024	
9.	Подання роботи рецензенту	20.11.2024	
10.	Подання роботи на державний захист	15.12.2024	

Студент

 Шелест І.І.

Керівник проекту (роботи)

 к.т.н., доцент Кроптя А.В.

АНОТАЦІЯ

Дипломний проект направлено на дослідження технологій та розробку локальної комп'ютерної мережі з системою захисту інформації на підприємстві а також відео спостереження.

Для підвищення ефективності роботи пропонується розробка та впровадження на підприємстві комп'ютерної інформаційно-обчислювальної мережі, яка дозволить оптимізувати процеси документообігу, діловодства та бухгалтерського обліку.

Розглянуто програмне та апаратне забезпечення, використане в розробці комп'ютерної мережі, системі відео спостереження та системі захисту інформації.

Проведені техніко-економічні розрахунки локальної обчислювальної мережі.

Робота складається з восьми глав, вступу та висновків, загальним обсягом 122 аркушів. Робота містить 19 таблиць, 35 рисунків, 1 додаток та список літератури з 15 найменувань.

Ключові слова: інформаційна мережа; система захисту інформації; проектування інформаційної мережі; технології захисту інформації; автоматизація виробничих процесів.

ABSTRACT

The diploma project aims to develop a local network with a system of information security in the enterprise as well as video surveillance.

To improve the effectiveness of the proposed development and implementation of the enterprise computer information network that will optimize workflow processes, record keeping and accounting.

We consider the software and hardware used in the development of computer networks, video surveillance systems and information security.

Conducted feasibility study on a local area network.

The work consists of eight chapters, introduction and conclusion, the total amount of 122 sheets. The work contains: 35 pictures, 19 tables, 1 appendixes and list of literature from the 15 names.

Keywords: information network; information protection system; information network design; information protection technologies; automation of production processes.

ЗМІСТ

Вступ	
1. Формування вимог та постановка задачі.....	
1.1 Характеристика підприємства ТОВ "Терновський хлібзавод"	
1.2 Постановка задачі.....	
2. Функціональна схема локальної обчислювальної мережі підприємства ТОВ "Терновський хлібзавод"	
2.1 Інформаційні потоки в локальній обчислювальній мережі підприємства ТОВ "Терновський хлібзавод"	
2.1.1 Організаційного-штатна структура підприємства.....	
2.1.2 Структура підрозділів підприємства.....	
2.1.3 Інформаційні потоки на підприємстві	
2.2 Планування структури ЛОМ ТОВ "Терновський хлібзавод"	
2.3 Вибір способу управління мережею	
2.4. Вибір місця для розміщення серверу	
2.5. Організація охорони підприємства	
2.5.1 Комп'ютерне відео спостереження.....	
3. Проектування локальної обчислювальної мережі підприємства ТОВ "Терновський хлібзавод"	
3.1 Класифікація локальних мереж	
3.1.1 Види топології локальних мереж	
3.1.2 Архітектура локальних мереж	
3.1.3. Технології локальних мереж.....	
3.1.4. Види мережевих протоколів	
3.2 Мережна архітектура локальної обчислювальної мережі підприємства ТОВ "Терновський хлібзавод"	
3.2.1 Вибір мережевої архітектури.....	
3.2.2 Вибір топології проекту	
3.2.3 Вибір технології проекту.....	
3.3 Організація мережі на основі ОС	
3.3.1 ОС Unix Linux.....	
3.3.2 ОС Windows Server	
3.4 Вибір устаткування ЛОМ.....	
3.4.1 Кінцеве мережне обладнання	
3.4.2 Комутаційне обладнання.....	
3.5 Кабельна система	
3.5.1 Вибір місць прокладання кабелю	
3.6 Організація робочих місць на підприємстві.....	
3.7 Проектування відео спостереження	
3.7.1 Призначення систем відео спостереження	
3.7.2 Вибір системи відео спостереження	
3.7.3 Вибір устаткування для відео спостереження	

3.7.4 Розміщення обладнання для відео спостереження на підприємстві ТОВ "Терновський хлібзавод"	
4. Захист інформації в мережі	
4.1 Потенційні погрози безпеці інформації	
4.1.1 Випадкові погрози	
4.1.2 Навмисні погрози	
4.2 Засоби захисту інформації в ЛОМ	
4.2.1 Технічні засоби захисту інформації	
4.2.2 Програмні засоби захисту інформації	
4.2.3 Криптографічні засоби захисту інформації	
4.2.4 Криптографічні засоби захисту інформації	
4.2.5 Законодавчі засоби захисту інформації	
4.3 Структура системи захисту інформації	
5. Розрахунок надійності мережі	
6. Економічний розрахунок локальної мережі підприємства ТОВ "Терновський хлібзавод"	
6.1 Економічна ефективність розробки й впровадження системи	
7. Охорона праці	
7.1 Аналіз умов праці	
7.2 Оздоровлення повітряного середовища	
7.3 Електробезпека	
7.4 Захист від шуму і вібрації	
7.5 Вимоги до моніторів та ЕОМ	
8. Охорона навколишнього середовища	
8.1 Вступна частина	
8.2 Забруднення навколишнього середовища підприємствами	
8.3 Основні заходи щодо зниження забруднення атмосферного повітря викидами автомобільного транспорту	
8.4. Заходи запобігання забруднення навколишнього середовища застарілою комп'ютерною технікою підприємства	
Висновки	
Список використаних джерел	
Додаток А	

Вступ

У даному дипломному проекті розглядається проблема побудови локальної обчислювальної мережі та відео спостереження ТОВ «Терновський хлібзавод» під управлінням операційної системи MS Windows Server.

Реалізація запропонованого проекту дозволить скоротити паперовий документообіг усередині підприємства, підвищити продуктивність праці, скоротити час на здобуття і обробку інформації, виконувати точний і повний аналіз даних, забезпечувати здобуття будь-яких форм звітів за підсумками роботи. Як наслідок, утворюються додаткові тимчасові ресурси для розробки і реалізації нових проектів. Таким чином, вирішиться проблема окупності і рентабельності впровадження локальної мережі та відео спостереження. Локальна обчислювальна мережа має бути спроектована так, щоб забезпечити належну міру захищеності даних.

Метою дипломного проекту є організація локальної комп'ютерної мережі а також відео спостереження.

Для вирішення поставленої мети в роботі вирішуються наступні завдання:

- вибір топології, устаткування і програмного забезпечення;
- вибір способу управління мережею;
- управління мережевими ресурсами і користувачами мережі;
- розглядаються питання безпеки мережі;
- вибір системи відео спостереження;
- вибір обладнання відео спостереження та розміщення на об'єкті.

Необхідно розробити раціональну, гнучку структурну схему мережі підприємства, вибрати апаратну і програмну конфігурацію сервера, а так само пропрацювати питання забезпечення необхідного рівня захисту даних.

1. ФОРМУВАННЯ ВИМОГ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Характеристика підприємства ТОВ «Терновський хлібзавод»

Підприємство ТОВ «Терновський хлібзавод» існує на Українському ринку протягом п'ять років. Воно розташовано в пригороді міста Миколаїв. Основним видом діяльності даного підприємства є:

- виробництво і реалізація хлібобулочних і кондитерських виробів;
- виробництво, переробка і реалізація сільськогосподарської продукції;
- організація та здійснення оптової та роздрібної торгівлі хлібобулочними, кондитерськими виробами та іншою продукцією власного виробництва.

Асортимент продукції за період існування підприємства було розширено до сорока видів хліба, а також кондитерської випічки. Потужність підприємства становить 30 тон на добу. ТОВ «Терновський хлібзавод» працює відповідно до заявок торговельних організацій. Тому обсяги продукції, що випускається коливаються в залежності від попиту, а також платоспроможності населення міста.

Підприємство займає велику площу будівлі, приблизно 1000 м².

ТОВ «Терновський хлібзавод» складається з основних цехів: хлібно-булочного та кондитерського. Зараз закінчується будівництво цеху з виробництва житнього солоду. Існує мережа фірмових магазинчиків «Терновський хліб». У робочому стані знаходяться дві тунельні газові печі, одна формова піч та дві жарові обертові газові шафи. Тунельні печі служать для випічки батонної лінії, а жарові обертові шафи для випічки асортименту, та кондитерських виробів. Підприємство оснащено сучасним обладнанням. Придбано і встановлено в хлібно-булочному цеху електропіч з випікання батонів. З метою підвищення якості подового хліба в 2008 році в хлібному цеху встановлена тунельна піч ППЦ 212250Х2.

Перед будівлею є великий під'їзд, так звана рампа, яка служить для надійного та зручного завантаження та відвантаження товарів у спеціальні вантажні автомобілі.

В даний час на підприємстві випускається 8-10 найменувань хліба, 10-15 найменувань булочних та здобних виробів, 8-10 найменувань кондитерських виробів. Середньодобове виробництво становить 20 т.

Сьогодні на хлібозаводі працює сімдесят п'ять чоловік.

Виробництво ведеться в дві зміни. Дрібноштучні та здобні вироби випікаються в другу зміну.

З поміж інших підприємств підприємство ТОВ «Терновський хлібзавод» має багато таких рис, які не можуть бути притаманні великим підприємствам. Крім цього воно має можливість торгувати за ціною нижче ціни продукції великих хлібозаводів, бо здійснює більш гнучку цінову політику.

З усього вищезазначеного, робота підприємства набуває оберти у розвитку своєї галузі на ринку Миколаївщини та її районних центрів.

1.2 Постановка задачі

Від підприємства ТОВ «Терновський хлібзавод» було отримане замовлення на розробку комп'ютерної мережі та відео спостереження. Суть замовлення складається в тому, що працівники повинні мати свої окремі робочі місця з встановленими там персональними комп'ютерами (ПК), які треба об'єднати у локальну мережу, яка повинна мати доступ до мережі Internet та забезпечувати відео спостереження на підприємстві.

Підвищення економічної ефективності і конкурентоспроможності можна досягнути замінивши деяке фізично застаріле обладнання, що допоможе підвищити ефективність роботи, усунути простої обладнання із

технічних причин, вести технологічний процес безперервно і максимально використовувати технічну потужність цеху.

Крім того для покращення результатів діяльності в найближчий час потрібним є:

- розширення зовнішньоекономічної діяльності;
- використання різноманітних методів стимулювання праці;
- поліпшення якості робочої сили;
- зниження простоїв обладнання;

- залучення персоналу в процес управління;
- впровадження заходів для покращенню організації праці;
- раціоналізація робочих місць;
- проведення робіт по дослідженню та розширенню ринків збуту.

Також потрібно безперервно здійснювати роботу по поліпшенню якості продукції, що виробляється, розширення асортименту, зниження собівартості та пошуки додаткових ринків збуту.

Виходячи з розглянутої структури організації й розв'язуваних нею завдань, можна зробити висновок про те що, для забезпечення нормальної роботи необхідна сучасна локальна мережа.

Для рішення поставленої мети в дипломній роботі виділено наступні задачі:

- аналіз потоків інформації на підприємстві;
- вибір структури, топології, мережної архітектури для комп'ютерної мережі, метод доступу, тип кабельної системи;
- вибір способу керування мережею;
- конфігурація мережного встаткування;
- керування мережними ресурсами й користувачами мережі;
- розглядаються питання безпеки мережі;
- забезпечення гнучкості адміністрування та зручності масштабування (наращення);
- забезпечення інформаційної безпеки та захисту інформації;
- розглядається організація відео спостереження.

В будівлі в якій знаходиться офіс відсутні лінії Internet, але є телефонні лінії.

В проекті розглядається проблема побудови локальної обчислювальної мережі, а також проектування та побудова відео спостереження. Локальна обчислювальна мережа повинна бути спроектована так, щоб забезпечити захищеність даних, при цьому мати належний рівень доступу кожному з працівників свого напрямку.

Дана комп'ютерна мережа має розроблятися з розрахунком на подальшу модернізацію та розширення.

2. ФУНКЦІОНАЛЬНА СХЕМА ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТВА ТОВ «ТЕРНОВСЬКИЙ ХЛІБЗАВОД»

2.1 Інформаційні потоки в локальній обчислювальній мережі підприємства ТОВ «Терновський хлібзавод»

2.1.1 Організаційно-штатна структура підприємства

На чолі підприємства знаходиться директор, який організовує і контролює роботу підпорядкованих йому працівників, розробляє стратегію підприємства з урахуванням перспектив розвитку, веде співбесіди з потенційними працівниками, приймає на постійну, або тимчасову роботу, приймає рішення про звільнення працівників.

Старший бригадир контролює роботу підпорядкованих йому підлеглих.

Бригадири контролюють роботу підлеглих їм працівників конкретних підрозділів.

Технологи здійснюють контроль над рецептурою, дають вказівки іншим упорядкованим працівникам по виготовленню хлібобулочної продукції.

Завідуючий складом здійснює контроль за наявністю сировини на складі, веде оперативний облік надходження сировинних матеріалів та контролює своєчасність завантаження сировини за доставками.

Торгові агенти проводять маркетингові дослідження на ринку товарів, розробляють стратегію просування товарів на ринку, керують роботою зі створення дилерської мережі збуту та доставки готової продукції.

Головний бухгалтер несе безпосередню відповідальність за правильну організацію обліку, достовірність звітних показників, здійснює облік затрат на виробництво, складає калькуляції собівартості продукції, робіт і послуг, виявляє результати роботи окремих виробничих ділянок і підприємства в цілому.

Касир займається обліком і розподілом коштів на підприємстві, а також нарахуванням заробітних плат.

Лаборанти проводять аналізи як на сировинному матеріалі так і на готовій продукції.

Оператори зв'язуються з клієнтами проводять заклази на хлібобулочну продукцію, реєструють їх у комп'ютері та випускають всі необхідні папери (накладні, реєстри тощо.)

Охорона здійснює моніторинг та огляд в середині підприємства і на підлеглий території пекарні.

2.1.2 Структура підрозділів підприємства

До структури підприємства ТОВ «Терновський хлібзавод» входять наступні підрозділи: дирекція, бухгалтерія, операторський відділ, технологічний відділ, лабораторія, склад, охорона.

До штату працівників бухгалтерії входять три чоловіка: головний бухгалтер, бухгалтер, касир.

Обов'язки:

- оформлення документів (рахунки, видаткові та прибуткові накладні; довіреності, договори);
- нарахування заробітної плати;
- здійснення обліку коштів у касі;
- контроль додержання платіжної дисципліни;
- ведення обліку матеріальних цінностей придбання і використання їх;
- здійснення обліку розрахунків з постачальниками і підрядчиками;
- контроль стану складського обліку участь в інвентаризації цих цінностей;
- складання встановленої звітності;
- здійснення обліку затрат на виробництво;
- складання калькуляції собівартості продукції, робіт і послуг;
- виявлення результату роботи окремих виробничих ділянок і підприємства в цілому;
- проведення участі в інвентаризації даного виробництва;
- складання звітності про виконання плану виробництва і собівартості продукції;

- облік надходження з виробництва готової продукції, її відвантаження і реалізація;
- ведення розрахунків з покупцями, а також складання звітності про реалізацію продукції;
- здійснення обліку решти господарських операцій;
- ведення узагальнюючі облікові, складання балансу та інші форми звітності з основної діяльності підприємства;
- організація бухгалтерського архіву.

Головний бухгалтер здійснює загальне керівництво роботою всього бухгалтерського апарату і, як правило, безпосередньо керує роботою фінансово-розрахункової і зведено-балансової групи.

До штату працівників операторського відділу входять чотири чоловіка, старший оператор та оператори.

Обов'язки:

- прийом заказів даної продукції по телефону;
- підтримання зв'язку з клієнтами;
- ведення накладних та інших важливих документів;
- контролювання поверненого товару (браку);
- ведення статистики по товару;
- оформлення накладних;
- відповіді на телефонні дзвінки.

До штату працівників лабораторії входять два чоловіка:

- старший лаборант;
- лаборант.

Обов'язки:

- дослідження і аналізування тіста на вологість та кислотність;
- аналізування гатунку сорту муки та її якість;
- контроль чистоти на підприємстві.

До штату працівників технологічного відділу входять три чоловіка:

- технолог батонної лінії;

- технолог асортименту;
- кондитерський технолог.

Обов'язки:

- контролювання виготовлення по рецептурі даної продукції;
- контроль замішування тіста у чанах;
- контроль самого процесу випічки: (подача тіста по конвеєру, регулювання температури як у розстоечній шафі, так і в даній печі). Все це контролюється технологами по спеціальній автоматичі даної печі.

До штату працівників складу входить один чоловік: (завідуючий складом).

Обов'язки:

- прийом сировинних матеріалів за видатковою накладною постачальника;
- відпускання сировини в технологічний відділ (ЦЕХ) за подальшою обробкою та виготовленням продукції;
- вчасне інформування Директора та Технолога про сировину, яка майже закінчилась, тощо.

До штату працівників охорони входить шість чоловік: (охоронники).

Обов'язки:

- контроль та охорона даного об'єкту та підлеглим її територіям.

Взаємозв'язки у функціональній структурі підрозділів ТОВ «Терновський хлібзавод» зображено на рисунку 2.1.

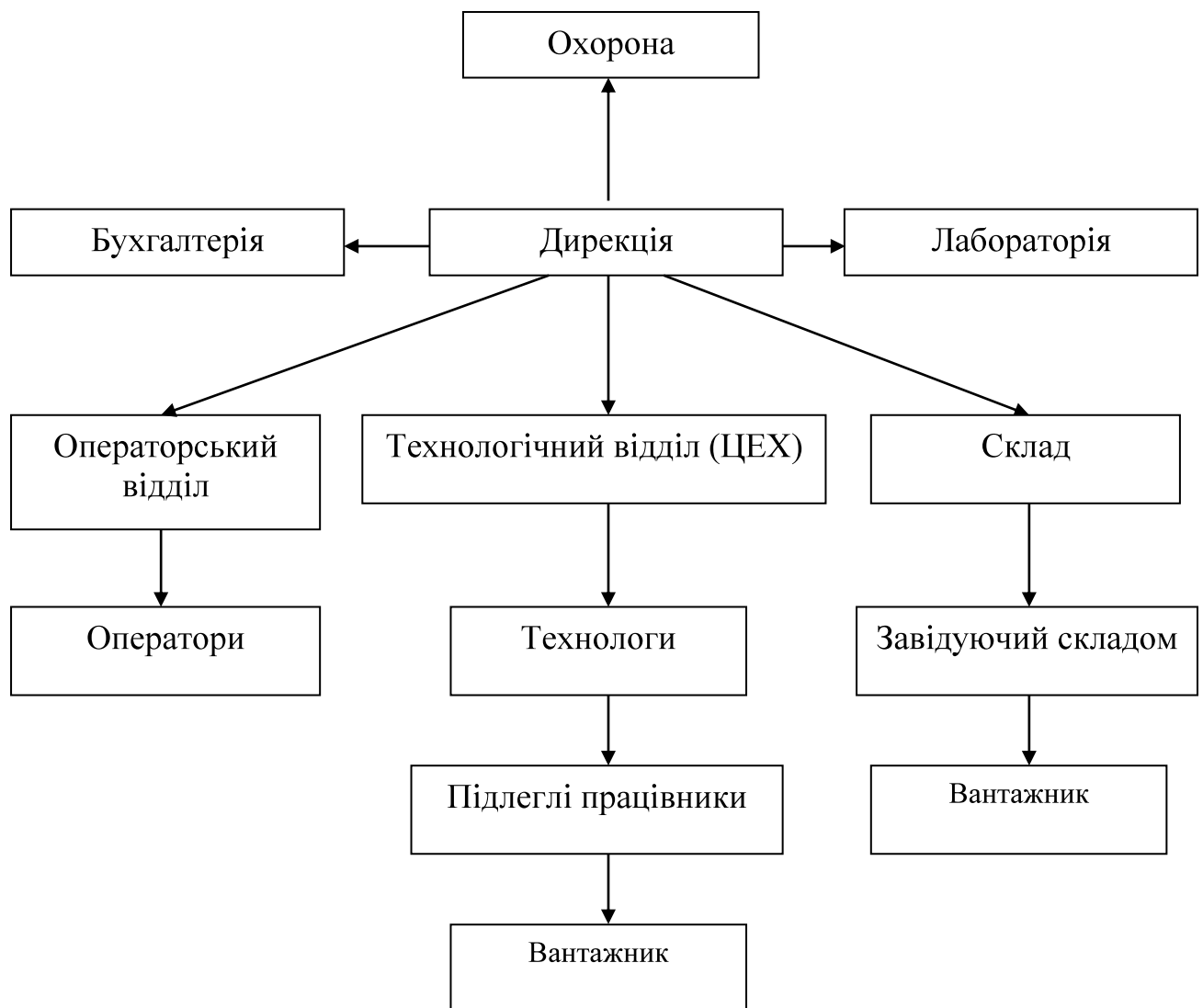


Рисунок 2.1 - Схема функціональних зв'язків між підрозділами структури

Всього на підприємстві задіяні сімдесят п'ять чоловік, дванадцяти з яких передбачається виділити в користування персональні комп'ютери.

На базі сформульованої постановки задачі ТОВ «Терновський хлібзавод» були отримані наступні загальносистемні рішення:

- рішення щодо організаційної структури;
- рішення щодо функціональної структури;
- рішення щодо функцій, що автоматизуються.

Комп'ютерна мережа призначена для автоматизації обігу інформації та підвищення якості обробки інформації.

Функції, що автоматизуються:

- використання загальної бази даних;
- контроль за доступом до важливої інформації;

- високий ступінь захисту даних;
- вихід до глобальної мережі;
- сумісне використання файлів;
- сумісне використання периферійних пристроїв (принтерів);
- організація зв'язку між користувачами;
- централізоване управління комп'ютерами;
- централізоване резервне копіювання всіх даних;
- відео спостереження.

Для реалізації вище зазначених функцій необхідно прийняти рішення щодо організаційного, інформаційного, технічного та програмного забезпечення на базі обраної концепції.

2.1.3 Інформаційні потоки на підприємстві

Ґрунтуючись на схемі функціональної структури ТОВ «Терновський хлібзавод», побудуємо схему інформаційних потоків, що представлено на рисунку 2.2.

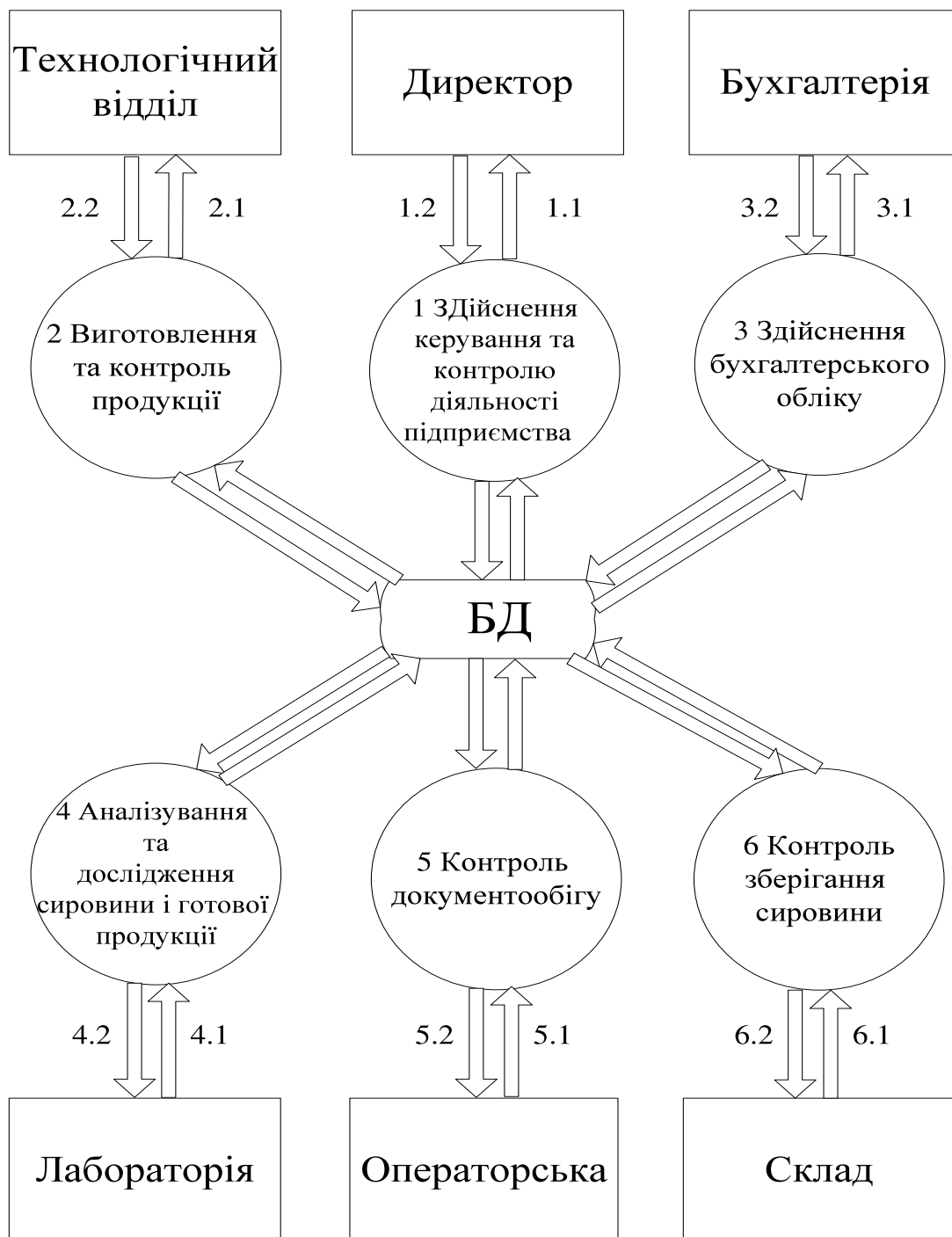


Рисунок 2.2 - Схема інформаційних потоків

Перелік інформаційних процесів:

- 1.1 – вхідна інформація щодо діяльності підприємства;
- 1.2 – вихідна інформація щодо діяльності підприємства;
- 2.1 – вхідна інформація щодо виготовлення продукції;
- 2.2 – вихідна інформація щодо виготовлення продукції;
- 3.1 – вхідна бухгалтерська інформація (заробітна платня, тощо);
- 3.2 – вихідна бухгалтерська інформація;

4.1 – вхідна інформація щодо дослідження та аналізування сировини;

4.2 – вихідна інформація щодо дослідження та аналізування сировини;

5.1 – вхідна інформація щодо прийому заказів на продукцію та контроль документообігу;

5.2– вихідна інформація щодо прийому заказів на продукцію та контроль документообігу;

6.1– вхідна інформація щодо процесу зберігання та доставки сировинних матеріалів;

6.2– вихідна інформація щодо процесу зберігання та доставки сировинних матеріалів;

Проектована комп'ютерна мережа повинна автоматизувати наступні функції:

- ведення довідника відомостей;
- ведення довідника накладних;
- ведення довідника товарів;
- ведення довідника клієнтів;
- формування звітів з виконання поставок, продажу.

Збереження інформації треба реалізувати у базі даних під управлінням «1С Підприємство».

Основними принципами створення інформаційного забезпечення є цілісність, контроль, захист від несанкціонованого доступу, єдність і гнучкість, стандартизація, адаптивність, мінімізація введення і виведення інформації.

2.2 Планування структури ЛОМ ТОВ «Терновський хлібзавод»

Приміщення підприємства знаходяться на першому та другому поверхах загальною площею приміщень 1000 м². Перший поверх займає 700 м², а другий поверх займає 300 м².

Розташування робочих місць працівників підприємства здійснене наступним чином:

Перший поверх:

- у приміщенні складу одне робоче місце (завідуючий складом);
- у технологічному відділенні три робочих місця (технологи);
- у охоронному приміщенні два робочих місця (охоронники).

Другий поверх:

- у приміщенні директора одне робоче місце (директор);
- у приміщенні бухгалтерії три робочих місця (головний бухгалтер, бухгалтер, касир);
- у приміщенні лабораторії два робочих місця (старший лаборант, лаборант);
- у операторському приміщенні чотири робочих місця (старший оператор, оператори).

План-схема існуючих на сьогоднішній день приміщень пекарні показана на рисунках 2.3 та 2.4.

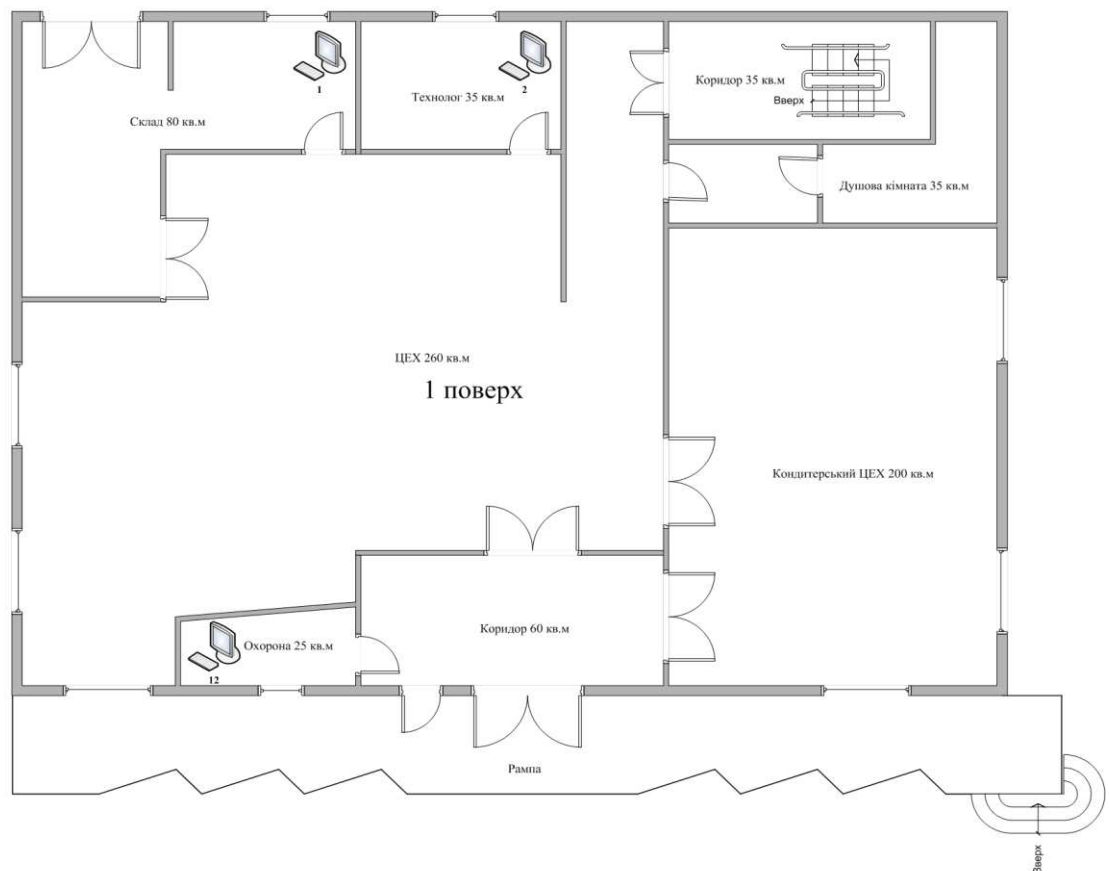


Рисунок 2.3 – План-схема існуючого підприємства перший поверх

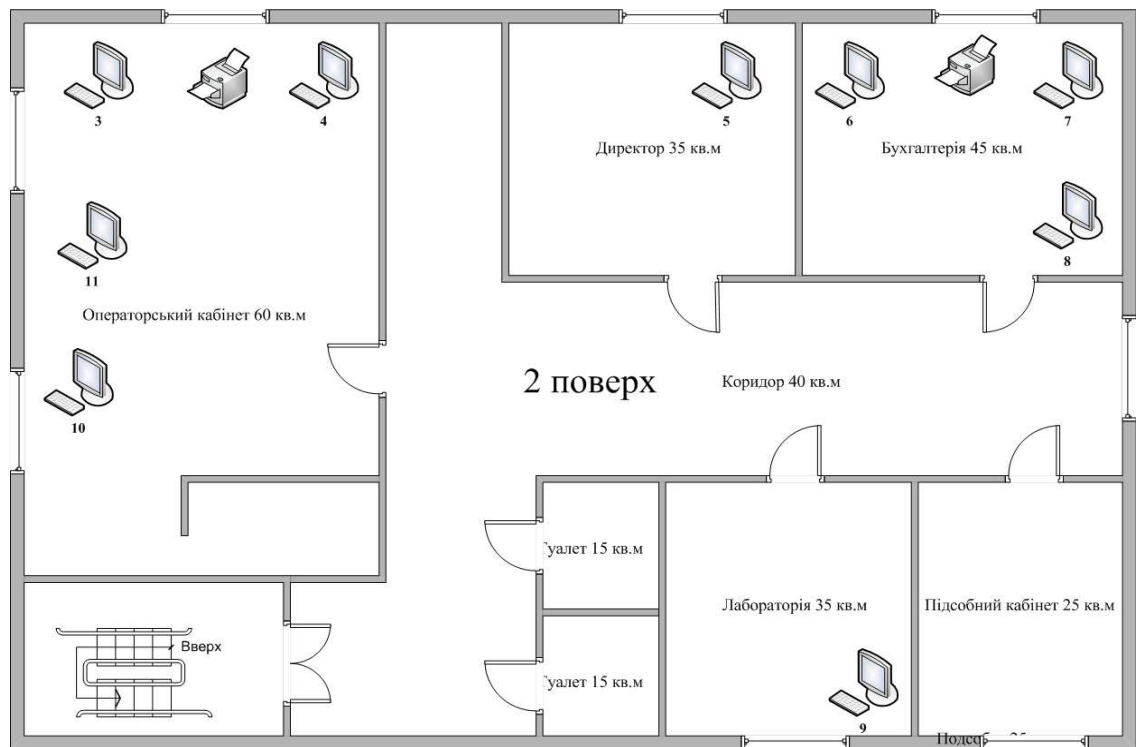


Рисунок 2.4 – План-схема існуючого підприємства другий поверх

Таким чином, проектована мережа повинна забезпечувати автоматизацію роботи всіх працівників підприємства, тобто нараховувати дванадцять робочих станцій.

2.3 Вибір способу управління мережею

Першим необхідно визначити, кількість працюючих в мережі одночасно. Від цього рішення залежатимуть всі подальші етапи створення мережі.

Кількість робочих станцій прямо залежить від передбачуваного числа співробітників. Для фірми з горизонтальною структурою, де всі співробітники повинні мати доступ до даних один одного, оптимальним рішенням є проста однорангова мережа.

Фірмі, побудованій за принципом вертикальної структури, в якій точно відомо, який співробітник і до якої інформації повинен мати доступ, слід

орієнтуватися на дорожчий варіант мережі - з виділеним сервером [1]. Тільки в такій мережі існує можливість адміністрування прав доступу (рисунок 2.5).

В даному випадку на підприємстві планується мати дванадцять робочих станцій, які і необхідно об'єднати в корпоративну мережу. Причому вони повинні бути об'єднані в наступні групи:

- Директор підприємства – одна робоча станція;
- Бухгалтерія – три робочі станції;
- Лабораторія – одна робоча станція;
- Склад – одна робоча станція;
- Технологічний відділ – одна робоча станція;
- Операторський відділ – чотири робочі станції;
- Охорона – одна робоча станція.

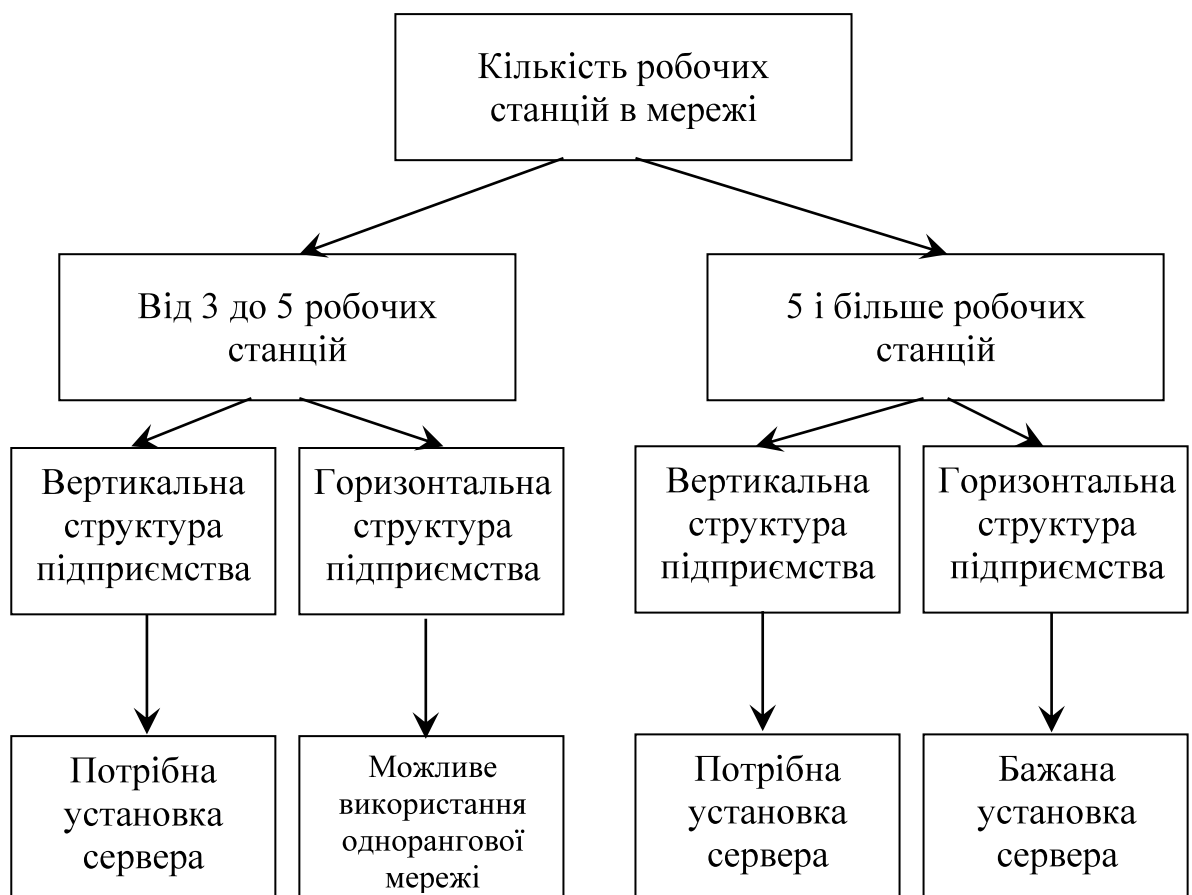


Рисунок 2.5- Вибір способу управління

Зі схеми вибору типу мережі, можна вирішити, що в даному випадку потрібна установка сервера, оскільки ми маємо горизонтальну структуру підприємства, тобто розмежований доступ до інформації.

Одним з головних етапів планування є створення схеми. При цьому залежно від типу мережі виникає питання про обмеження довжини кабельного сегменту. Це може бути неістотно для невеликого офісу, проте якщо мережа охоплює декілька поверхів будівлі, проблема настає в абсолютно іншому світлі.

2.4 Вибір місця для розміщення серверу

При побудові ЛОМ з сервером виникає ще одне питання - де краще всього встановити сервер.

На вибір місця впливає декілька чинників:

- через підвищений рівень шуму сервер бажано встановити окремо від решти робочих станцій;
- необхідно забезпечити постійний доступ до сервера для технічного обслуговування;
- по міркуваннях захисту інформації вимагається обмежити доступ до серверу.

В даному випадку з значною нестачею коштів та рядом других чинників було вибране єдине можливе місце установки серверу, не вимагаючи перебудови внутрішніх приміщень. Сервер було вирішено встановити в операторському кабінеті за спеціально встановленою перегородкою, яка ізолює шум роботи даного сервера.

2.5 Організація охорони підприємства

Цифрові системи відео спостереження стали невід'ємною частиною інженерних систем. Сучасне обладнання системи відео спостереження дозволяє не тільки спостерігати і записувати що відбувається, події, але і програмувати реакцію всієї системи безпеки при виникненні позаштатних ситуацій. З приходом комп'ютерних технологій в системи безпеки, крім функції безпосереднього відео спостереження, з'явилася можливість зберігати

відеозапис, тривалістю в кілька тижнів. В залежності від типу використовуваного обладнання системи відео спостереження поділяються на цифрові й аналогові. Охоронні системи відео спостереження призначені для візуального спостереження за охоронюваним об'єктом за допомогою відеокамер. Системи відео спостереження дозволяють стежити одночасно за одним або кількома об'єктами. Камери відео спостереження можна встановити як усередині приміщення, так і зовні. Завдання охоронної системи відео спостереження полягає в наочному представленні відеоінформації про оперативні обстановки на контрольованому об'єкті.

Найпростіша система відео спостереження включає в себе одну або кілька відеокамер і монітор, або телевізор. Камери відео спостереження можуть встановлюватися на поворотних пристроях зовні або всередині приміщення і дозволяють здійснювати цілодобове спостереження за охоронною територією. Спільно з системою відео спостереження можна використовувати датчики руху (детектори), системи освітлення та інші додаткові пристрої.

У системах відео спостереження, розрахованих на використання декількох відеокамер, на екрані одного монітора можна одночасно відображати зображення від всіх відеокамер. Для цього служать квадратори (ділителі екрану). Для послідовного виводу зображення використовуються мультиплексори (комутатори), які послідовно підключають відеокамери до монітора або телевізора. Охоронні системи відео спостереження дозволяють створити гнучку систему безпеки, до якої можуть входити не тільки компоненти систем відео спостереження, але й охоронно-пожежна сигналізація та системи контролю доступу.

На підприємстві планується розмістити камери у приміщенні першого поверху, та камери для зовнішнього відео спостереження.

2.5.1 Комп'ютерне відео спостереження

Використання сучасних цифрових технологій в системах відео спостереження дозволяє істотно розширити якість і функціональність контролю за охоронними об'єктами. Сучасні комп'ютерні системи відео спостереження

являють собою звичайні комп'ютерні плати (що встановлюються, як правило, в PCI або PCI-E слоти) і програмне забезпечення, яке встановлюється на відео сервері та робочих місцях. Подібне рішення дозволяє отримати масу переваг:

- Простота управління та користування - вся робота проводиться на звичному комп'ютері зі звичним графічним інтерфейсом і інтуїтивно зрозумілою системою команд.

- Простота комплектації і підключень - замість великої кількості пристроїв використовується один комп'ютер(сервер), до якого треба всього лише підключити камери відео спостереження.

- Можливість побудови систем будь-якого масштабу - Від простої локальної системи на кілька камер до великих розподілених систем, що складаються з багатьох відео серверів, встановлених в різних віддалених один від одного місцях і керованих віддалено через глобальну мережу. Застосування сучасних каналів передачі даних (від dial-up модемів до оптико волоконних мереж) дозволяє передавати необхідні обсяги інформації між різними частинами системи з необхідною швидкістю та якістю.

- Постійне зростання продуктивності комп'ютерів та процесорів дозволяє застосовувати більш досконалі алгоритми стиснення, пошуку і передачі відеоінформації, отримувати додаткові сервісні можливості та більш якісне відео.

- Запис на цифрові носії (жорсткі диски, оптичні диски і т.д.) набагато вища за якістю, ніж запис на відеокасети. Ці носії більш компактні, легко зберігаються і дозволяють переглядати записану інформацію необмежену кількість разів без втрати якості, а також швидко знаходити необхідні фрагменти відео зображення.

- Можливість постійного оновлення ПО розробником, а також налагодження системи під конкретні потреби користувача за допомогою розробки спеціальних скриптів для вирішення конкретних завдань, відсутніх у базовому варіанті поставки.

– Система захисту інформації та контролю доступу до архівних даних і адміністрування системи може бути вирішена шляхом застосування відомих методів захисту інформації в комп'ютерних мережах.

Проаналізувавши задачі, які повинна виконувати система відео спостереження планується установка чотирьох камер у приміщеннях першого поверху та чотирьох камер зовнішнього відео спостереження.

3. ПРОЕКТУВАННЯ ЛОКАЛЬНОЇ ОБЧИСЛЮВАЛЬНОЇ МЕРЕЖІ ПІДПРИЄМСТВА ТОВ «ТЕРНОВСЬКИЙ ХЛІБЗАВОД»

3.1 Класифікація локальних мереж

Комп'ютерна мережа – це група розташованих в межах деякої території комп'ютерів, пов'язаних один з одним за допомогою відповідних засобів комунікацій, які спільно використовують програмні і апаратні ресурси. Така мережа призначається для збору, передачі і обробки інформації в межах одного підприємства або організації. Вона може бути орієнтована на виконання певних функцій відповідно до профілю діяльності підприємства.

Усе різноманіття комп'ютерних мереж можна класифікувати за групою ознак:

- територіальна поширеність;
- відомча приналежність;
- швидкість передачі інформації;
- тип середовища передачі.

По територіальній поширеності мережі можуть бути локальними, кампусними, міськими, регіональними, і глобальними.

Локальні (1-3000 м) – об'єднують комп'ютери в межах декількох будівель.

Кампусні (100-10000 м) – локальні мережі масштабу «кампусу» – невеликого містечка.

Міські (5-20 км) – високошвидкісні канали зв'язку в межах великого міста.

Регіональні (територіальні) (100-1000 км) – об'єднують комп'ютери географічної області.

Глобальні (10000-20000 км) – об'єднання комп'ютерів в різних частинах світу (Інтернет).

Найважливіша характеристика комп'ютерної мережі – її пропускна спроможність.

Залежно від характеру розподілу функцій розрізняють:

- однорангові мережі – невеликі локальні мережі, в яких всі комп'ютери є функціонально рівноправними; звичайно включають до 15 станцій;

- мережі з виділеними серверами (дворангові мережі) – середні і крупні мережі, в яких частина виконуваних функцій по обслуговуванню станцій покладена на сервери.

Мережі з виділеними серверами характеризуються типами використовуваних в них мережевих служб (серверів).

У класифікації мереж існує три основних терміни: LAN, WAN і MAN.

LAN (Local Area Network) – локальні мережі – це мережі, що мають замкнуту інфраструктуру до виходу на постачальників послуг. Термін «LAN» може описувати і маленьку офісну мережу, і мережу рівня великого заводу, що займає кілька сотень гектарів. Закордонні джерела дають навіть близьку оцінку – біля шести миль (10 км) у радіусі.

WAN (Wide Area Network) – глобальні мережі – це мережі, що покривають великі географічні регіони, що включають у себе як локальні мережі, так і інші телекомунікаційні мережі й пристрої. Приклад WAN – мережі з комутацією пакетів (Frame Relay), через яку можуть «розмовляти» між собою різні комп'ютерні мережі.

MAN (Metropolitan Area Network) – міські мережі – це мережі призначені для обслуговування території великого міста (мегаполіса), використовуючи цифрові магістральні лінії зв'язку, із швидкостями від 45 Мбіт/с. Вони служать для зв'язку локальних мереж у масштабах міста й з'єднання локальних мереж із глобальними.

За приналежністю розрізняють мережі – відомчі й державні.

Відомчі – це мережі приналежні одній організації і розташовуються на її території.

Державні – це мережі, використовувані в державних структурах.

По швидкості передачі інформації комп'ютерні мережі поділяються на низько – , середньо – і високошвидкісні.

По типу середовища передачі розділяються на мережі коаксіальні, на кручений парі, оптоволоконні, із передачею інформації у радіоканалах, в інфрачервоному діапазоні [2].

3.1.1 Види топології локальних мереж

Мережна топологія – це геометрична форма мережі, яка характеризує фізичне розташування комп'ютерів, кабелів і других компонентів мережі. Топологія – це стандартний термін, який використовується професіоналами при описі основної компоновки мережі.

Топологія мереж обумовлює її характеристики. Зокрема, вибір тої або іншій топології впливає:

- на склад необхідного мережевого устаткування;
- характеристики мережевого устаткування;
- можливості розширення мережі;
- спосіб управління мережею.

Якщо чітко з'ясувати, як використовуються різні топології, то нескладно зрозуміти, якими можливостями володіють різні типи мереж.

Щоб разом використовувати ресурси або робити другі мережеві задачі, комп'ютери повинні бути під'єднанні один до одного. Для цієї мети в більшості мереж застосовується кабель.

Проте просто підключити комп'ютер до кабелю, що сполучає інші комп'ютери, не досить. Різні типи кабелів у поєднанні з різними мережевими платами, мережевими операційними системами і другими компонентами вимагають і різного взаємного розташування комп'ютерів.

Кожна топологія мережі накладає ряд умов. Може диктувати не лише типи кабелю, але і спосіб його прокладки.

Топологія може також визначати спосіб взаємодії комп'ютерів в мережі. Різним видам топологій відповідають різні методи взаємодії, і ці методи роблять великий вплив на мережу.

Всі мережі будуються на основі трьох базових топологій:

- шина (bus);
- зірка (star);
- кільце (ring).

Якщо комп'ютери підключені уздовж одного кабелю, топологія називається шиною. У тому випадку, коли комп'ютери підключені до сегментів

кабелю, витікаючи з однієї крапки, або концентратора, топологія називається зіркою. Якщо кабель, до якого підключені комп'ютери, замкнутий в кільце, така топологія носить назву кільця.

Хоча самі по собі базові топології нескладні, в реальності часто зустрічаються досить складні комбінації, які об'єднуючи властивості декілька топологій.

Топологія "шина"

Цю топологію часто звать "лінійною шиною" (linear bus). Дана топологія відноситься до найбільш простих і широко поширених топологій. У ній використовується один кабель, який зветься магістраллю або сегментом, уздовж якого паралельно підключені всі комп'ютери мережі (рисунок 3.1).



Рисунок 3.1 - Проста мережа з топологією "шина"

У мережі з топологією "шина" комп'ютери адресують дані конкретному комп'ютеру, передавая їх по кабелю у вигляді електричних сигналів.

Дані у вигляді електричних сигналів передаються всім комп'ютерам мережі, проте інформацію приймає лише той, адреса якого відповідає адресі одержувача, зашифрований в цих сигналах. Причому в кожен момент часу лише один комп'ютер може вести передачу (рисунок 3.2).

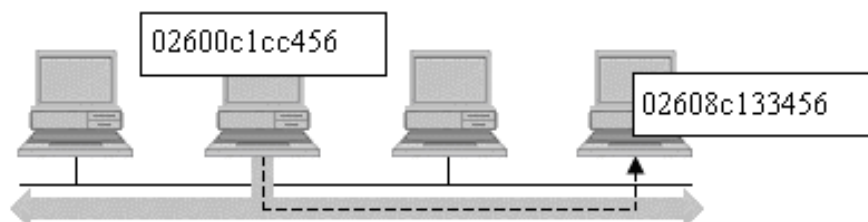


Рисунок 3.2 - Дані посилаються всім комп'ютерам, але приймає їх лише адресат

Так як дані в мережі передаються лише одним комп'ютером, її продуктивність залежить від кількості комп'ютерів підключених до шини. Чим більше комп'ютерів, що чекають передачі даних, тим повільніше мережа.

Проте вивести пряму залежність між пропускнуою спроможністю мережі і кількістю комп'ютерів в ній не можна. Бо, окрім числа комп'ютерів, на швидкодію мережі впливає безліч чинників, у тому числі:

- характеристики апаратного забезпечення комп'ютерів в мережі;
- частота, з якою комп'ютери передають дані;
- тип працюючих мережевих застосувань;
- тип мережевого кабелю;
- відстань між комп'ютерами в мережі.

Шина - пасивна топологія. Це означає, що комп'ютери лише "слухають" передані по мережі дані, але не переміщують їх від відправника до одержувача. Тому, якщо один з комп'ютерів вийде з ладу, це не позначиться на роботі останніх. У активних топологіях комп'ютери регенерують сигнали і передають їх по мережі.

Дані, або електричні сигнали, поширюються по всій мережі - від одного кінця кабелю до іншого. Якщо не робити жодних спеціальних дій, сигнал, досягаючи кінця кабелю, відбиватиметься і не дозволить іншим комп'ютерам здійснювати передачу. Тому, після того, як дані досягнуть адресата, електричні сигнали необхідно погасити.

Щоб запобігти віддзеркаленню електричних сигналів, на кожному кінці кабелю встановлюють термінатори (terminators), що поглинають ці сигнали.

Топологія "зірка"

При топології "зірка" всі комп'ютери за допомогою сегментів кабелю підключаються до центрального компонента, який називається концентратором (hub). Сигнали від передавального комп'ютера поступають через концентратор. Сигнали від передавального комп'ютера поступають через концентратор до всіх останніх (рисунок 3.3).

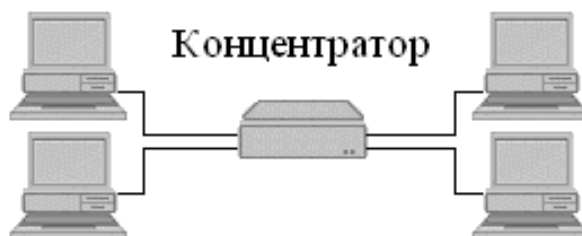


Рисунок 3.3 - Проста мережа з топологією "зірка"

У мережах з топологією "зірка" підключення кабелю і управління конфігурацією мережі проходить централізовано. Але є і недолік: оскільки всі комп'ютери підключені до центральній крапки, для великих мереж значно збільшується витрата кабелю. До того ж, якщо центральний компонент вийде з ладу, порушиться робота всієї мережі.

А якщо вийде з ладу лише один комп'ютер (або кабель, що сполучає його з концентратором), то лише цей комп'ютер не зможе передавати або приймати дані по мережі. На решту комп'ютерів в мережі це не вплине.

Топологія "кільце"

При топології "кільце" комп'ютери підключаються до кабелю, замкнутого в кільце. Тому у кабеля просто не може бути вільного кінця, до якого треба підключати термінатор. Сигнали передаються по кільцю в одному напрямі і проходять через кожен комп'ютер. На відміну від пасивної топології "шина" тут кожен комп'ютер виступає в ролі репітера, підсилюючи сигнали і передаючи їх наступному комп'ютеру. Тому, якщо вийде з ладу один комп'ютер, припиняє функціонувати вся мережа (рисунок 3.4).

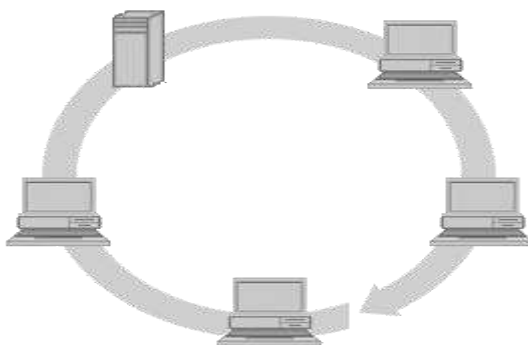


Рисунок 3.4 - Проста мережа з топологією "кільце"

Один з принципів передачі даних в кільцевій мережі носить назву передачі маркера. Маркер послідовно, від одного комп'ютера до іншого, передається до тих пір, поки його не отримає той, який "хоче" передати дані. Передавальний комп'ютер змінює маркер, поміщає електронну адресу в дані і посилає їх по кільцю (рисунк 3.5).

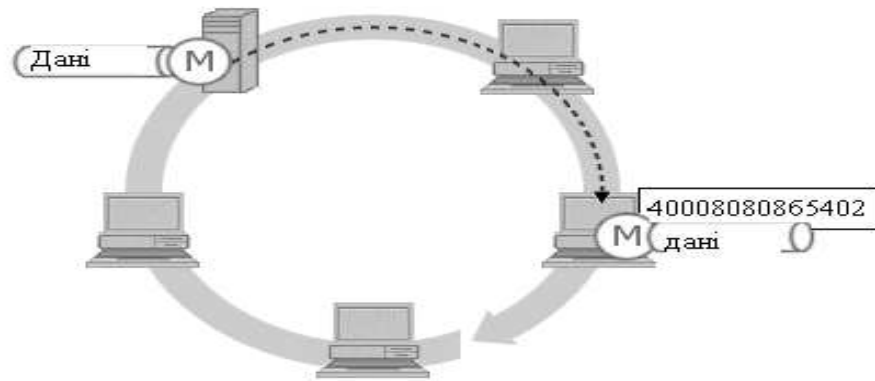


Рисунок 3.5 - Комп'ютер захоплює маркер і передає його по кільцю

Після цього приймаючий комп'ютер посилає передавальному комп'ютеру повідомлення, де підтверджує факт прийому даних. Отримавши підтвердження, передавальний комп'ютер створює новий маркер і повертає його в мережу.

На перший погляд видається, що передача маркера віднімає багато часу, проте насправді маркер пересувається практично із швидкістю світла. У кільці маркер може циркулювати з частотою 10 000 зворотів в секунду.

Комбіновані топології

В даний час часто використовуються топології, які комбінують компоновку мережі за принципом шини, зірки і кільця.

Зірка-шина (star-bus) - це комбінація топологій "шина" і "зірка". Найчастіше це виглядає так: декілька мереж з топологією "зірка" об'єднуються за допомогою магістральної лінійної шини.

В цьому випадку вихід з ладу одного комп'ютера не робить жодного впливу на мережу - решта комп'ютерів як і раніше взаємодіє один з одним. А

вихід з ладу концентратора спричинить зупинку підключених до нього комп'ютерів і концентраторів (рисунок 3.6).



Рисунок 3.6 - Мережа з топологією "зірка-шина"

Зірка-кільце (star-ring) видається декілька схожою на зірку-шину. І у тій, і в іншій топології комп'ютери підключені до концентратора, який фактично і формує кільце або шину. Відзнака в тому, що концентратори в зірці-шині сполучені магистральною лінійною шиною, а в зірці-кільці на основі головного концентратора вони утворюють зірку (рисунок 3.7).



Рисунок 3.7 - Мережа з топологією "зірка-кільце"

Існує безліч чинників, які необхідно враховувати при виборі найбільш відповідної до даної ситуації топології [2]. Переваги та недоліки різних топологій наведені в таблиці 3.1

Таблиця 3.1 - Переваги та недоліки різних топологій

Топологія	Переваги	Недоліки
Шина	Економна витрата кабелю. Порівняно недорога і нескладна у використанні середя передачі. Простота, надійність. Легко розширюється	При значних об'ємах графіка зменшується пропускна спроможність мережі. Важко локалізувати проблеми. Вихід з буд кабелю зупиняє роботу багатьох користувачів
Кільце	Всі комп'ютери мають рівний доступ. Кількість користувачів не робить скільки-небудь значного впливу на продуктивність	Вихід з буд одного комп'ютера може вивести з буд всю мережу. Важко локалізувати проблеми. Зміна конфігурації мережі вимагає зупинки роботи всієї мережі
Зірка	Легко модифікувати мережу, додаючи нові комп'ютери. Централізований контроль і управління. Вихід з буд одного комп'ютера не впливає на працездатність мережі	Вихід з буд центрального вузла виводить з ладу всю мережу

3.1.2 Архітектура локальних мереж

Архітектура мережі визначає основні елементи мережі, характеризує її загальну логічну організацію, технічне забезпечення, програмне забезпечення, описує методи кодування. Архітектура також визначає принципи функціонування й інтерфейс користувача. Найбільш поширені три типи мережевих архітектур:

- архітектура «термінал – головний комп'ютер»;
- однорангова архітектура;
- архітектура «клієнт – сервер».

Архітектура «термінал - головний комп'ютер» (terminal - host computer architecture) - це концепція інформаційної мережі, у якій вся обробка даних здійснюється одним або групою головних комп'ютерів.

Ця архітектура припускає два типа встаткування:

- головний комп'ютер, де здійснюється керування мережею, зберігання й обробки даних;

- термінали, призначені для передачі головному комп'ютеру команд на організацію сеансів і виконання завдань, введення даних для виконання завдань й одержання результатів.

Головний комп'ютер через мультиплексори передачі даних взаємодіє із терміналами.

Однорангова архітектура (peer-to-peer architecture) - це концепція інформаційної мережі, у якій її ресурси розосереджені по всіх системах. Дана архітектура характеризується тим, що в ній всі системи рівноправні.

До однорангових мереж відносяться малі мережі, де будь-яка робоча станція може виконувати одночасно функції файлового сервера й робочої станції. В однорангових комп'ютерних мережах дисковий простір і файли на будь-якому комп'ютері можуть бути загальними. Щоб ресурс став загальним, його необхідно віддати в загальне користування, використовуючи служби віддаленого доступу мережних однорангових операційних систем. Однорангові ЛОМ досить якісні тільки для невеликих робочих груп.

Використання однорангової архітектури не виключає застосування в тій же мережі також архітектури «термінал - головний комп'ютер» або архітектури «клієнт - сервер».

Архітектура «клієнт – сервер» (client-server architecture) – це концепція інформаційної мережі, у якій основна частина її ресурсів зосереджена в серверах, що обслуговують своїх клієнтів. Розглянута архітектура була прийнята для побудови локальної мережі при побудові локальної мережі підприємства і визначає два типи компонентів: сервери й клієнти.

Сервер – це об'єкт, що надає сервіс іншим об'єктам мережі по їхніх запитах. Сервіс – це процес обслуговування клієнтів.

Сервер працює по завданнях клієнтів й управляє виконанням їхніх завдань. Після виконання кожного завдання сервер посилає отримані результати клієнтові, що послав це завдання.

Сервісна функція в архітектурі клієнт – сервер описується комплексом прикладних програм, відповідно до якого виконуються різноманітні прикладні процеси.

Процес, що викликає сервісну функцію за допомогою певних операцій, називається клієнтом. Ним може бути програма або користувач.

У сучасній клієнт – серверній архітектурі виділяється чотири групи об'єктів: клієнти, сервери, дані й мережні служби. Клієнти розташовуються в системах на робочих місцях користувачів. Дані в основному зберігаються в серверах. Мережні служби є спільно використовуваними серверами й даними. Крім того служби управляють процедурами обробки даних [3].

Мережі клієнт - серверної архітектури мають наступні переваги:

- дозволяють організовувати мережі з більшою кількістю робочих станцій;
 - забезпечують централізоване керування обліковими записами користувачів, безпекою й доступом, що спрощує мережне адміністрування;
 - ефективний доступ до мережних ресурсів;
- користувачеві потрібний один пароль для входу в мережу й для одержання доступу до всіх ресурсів, на які поширюються права користувача.

Поряд з перевагами мережі клієнт - серверної архітектури мають і ряд недоліків:

- несправність сервера може зробити мережу непридатною, як мінімум втрату мережних ресурсів;
- вимагають кваліфікованого персоналу для адміністрування;
- мають більше високу вартість мереж і мережного встаткування.

3.1.3 Технології локальних мереж

Технологія описує як працює мережа. Найбільш поширені чотири технології: Ethernet, Token Ring, ARCNET і FDDI.

Першою з'явилася технологія Ethernet - в другій половині 70-х років (рисунки 3.8). Її розробили спільно фірми DEC, Intel і Xerox. В даний час ця технологія найбільш доступна і популярна.

Кожна станція працює в Ethernet згідно принципу «Слухай канал передачі, перш ніж відправити повідомлення; слухай, коли відправляєш; припини роботу у разі перешкод і спробуй ще раз».

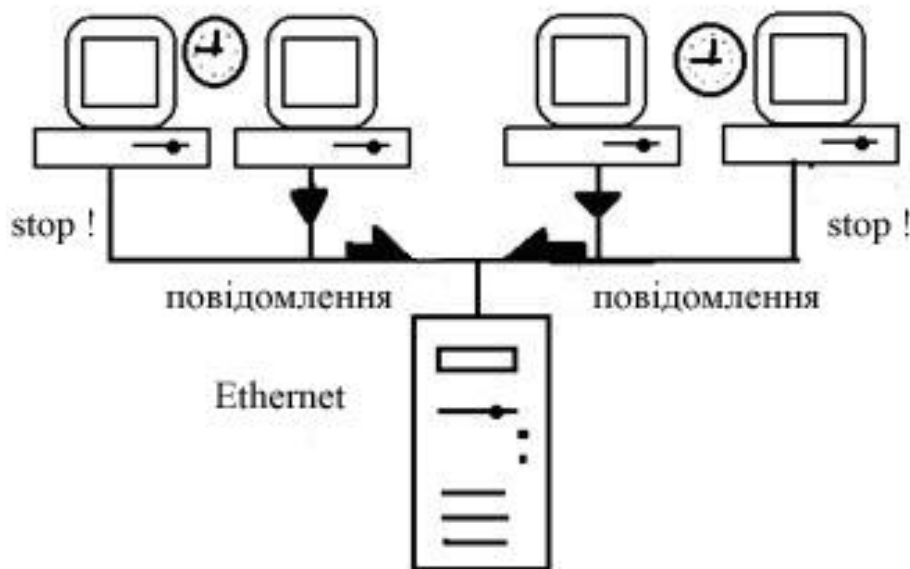


Рисунок 3.8 - Принцип технології Ethernet

Даний принцип можна розшифрувати (пояснити) таким чином:

- нікому не дозволяється посилати повідомлення в той час, коли цим зайнятий вже хтось інший (слухай перед тим, як відправити);
- якщо два або декілька відправників починають посилати повідомлення приблизно в один і той же момент, рано чи пізно їх повідомлення «зіткнуться» один з одним в дроті, що називається колізією.

Колізії неважко розпізнати, оскільки вони завжди викликають сигнал перешкоди, який не схожий на допустиме повідомлення. Ethernet може розпізнати перешкоди і примушує відправника припинити передачу, почекати якийсь час, перш, ніж повторно відправити повідомлення.

Причини широкої поширеності і популярності (достоїнства Ethernet):

- дешевизна;
- великий досвід використання;
- нововведення, що продовжуються;
- багатство вибору.

Багато виготівників пропонують апаратуру побудови мереж, що базується на Ethernet.

Недоліки Ethernet:

- можливість зіткнень повідомлень (колізії, перешкоди);
- у разі великого завантаження мережі час передачі повідомлень непередбачено.

Молодшою, в порівнянні з Ethernet, є технологія Token Ring (рисунок 3.9). Вона була розроблена фірмою IBM. Технологія орієнтована на кільце, по якому постійно рухається маркер.

Кожна станція працює в Token Ring згідно принципу «Чекати маркера, якщо необхідно послати повідомлення, приєднати його до маркера, коли він проходить мимо. Якщо проходить маркер, зняти з нього повідомлення і послати маркер далі».

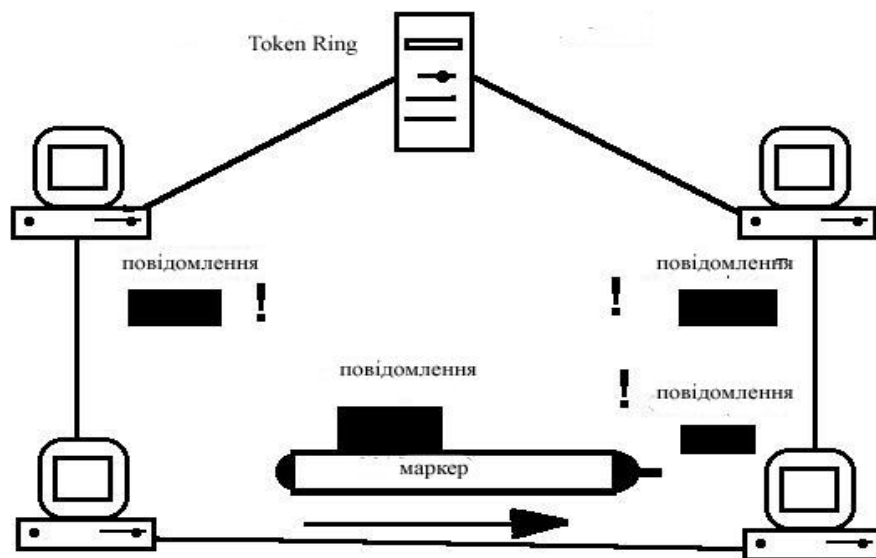


Рисунок 3.9 - Принцип технології Token Ring

Переваги:

- гарантована доставка повідомлень;
- висока швидкість (160 % Ethernet).

Недоліки:

- необхідні дорогі пристрої доступу до середовища;
- технологія складніша в реалізації;
- необхідні два кабелі (для підвищення надійності): один входить,

інший витікаючий від комп'ютера до концентратора (2-а модифікація кільця, комутатор);

- висока вартість (160-200 % від Ethernet).

Технологія ARCNET була розроблена фірмою Datapoint Corporation (рисунок 3.10). Принцип роботи мережі ARCNET аналогічний Token Ring, тобто використовується маркер для дозволу станції передати інформацію у відповідний момент часу.

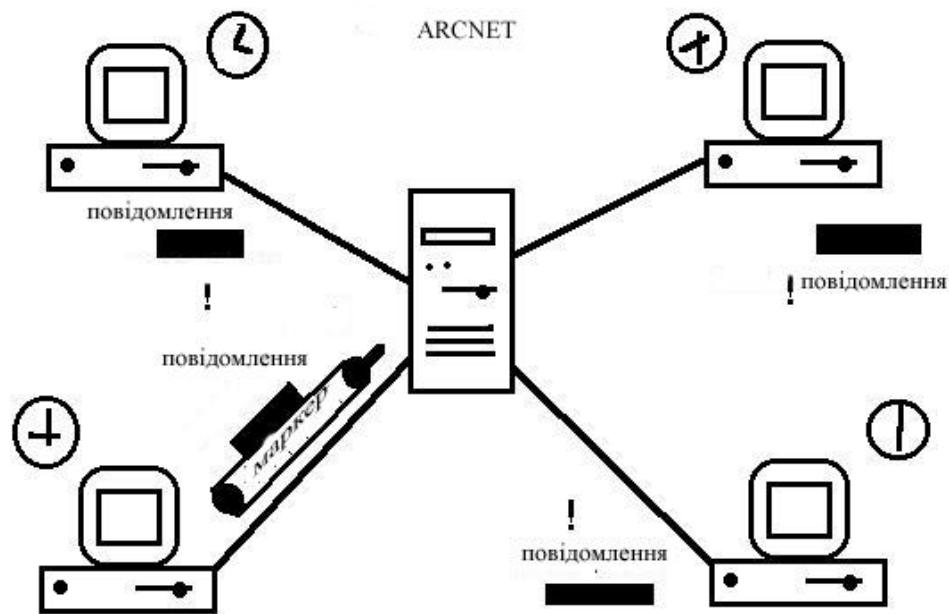


Рисунок 3.10 - Принцип технології Arcnet

Проте «спосіб» реалізації маркера тут відмінний від Token Ring. Крім того, технологія ARCNET орієнтована на шину (у разі коаксіального кабелю) або зірку (за наявності виті парі дротів).

Переваги ARCNET:

- невисока вартість(найдешевша);
- простота використання;
- гнучкість.

Недоліки:

- низька швидкодія (1/4 Ethernet, 1/2 - 1/7 Token Ring);
- погано працює в умовах мультимедіа, режимі реального часу;

- відсутні перспективи розвитку.

Переваги:

- дуже висока швидкість передачі;
- кільце може бути колом до 200 км і включати до 1000 пристроїв.

Недоліки:

- висока вартість.

3.1.4 Види мережевих протоколів

У моделі OSI розрізняється два основні типи протоколів. У протоколах зі встановленням з'єднання (connection-oriented network service, CONS) перед обміном даними відправник і одержувач повинні спочатку встановити з'єднання і, можливо, вибрати протокол, який вони використовуватимуть. Після завершення діалогу вони повинні розірвати це з'єднання.

Друга група протоколів – протоколи без попереднього встановлення з'єднання (connectionless network service, CLNS). Такі протоколи називаються також дейтаграмними протоколами. Відправник просто передає повідомлення, коли воно готове. При взаємодії комп'ютерів використовуються як ті, так і інші протоколи.

Особливості протоколів, використовуваних в локальних і глобальних мережах.

В даний час спостерігається тенденція до зближення протоколів локальних і глобальних мереж. Відмінності між протоколами локальних і глобальних мереж відбуваються в основному через відмінності між властивостями каналів, що використовуються в цих мережах.

Канали локальних мереж мають невелику довжину і високу якість, а канали глобальних мереж – навпаки, велику довжину і низьку якість.

Практично всі протоколи локальних мереж мають версію роботи на середовищах передачі даних, що розділяються, хоча пізніші протоколи (Fast Ethernet, Gigabit Ethernet) мають також і версію роботи на індивідуальних каналах в повнодуплексному режимі. Велика протяжність каналів глобальних мереж робить нераціональними будь-які процедури розділення каналу в часі,

оскільки тривалість цих процедур стає дуже великою. Тому канали глобальних мереж використовуються завжди на індивідуальній основі як зв'язку типу "точка-точка".

Висока якість кабелів локальних мереж послужила причиною відмови від використання в протоколах локальних мереж процедур відновлення спотворених і втрачених кадрів. Цих процедур немає ні в протоколах сімейства Ethernet, ні у протоколі Token Ring, ні у протоколі FDDI. В той же час в протоколах глобальних мереж, що орієнтуються на канали поганої якості, процедурам відновлення кадрів завжди надавалася велика увага [2].

3.2 Мережна архітектура ЛОМ підприємства ТОВ «Терновський хлібзавод»

3.2.1 Вибір мережевої архітектури

При розробці ЛОМ було обрано клієнт серверну мережу тому що:

- кількість користувачів перевищує десять;
- потрібне централізоване керування, безпека, керування ресурсами або резервне копіювання;
- необхідний спеціалізований сервер;
- потрібний доступ до глобальної мережі;
- потрібно розділяти ресурси на рівні користувачів.

3.2.2 Вибір топології проекту

Вибір топології залежить від умов, завдань і можливостей, або ж визначається стандартом використовуваної мережі. Основними факторами, що впливають на вибір топології для побудови мережі, є:

- середовище передачі інформації (тип кабелю);
- метод доступу до середовища;
- максимальна довжина мережі;
- пропускна здатність мережі;

– метод передачі й ін.

У даному проекті ставиться завдання зв'язати робочі станції підприємства між собою за допомогою високошвидкісної мережі із швидкістю передачі даних – 100 Мбіт/с. При проектуванні локальної мережі підприємства ТОВ «Терновський хлібзавод» слід обрати топологію ієрархічної зірки, оскільки основною гідністю зіркоподібної структури є незалежність кожного радіального напрямку від інших, тобто неполадки на одній з ділянок кабелю ніяк не вплинуть на роботу решти користувачів (рисунок 3.11).

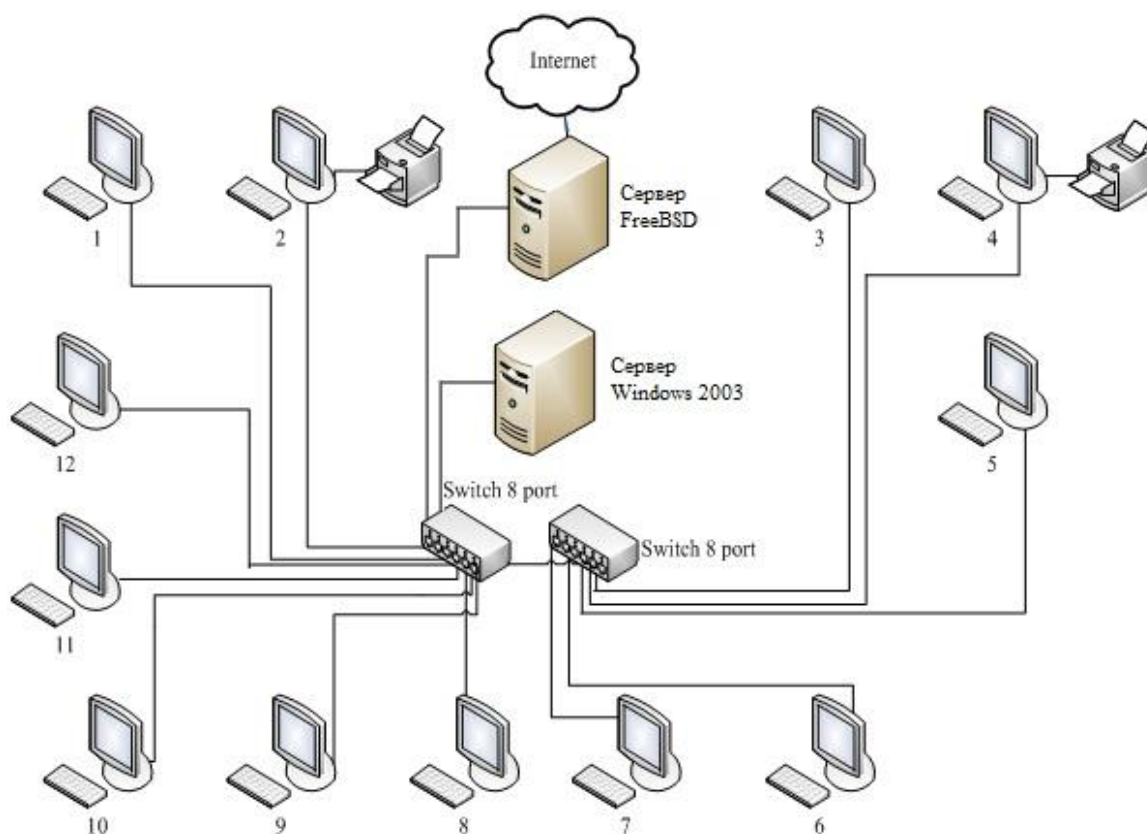


Рисунок 3.11 – Структурна схема ЛОМ

3.2.3 Вибір технології проекту

Для побудови мережі використовується варіант технології Fast Ethernet.

Даний стандарт передбачає швидкість передачі даних 100 Мбіт/с і підтримує два види передавального середовища - неекранована кручена пара й

волоконно-оптичний кабель. Для опису типу передавального середовища використовуються наступні аббревіатури надані в таблиці 3.2.

Таблиця 3.2 - Стандарт Fast Ethernet

Назва	Тип передавального середовища
100 Base-T	Основна назва для стандарту Fast Ethernet (включає всі типи передавальних середовищ)
100 Base-TX	Екранованої або неекранована кручена пари категорії 5 і вище
100 Base-FX	Богатомодовий двоволоконний оптичний кабель
100 Base-T4	Кручена пари. 4 пари категорії 3, 4 або 5.

Наступні топологічні правила й рекомендації для 100 Base-TX і

100 Base-FX мереж засновані на стандарті IEEE 802.3u:

а) 100 Base-TX.

Правило 1: Мережна топологія повинна бути фізичною топологією типу «зірка» без відгалужень або зациклень.

Правило 2: Повинен використовуватися кабель категорії 5 або 5е.

Правило 3: Клас використовуваних повторювачів визначає кількість концентраторів, які можна каскадувати.

– Клас 1. Можна каскадувати (стикувати) до п'яти включно концентраторів, використовуючи спеціальний каскадуючий кабель.

– Клас 2. Можна каскадувати (стикувати) тільки два концентратори, використовуючи кручену пару для з'єднання залежних портів MDI обох концентраторів.

Правило 4: Довжина сегмента обмежена 100 метрами.

Правило 5: Діаметр мережі не повинен перевищувати 205 метрів.

Правило 6: Метод доступу CSMA/CD.

б) 100 Base-FX.

Правило 1: Максимальна відстань між двома пристроями - два кілометри при повнодуплексному зв'язку й 412 метрів при напівдуплексному для з'єднань, що комутуються.

Правило 2: Відстань між концентратором і кінцевим пристроєм не повинна перевищувати 208 метрів.

Для реалізації проекту обираємо технологію Fast Ethernet, а в якості передавального середовища неекрановану кручену пару категорії 5.[9].

3.3 Організація мережі на основі ОС

Ключовою ланкою мережі є мережева ОС. Тому постає питання вибору ОС відповідно до виділених коштів та часу на впровадження та запуск системи. Практично всі сучасні ОС підтримують роботу в мережі. Однак у якості ОС для сервера найчастіше використовуються Unix, Linux і Windows Server 2003. На користь ОС від корпорації Microsoft свідчить надзвичайна розповсюдженість як різних продуктів цієї компанії, так і величезна кількість програм та програмних засобів сторонніх виробників для ОС цієї компанії. Слід також зауважити, що ОС сімейства Windows відрізняються деякою нестабільністю в роботі, і наявністю великої кількості програмних «лазів», які може використати зловмисник щоб отримати повний контроль над машиною, що працює під управлінням цих ОС. Ці недоліки виправляються «заплатами», або Service Pak'ами, які інсталиються на вже працюючу систему. Але на виявлення помилок в коді ОС, та на випуск Service Pak потрібен час, і тому є ризик «хакінгу», або проникненню в систему ОС Linux стала привабливою альтернативою комерційних ОС для всіх, хто працює на персональних комп'ютерах, бо в ній зосереджені потужність та гнучкість робочої UNIX-станції, можливість користування повним набором програмного забезпечення Internet, та повнофункціональний графічний інтерфейс (наприклад X Window). У фінансовому аспекті Linux має одну значну перевагу – це не комерційний продукт, а тому, на відміну від інших ОС, розповсюджується вільно, за відкритою генеральною ліцензією GNU в рамках Фонду вільного програмного забезпечення (Free Software Foundation), що робить Linux доступним для всіх бажаючих.

Як і всі UNIX-системи, Linux багатозадачна та розрахована на велику кількість користувачів операційна система. Головним її принципом є «Все

потрібне збери собі сам». Дійсно, Linux являє собою ядро плюс модулі плюс програмне забезпечення. І те, і інше, і навіть ядро користувач може скомпілювати на основі «сирців», тобто коду програм, які поставляються разом з ОС, під свої конкретні задачі та потреби. Цей принцип у поєднанні з прозорістю та гнучкістю конфігурації забезпечує Linux надзвичайну потужність, стабільність та ефективність при досить низьких вимогах до апаратного забезпечення.

3.3.1 ОС Unix Linux

ОС Unix є найстаршою мережною операційною системою (створена в 1969р.) і по сьогоднішній день використовується в Internet. Існує безліч клонів Unix - практично нічим не відрізняються друг від друга операційних систем різних виробників: FreeBSD, BSD Unix (університет Berkley), SunOS, Solaris (фірма Sun Microsystems), AIX (фірма IBM), HP-UX (фірми Hewlet Packard), SCO (фірми SCO) і ін.

До клонів Unix можна віднести й Linux, однак останнім часом він виділився в самостійну операційну систему й продовжує бурхливо розвиватися. Існує безліч дистрибутивів (пакетів установки) Linux різних фірм. Самі популярні з них - це Red Hat Linux (США) і Mandrake (Європа). Існують також Slackware Linux, Corel Linux, Caldera OpenLinux, Debian Linux, SuSE Linux, Black Cat Linux, Connectiva Linux і ін. Структура файлової системи, система розмежування доступу й основні команди в Linux і Unix подібні. Основною відмінністю Linux від ранніх версій Unix є зручний графічний інтерфейс, багато в чому подібний з інтерфейсом Windows (особливо в графічного робітничого середовища Gnome), а основною перевагою, у порівнянні з Windows, більша надійність і швидкість роботи, більша захищеність файлової системи (у тому числі й від вірусів) і більше професійні засоби роботи з локальною мережею й Internet. Для Linux існує й розробляється велика кількість програмного забезпечення: від офісного пакета Star Office і графічного редактора Corel Draw, до потужних СУБД (DB2 фірми IBM) і систем розробки програм на C++, Perl, Java і ін.

Найголовнішим достоїнством ОС Linux є те, що ця система розповсюджується безкоштовно. Також Linux практично не сприйнятлива до вірусів, оскільки багато хто з них написаний під Windows. У систему інтегрована велика кількість програм у вигляді пакетів, чого немає в Windows. Крім того, Linux має мінімальні системні вимоги, і завжди існує можливість набудувати систему під себе, природно за наявності відповідних знань. Основні ж недоліки Linux пов'язані з її низькою популярністю. Це і відсутність багатьох драйверів, деяких кодеків для відео, і неможливість підтримки сучасних ігор.

Переваги ОС Linux:

- доступність початкового коду. Оскільки вся система Linux поставляється за ліцензією GNU, то у людини, що достатньо розбирається, взагалі є можливість зібрати свою власну операційну систему і займатися її просуванням і розвитком.
- свобода вибору і менша вартість;
- налаштуваність;
- відкритість початкового коду дає людині можливість допрацювати програму повністю під свої потреби;
- забезпечення безпеки.

Недоліки ОС Linux:

- сумісність з апаратурою, технічна підтримка. Це полягає в тому, що виробники апаратури обходили Linux стороною, не виготовляючи для цієї ОС драйвери і необхідне ПЗ.
- нестабільність. Внаслідок того, що дуже багато людей зараз залучено в розробку і модифікацію програм для Linux, різні версії бібліотек, додатків і ядра змінюють один одного із зростаючою швидкістю. При цьому, часто, зворотна сумісність, та і якість коду, залишають бажати кращого.
- складність в розумінні звиканні [4].

3.3.2 ОС Windows Server 2003

Мережева операційна система виконується на мережевому сервері. З іншого боку, комп'ютери – клієнти можуть працювати під управлінням різних операційних систем. Щоб операційна система клієнта могла використовувати мережу, потрібно встановити спеціальні драйвери, які дозволять платі мережевого інтерфейсу комп'ютера-клієнта зв'язатися з мережею. Ці драйвери працюють подібно драйверам принтера, дозволяючи прикладним програмам посилати інформацію на принтер. Програмне забезпечення мережевого драйвера дає можливість програмам посилати і приймати інформацію по мережі. Кожен комп'ютер в мережі містить одну або більш плат мережевого інтерфейсу, яка з'єднує комп'ютер з мережею.

ОС Windows Server 2003 розроблена спеціально для малого бізнесу й невеликих відділів компаній і забезпечує ефективне створення загального доступу до файлів і принтерів, безпечне підключення до Інтернету, централізоване розгортання настільних додатків і веб-рішення для організації взаємодії співробітників, партнерів, клієнтів. Сервер Windows Server 2003 забезпечує високий рівень надійності, масштабованості й безпеці.

Сімейство продуктів Windows Server 2003 засновано на ефективному застосуванні технології ОС Windows 2000 Server і робить більше зручним розгортання, керування й використання. У результаті користувач одержує високопродуктивну операційну систему, що є безпечним і надійним рішенням, що не вимагає проведення спеціального налаштування й що забезпечує високий рівень доступності й масштабованості.

Windows Server 2003 на високому рівні забезпечує підтримку наступних можливостей:

- розширені можливості служби перевірки дійсності в Інтернеті (IAS);
- мережний міст;
- загальний доступ до підключень Інтернету (ICS);
- двостороння симетрична багатопроцесорна обробка (SMP);

ОС Windows Server 2003 містить удосконалені технології, уперше використані в сервері Windows 2000 Server, у тому числі підтримку старт – карт, смуг пропущення й технологію Plug and Play.

Служба Active Directory має підвищену гнучкість, продуктивністю й безпекою при підключенні до ненадійних глобальних мереж (WAN) завдяки більшій ефективній синхронізації й реплікації, а також кешированню облікових даних у контролерах доменів дочірніх підрозділів.

Нові принципи роботи на основі завдань у сімействі Windows Server 2003 значно полегшують виконання звичайних дій. Удосконалення консолі керування MMC і служби Active Directory підвищують продуктивність і роблять керування більше зручним.

Сімейство Windows Server 2003 включає кілька нових корисних засобів автоматичного керування, у тому числі службу Microsoft Software Update Service (SUS, служба Microsoft для автоматичного відновлення програм) і майстер налаштування серверів для автоматизації розгортання. Керування груповою політикою стало більше зручним завдяки новій консолі Group Policy Management Console, що дозволяє компаніям оптимізувати використання служби Active Directory і завдяки цьому підвищити ефективність керування. Крім того, засобу командного рядка дозволяють адміністраторові виконувати більшість завдань прямо з консолі.

Удосконалення й нові можливості роботи в мережі сімейства продуктів Windows Server 2003 розширюють функціональність, керуваність і надійність мережної інфраструктури. Сімейство Windows Server 2003 забезпечує зв'язок з інформаційним середовищем компанії практично з будь-якого місця й за допомогою будь-якого пристрою. Служби Microsoft Windows Media сімейства Windows Server 2003 надають надійний масштабований засіб для ефективного керування динамічним вмістом. Служби Windows Media перетворюють сімейство Windows Server 2003 в ідеальну платформу для поширення потокового аудіо й відео вмісту у внутрішніх мережах компанії або через Інтернет.

Не менш важлива оптимізована підтримка технологій Microsoft .NET і веб – служб XML, що споконвічно присутні в ОС Windows Server 2003, що представляє значний крок уперед у створенні платформи для розробки, поширення й забезпечення роботи веб – служб XML.

Технологія Microsoft .NET глибоко інтегрована в сімейство продуктів Windows Server 2003. Вона забезпечує безпрецедентний рівень програмної інтеграції за допомогою веб – служб XML: відособлені модульні додатки, які підключаються друг до друга, так само як і до інших більших додатків через Інтернет.

Технологія Microsoft.NET, впроваджена в більшість продуктів платформи Microsoft, дозволяє швидко й надійно розробляти, розгортати й застосовувати безпечні рішення з мережними підключеннями. Платформа Microsoft включає набір засобів для розробки, клієнтські додатки, веб –служби XML і сервери, що дозволяють домогтися тісної інформаційної взаємодії, необхідного для ефективного ведення діяльності в сучасному діловому середовищі.

Настроювання безпеки служб IIS 6.0 у процесі установки відключені за замовчуванням, що гарантує запуск тільки необхідних служб. Це відмінність від більше ранніх версій значно знижує рівень початкового ризику.

Directory services. Настроювання безпеки служби Active Directory для користувачів і мережних ресурсів мають величезну гнучкість і діапазоном і перетворюють концепцію абсолютно захищеної мережі в реальність.

Internet firewall. Підключення до інтернету стало більше безпечним завдяки убудованому брандмауєрові (міжмережевому екрану). Інтеграція брандмауєра в операційну систему дозволяє знизити витрати на підключення до Інтернету.

Remote access. Користувачі з комутирується підключенням, що, до інтернету можуть бути піддані карантину за допомогою відповідної політики адміністрування. Можна обмежити їхній доступ до мережі до підтвердження наявності в їхніх системах необхідного ПО, певного адміністратором, наприклад відновлень антивірусних додатків.

Application verification. Додатка, запущені на сервері Windows Server 2003 можуть бути протестовані за допомогою засобу Application Verifier (засіб перевірки додатків). Цей засіб орієнтований на виявлення схованих проблем, таких як ушкодження програмної купи й проблеми сумісності.

Server event tracking. Адміністратори мають можливість вести точний облік працездатного стану системи за допомогою засобу реєстрації часу відключення сервера. Цей засіб записує час завершення роботи сервера в спеціальний журнал

Shadow copy. Ця можливість забезпечує надійність і адекватність версій загальних мережних ресурсів. Адміністратори мають можливість переглянути вміст загального мережного ресурсу, що існував у певний момент часу. Кінцеві користувачі можуть відновити ненавмисно вилучені файли або загальні мережні ресурси без втручання адміністратора.

Web application server role. Продукт Windows Server 2003 також є повноцінним сервером веб-додатків. Інтеграція структурної основи .NET Framework у головні серверні ресурси полегшує розробку, розгортання й керування додатками й веб-службами XML.

Структура NET Framework забезпечує захищену, повністю контрольовану середовище для роботи додатків, що володіє багатими можливостями, а також більше зручну розробку й розгортання й бездоганну інтеграцію з різними мовами програмування. Сімейство Windows Server 2003 засноване на промислових стандартах, що дозволяють користувачам розширювати функціональність наявних програм і швидко створювати нові додатки.

До переваг ОС Windows можна віднести:

- дружній призначений для користувача інтерфейс. Будучи широко поширеним, інтерфейс Windows, мабуть, знайомий абсолютно всім. Навіть у середовищі Linux в даний час існують настройки графічного інтерфейсу, що дозволяють імітувати інтерфейс Windows.

- простота установки. Установка програм в середовищі Windows (так, дуже часто і самій ОС) є вельми простий процес, з яким легко може справитися навіть дитина. Крім того, завжди є включений режим установки "за

умовчанням", коли на ПК користувача буде встановлена якась стандартна конфігурація додатку.

- великий вибір доступного ПЗ

Недоліки ОС Windows:

- недостатній рівень забезпечення безпеки;
- нестабільність програм сторонніх виробників.

Мінімальні апаратні вимоги Windows Server 2003:

- Pentium-Сумісний процесор тактовою частотою не нижче 133 МГц;
- Windows Server підтримує до чотирьох процесорів;
- 128 Мб ОЗУ (рекомендується 256 Мб). Більша кількість пам'яті значно збільшує швидкодію системи. Windows Server 2003 підтримує ОЗУ обсягом до 4 Гб;
- вільні дискові простори 20 Гб - для установки Windows Server 2003 потрібно близько 15 Гб. Додаткове місце на диску необхідно для установки мережних компонентів.

Тому, спираючись на наведені вище факти, для сервера БД було обрано ОС сімейства Windows Server 2003/ SP 2 з використанням служби Terminal Server. Сервер терміналів дозволяє одержати доступ до запущеного на ньому додаткам із застарілих пристроїв. Наприклад, користувачі можуть працювати з віртуальним робочим столом Windows XP Professional і додатками x86 на комп'ютерах, що не дозволяють працювати із цими засобами локально.

Як операційну систему для сервера шлюза доступу до мережі Internet була обрана ОС FreeBSD 8.1. Ця система є дуже надійною. Має широкий спектр налаштувань мережі. Є надійним фаєрволом між локальною мережею і зовнішнім світом. До того ж вона розповсюджується безкоштовно за ліцензією GNU

Операційну систему для робочих станцій була обрана Windows XP Professional, вона розроблена для оснащення настільних робочих станцій корпоративних користувачів. Вона оптимізована для виконання функцій мережного клієнта й керування роботою персональної робочої станції [10].

3.4 Вибір устаткування ЛОМ

Для реалізації проекту локальної мережі на підприємстві ТОВ «Терновський хлібзавод» треба вибрати мережне та комутаційне обладнання, кабельну систему та обладнання для відео спостереження.

3.4.1 Кінцеве мережне обладнання

Як сервер для керування даних центрального файлового сервера повинен бути використаний комп'ютер з характеристиками не нижче, ніж наступні:

- не менш двох процесорів з параметрами не нижче: Pentium-3 1500 MHz, з об'ємом L 2-cache не менш 256 кб;
- оперативна пам'ять не менш 512 Мб;
- об'ємом дискового простору не менш 40 Гб;
- інтерфейс дисків - не нижче Ultra-3 Wide SCSI;
- дисковод DVD-RW;
- мережна карта 100 Base-TX.

Конфігурація обираємого сервера БД:

- процесор Intel Core 2 Quad Частота (2,66 ГГц);
- материнська плата Intel (G41) 6 USB / 1 x PCI-Ex16 / 1 x PCI-Ex1 / 2 x PCI / 1 x COM / 1 x LPT / RJ-45 (LAN) / VGA / DVI / HDMI / Audio;
- оперативна пам'ять 4 Гб DDR3 1333 МГц;
- жорсткий диск Samsung HD322GJ, 500 GB 7200 rpm 16Mb cache SATA II-300;
- мережева карта D-Link DFE-520TX 1-port UTP 10/100Mbps PCI, OEM;
- корпус CoolerMaster CMP 350.

Вибір робочих станцій

- процесор не нижче за Pentium-IV1500 MHz, з об'ємом L2-cache 256 Кб;
- оперативна пам'ять не менше 512 Мб;
- об'єм дискового простору не менше 40 Гб;
- інтерфейс дисків - не нижче Ultra-ATA/100;

- відеоадаптер не нижче за АСР 4х з відео-пам'яттю не менше 32 Мб;
- дисковод CD-ROM;
- мережева карта 100Base-TX;
- монітор не менше 17";

Конфігурація обираємої робочої станції:

- Процесор Intel Pentium Dual Core E5500 (2,8 ГГц);
- Материнська плата ASUS P5KPL-AM IN/ROEM/SI 4 USB / 1 x PCI-Ex16 / 1 x PCI-Ex1 / 2 x PCI / 1 x COM / 1 x LPT / RJ-45 (LAN) / VGA / DVI / Audio;
- Оперативна пам'ять DDR3-1333 1 Гб;
- Жорсткий диск ATA 250 GB WD WD2500AVJB 8MB 7200rpm;
- Відео карта Інтегрована Intel GMA 4500;
- Корпус Logispower 4401 - 400w 8cm;
- Монітор 18.5" Samsung E1920N LS19CLYSB Black;
- Клавіатура SVEN Standard 304, USB;
- Мишка Logitech B110 Optical Mouse USB.

Вибір сервера FreeBSD

- процесор не нижче: Pentium-2
- оперативна пам'ять не менш 256 Мб;
- об'ємом дискового простору не менш 4 Гб;
- дисковод DVD-RW;
- мережна карта 100 Base-TX.

Конфігурація обираемого сервера FreeBSD:

- Процесор Intel Pentium Dual Core E5500 (2,8 ГГц);
- Материнська плата ASUS P5KPL-AM IN/ROEM/SI 4 USB / 1 x PCI-Ex16 / 1 x PCI-Ex1 / 2 x PCI / 1 x COM / 1 x LPT / RJ-45 (LAN) / VGA / DVI / Audio;
- Оперативна пам'ять DDR3-1333 1 Гб;
- Жорсткий диск ATA 250 GB WD WD2500AVJB 8MB 7200rpm;

- Відео карта Інтегрована Intel GMA 4500;
- Корпус Logispower 4401 - 400w 8cm;
- Мережева карта D-Link DFE-520TX 1-port UTP 10/100Mbps PCI

Джерело безперебійного живлення

Як обладнання безперебійного живлення пропонується використовувати обладнання фірми APC сімейства Mustek Power Must 650 Office. Продукти цього сімейства відрізняються видатною продуктивністю й надійністю, а також оснащуються портом USB, передньою панеллю стандартного білого кольору й мають небагато підвищену вихідну потужність у порівнянні зі своїми попередниками - моделями потужністю 700 і 1400 Вт.

3.4.2 Комутаційне обладнання

Вибір комутаторів

З розрахунку того, що відома кількість користувачів мережі, потрібно використовувати два восьми - портових комутуючих концентраторів. Після ознайомлення з комутаторами даного виробника і вивчення відгуків про використання було вирішено використовувати два комутатори Switch D-Link 8-портовий 10/100 (DES-1008D). Оскільки вони при помірній ціні відрізнялися стабільною роботою.

Стандарти:

- IEEE802.310 Base-T Ethernet IEEE 802.3u 100Base-TX Fast Ethernet;
- топологія: зірка;
- архітектура: "Store-and-Forward";
- мережеві порти: 8 портів з роз'ємами RJ-45;
- обсяг буфера: 64 К на пристрій (версії G1, G2, H1) ;
- режими дуплексу: Ethernet:10 М біт/с (полудуплекс)
20 М біт/с (повний дуплекс) Fast Ethernet: 100 М біт/с (полудуплекс)
200 М біт/с (повний дуплекс);
- джерело живлення: зовнішній 7,5 В, 1 А;

- енергоспоживання: 3.3 Вт (тільки пристрій) 5.45 Вт (пристрій + адаптер живлення, від мережі 220 В);
- мережеві кабелі: UTP (неекранована вита пара) 3, 4 або 5 категорії;
- фільтрація: 148800 пакетів/с при 100 М біт/с;
- час очікування: 8,5 мс мінімум при 100 М біт/с, 75 мс мінімум при 10 М біт/с;
- MAC адреси: автоматичне;
- зовнішнє середовище: робоча температура від 0 до 50 °С, вологість від 5 до 90 %;
- розміри: 192 x 118 x 32 мм.

Вибір способу підключення до Інтернету

Багатьох користувачів мережі Інтернет не задовольняє якість зв'язку забезпечуване аналоговими модемами при підключенні до Інтернет. Крім того, часто кінцевим користувачам, тобто співробітникам підприємства економічно вигідніше підключення до Інтернет по виділеному швидкісному каналу за рахунок того, що у такому разі оплачується трафік, а не тривалість з'єднання як при використанні аналогових модемів. Обрана технологія Інтернету була – Ethernet. Налаштування сервера FreeBSD знаходиться у додатку А.

3.5 Кабельна система

Як середовище передачі даних в локальній мережі найчастіше використовують кабель. При виборі середовища передачі даних для локальної мережі приймаються до уваги наступні чинники:

- вартість монтажу і подальшого обслуговування;
- швидкість передачі даних;
- наявність обмежень на дальність переданих даних (без урахування використання повторювачів сигналу);
- безпека переданої інформації.

При монтажі мережі на основі витой пари необхідно пам'ятати про основні обмеження мережі:

- довжина сегменту не повинна перевищувати 100 м;
- кількість комп'ютерів, що підключаються до мережі, менше 1024;
- кількість повторювачів в мережі - не більше 3.

Найчастіше як середовище передачі даних використовується вита пара.

В даному випадку витрати будуть мінімальними, хоча цьому рішенню властиві свої недоліки, головний з яких полягає в низькій перешкодозахищеності. Проте ці недоліки окупаються простотою монтажу кабельної системи.

Кабелі категорії 1 застосовуються там, де вимоги до швидкості передачі мінімальні. Звичайно це кабель для цифрової і аналогової передачі голосу і низько швидкісної (до 20 кбіт/с) передачі даних. До 1983 року це був основний тип кабелю для телефонної розводки.

Кабелі категорії 2 були вперше використані фірмою IBM при побудові власної кабельної системи. Головна вимога до кабелів цієї категорії - здатність передавати сигнали із спектром до 1 МГц.

Кабелі категорії 3 були стандартизовані в 1991 році. Стандарт EIA-568 визначив електричні характеристики кабелів для частот в діапазоні до 16 МГц. Кабелі категорії 3 призначені як для передачі даних, так і для передачі голосу, складають зараз основу багатьох кабельних систем будівель.

Для абонентської системи підприємства оптимальним вибором служить неекранована вита пара категорії 5 або 5е. Вона дозволяє передавати дані із швидкістю 100 Мбіт/с, зручна в прокладці, володіє достатньо низькою вартістю і відповідає всім вимогам по надійності, що пред'являються до локальної обчислювальної мережі підприємства.

Витою парою називається скручена пара дротів. Скручування дротів знижує вплив зовнішніх і взаємних перешкод на корисні сигнали, передані по кабелю. Для проекту обрано кабельну систему на базі неекранованої витної пари категорії 5, тому що неекранована вита пара застосовується для монтажу мережі усередині будівлі. Був вибраний кабель 5-ої категорії, оскільки такі кабелі спеціально розроблені для підтримки високошвидкісних протоколів, таких як 100VG-AnyLAN. Всі кабелі UTP (неекранована вита пара) незалежно

від їх категорії випускаються в 4-парному виконанні. Кожна з чотирьох пар кабелю має певний колір і крок скручування. Звичайно дві пари призначені для передачі даних, а дві - для передачі голосу. Кожний з кабелів звичайно закінчується роз'ємами типу RJ-45, які найчастіше використовуються для підключення до мережевих інтерфейсних карт і комутаторів [10].

3.5.1 Вибір місць прокладання кабелю

Місце розташування устаткування, вибирається виходячи з оптимальної віддаленості, і з урахуванням перспективи підключення нових, а також з виключенням доступу до устаткування сторонніх осіб. Часто в шахтах слабкострумової проводки немає місця для кабелів, і ще частіше - відсутнє місце для розміщення устаткування.

Найважливіший чинник при виборі місця вузла - умова його довгострокового існування. Адже до активного устаткування зводяться кабелі, і переносити їх рік-два буде економічно не вигідно.

У центрі будівлі розташовують комутатори, від яких до робочих станцій прокладаються лінії. Кабель прокладений в коробі. Переважно прокладати кабель в коробах і забезпечувати їх розетками, ніж тягнути кабель безпосередньо в мережеву карту комп'ютера. Відсутність коробів загрожує пошкодженням кабелю в процесі експлуатації, а відсутність розеток погрожує тим, що у разі пошкодження доведеться замінити не тільки пошкоджений відрізок, а декілька метрів кабелю.

Короб захищає кабель від механічних пошкоджень, перепадів температур, пилу і вологи, що благотворно впливає на термін служби кабелю.

При прокладці кабелю перш за все необхідно підготувати кабель, потім обжати конвектори.

Вимоги до прокладання:

- щоб уникнути розтягування сила натягнення для чотирьохпарних кабелів не повинна перевищувати 110 Н (зусилля приблизно в 12 кг). Як правило, зусилля понад 250 Н приводить до необоротних змін параметрів UTP-кабелю;

- радіуси вигину встановлених кабелів не повинні бути менше чотирьох (деякі виробники наполягають на восьми) діаметрів для кабелів UTP горизонтальної системи. Припустимий вигин в ході монтажу не менше трьох-чотирьох діаметрів.
- слід уникати зайвого навантаження на кабелі, що звичайно викликається їх перекрученням під час протяжки або монтажу, надмірним натягненням на підвісних ділянках трас, туго затягнутими вузькими кабельними хомутами (або «пристреленими» скобами);
- кабелі горизонтальної системи повинні використовуватися в поєднанні з комутаційним устаткуванням і патч-кордом (або перемичками) тієї ж або вищої категорії робочих характеристик;
- якість зібраної кабельної системи в цілому визначається по компоненту лінії з якнайгіршими робочими характеристиками;
- необхідно виключати ситуації, коли на кабель можна буде випадково наступити;
- не можна прокладати кабель біля електрощитів і опалювальних елементів.

Локальна мережа досить гнучка, і при необхідності її можна легко розширити, додати ще один комутатор, з'єднати мережу на витій парі і так далі.

3.6 Організація робочих місць на підприємстві

Товариство з обмеженою відповідальністю «Терновський хлібзавод» займає 1-й та 2-й поверхи. Частини об'єднують три кімнати на першому, та шість кімнат на другому поверхах, загальна площа яких складає близько 1000 квадратних метрів.

Всю кабельну мережу буде прокладено в проміжку між фальш-підлогою і плитами перекриття поверху. Структурована кабельна система прокладатиметься з використанням кабелю UTP (Unshielded Twisted Pair – неекранована кручена пара), стандарту EIA/TIA 568B TP категорії 5 (міжнародного стандарту кабельних систем). Даний стандарт вимагає наявності

чотирьох пар мідного проводу, з можливістю передачі даних із швидкістю 100 Мбіт/с по двох з них. Технологію монтажу і розгортання кабельної системи можна розглянути на прикладі одного робочого місця, оскільки всі робочі місця організовані ідентично. Монтаж (після складання проекту) починається з прокладання кабелю між серверним і клієнтськими робочими станціями.

Фізична топологія комп'ютерної мережі підприємства є деревом: всі клієнти мережі є відгалуженнями центрального «магістрального» каналу. Але за логічною топологією вся мережа є «зіркою», у вигляді мережевих комутаторів. Два мережеві комутатори об'єднуються в каскад за допомогою патч-корду п'ятої категорії. Таким чином, два комутатори утворюють місткість в 16 портів п'ятої категорії.

Схему з'єднання комп'ютерів в ЛОМ, розміщення обладнання та прокладання кабелю в приміщенні пекарні «Терновський хлібзавод» наведено на рисунку 3.12 та 3.13.

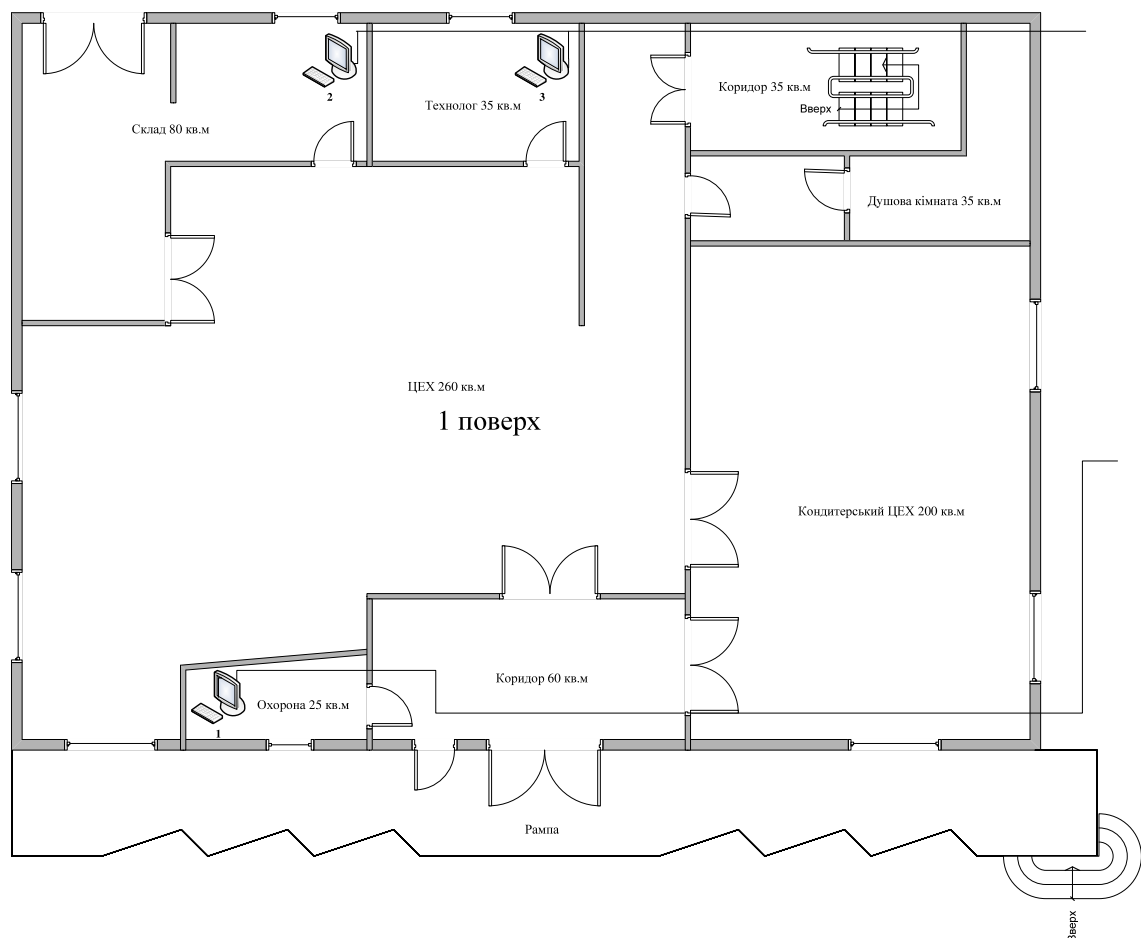


Рисунок 3.12 – План прокладки кабелю на підприємстві першого поверху

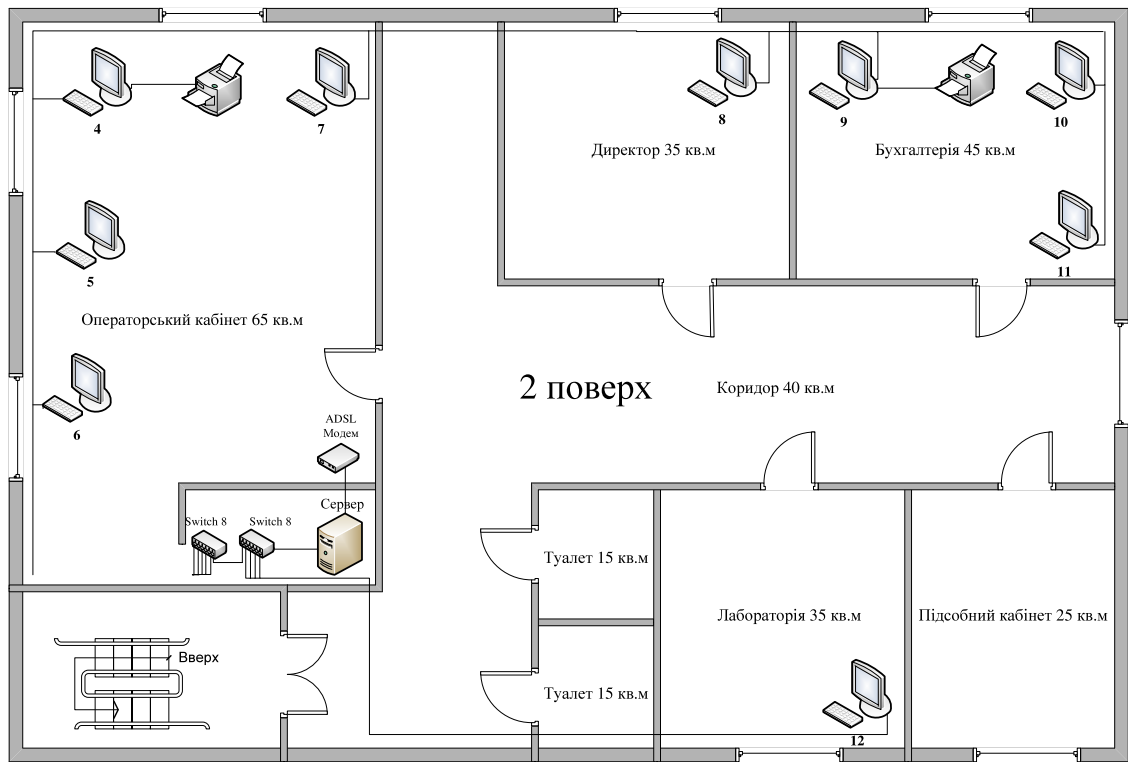


Рисунок 3.13 – План прокладки кабелю на підприємстві другого поверху

3.7 Проектування відео спостереження

3.7.1 Призначення систем відео спостереження

Система телевізійного відео спостереження призначена для візуального спостереження і реєстрації (запису) поточних подій і для подальшого перегляду зображень зон об'єкту, що охороняються і технологічних.

Система відео спостереження повинна забезпечити:

- цілодобовий візуальний контроль оперативної обстановки в зонах відео спостереження;
- реєстрацію (запис) зображень зі встановлених відеокamer;
- автоматичний вивід на «тривожні монітори» операторів зображень, пов'язаних з виниклою тривожною ситуацією; режим детектування активності (рухи) в зоні огляду відеокamerи;
- можливість виведення зображень з декількох камер на монітори в режимі мультиекрана;

- можливість виведення зображення із заданої камери на екран монітора в повноекранному режимі;
- можливість збереження архіву на зовнішніх носіях, перегляду і передачі архіву зображень стандартними засобами комп'ютерної технології.

3.7.2 Вибір системи відео спостереження

Системи відео спостереження для підприємств можна розділити на дві основні групи – відео спостереження на базі DVR і відео спостереження на базі комп'ютера. Наступна основна відмінність - наявність можливості моніторингу та контролю касових і товарних операцій.

Системи на базі DVR застосовуються на невеликих підприємствах або відділах. За допомогою DVR можна швидко, а головне не дорого організувати відео спостереження за відділом або філією. Якщо до цієї філії або відділу можна підвести Інтернет - спостереження і роботу з архівом можна виконувати віддалено (рисунок 3.14).



Рисунок 3.14 – Система відеоспостереження на базі DVR відеореєстратора

Для великих магазинів (супермаркет, гіпермаркет), а також мережі з кількох магазинів вигідно застосовувати системи відео спостереження для магазинів з контролем касових і товарних операцій. До цих систем відео

спостереження можна підключати касові апарати, POS-обладнання, ваги, термінали збору даних для передачі даних про продажі. Ці дані синхронізуються з відео і дозволяють вибрати і переглянути відео фрагмент з будь-якої події або виробничої операції: зважування, продаж товару, прийом товару, повернення товару, інвентаризація і т.д. (рисунок 3.15).

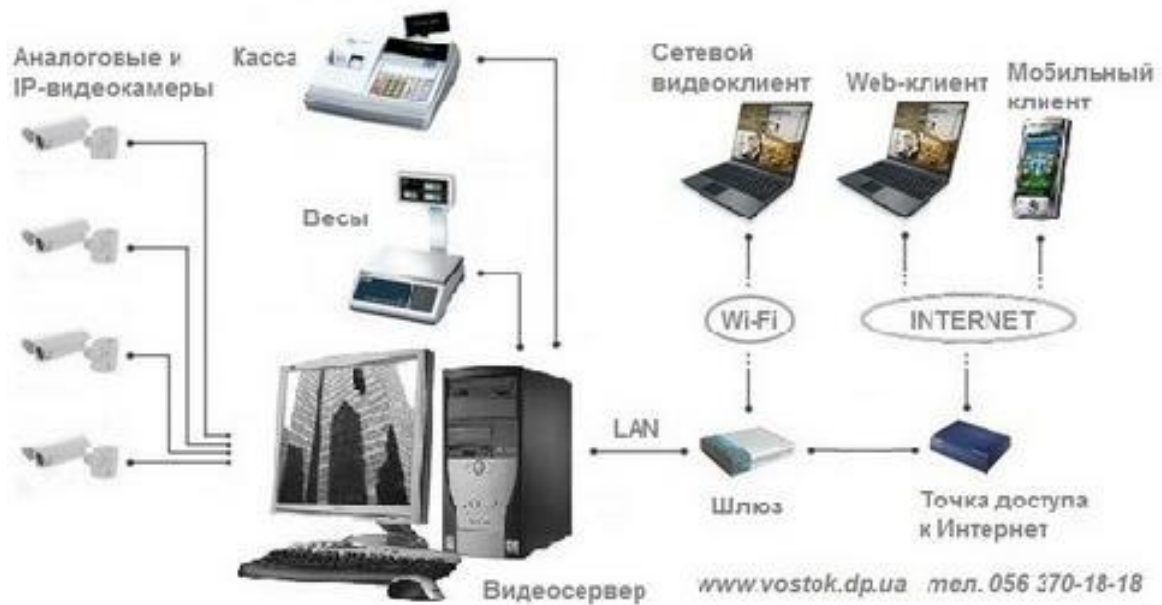


Рисунок 3.15 – Система відео спостереження з контролем касових і товарних операцій

Можна комбінувати кілька різних систем. Хоча й існує думка, що для одного об'єкта необхідно вибудовувати все на одній платформі - практика показує, що це не так. Для великих об'єктів можна і навіть потрібно використовувати комбіновані системи - наприклад Інтелект відмінно справляється з контролем POS-операцій, може бути інтегрований в пожежну та охоронну систему торговельного комплексу. Але для звичайних охоронних функцій або швидкого аналізу подій на які Інтелект не був запрограмований він буде «важкуватий», ось тут вже можна цілком успішно застосувати систему відеоспостереження «Патріот».

Для того, щоб точно визначити, яка система чи комбінація систем буде максимально ефективною і вигідною необхідно ретельно опрацювати технічне завдання.

Існує кілька типів відеокамер, зокрема:

- стаціонарні;
- поворотні;
- купольні;
- IP-камери.

Зображення від камер передається по кабелях (коаксіальні кабелі, оптиковолокно , вита пара) або бездротовим способом. Якщо відеокамер не багато, то зображення від них можна записувати на відео реєстратори (цифрові відеорекодери) та / або виводити на монітори. Відео реєстратори записують зображення від камер, на жорсткі носії в цифровому форматі. . Деякі цифрові відео реєстратори містять вбудовані детектори руху. Вони обробляють зображення в кадрі, реагують на рух і записують його.

Якщо система відео спостереження складна і складається з багатьох камер, тоді є можливість побудувати систему для управління зображеннями, документувати, аналізувати за допомогою систем комутації, обробки зображення (квадратори, мультиплексори і т.д.) і систем управління (системні контролери). Пристрої обробки аналізують відео зображення, переводять відеозображення від камер в необхідний формат, і передають на відеореєстратори та / або монітори.

Квадратори виводять зображення від 4-х камер на один монітор одночасно.

Мультиплексори призначені для послідовного запису відеозображення з камер на відеореєстратор. Мультиплексори дають можливість переглянути відео з декількох камер одночасно і заздалегідь записане відео.

Стаціонарні відеокамери встановлюються у випадках, коли необхідно отримати відеозображення фіксованої області. Стаціонарні відеокамери, як правило, використовуються з широкофокусними об'єктивами для того щоб отримати зображення великої області. Якщо є необхідність змінювати кут огляду і якість відеозображення, використовуються трансфокатори - об'єктиви зі змінними фокусними відстанями.

Поворотні відеокамери застосовуються, коли стоїть завдання фіксації рухомих об'єктів і коли необхідно вести нагляд за великою областю спостереження. Поворотні камери складаються з камери та механізму панорамування, який призначений для повороту камери в горизонтальних і вертикальних площинах.

Купольні відеокамери зазвичай являють собою напівсферу, що встановлюється на стелю в приміщенні. Перевагою таких камер є прихований вид напрямку самої камери в середині тонованого скла в куполі.

Купольні відеокамери роботизовані складаються з поворотної голівки в захисному куполоподібному корпусі. У купольних камерах на відміну від поворотних більший кут огляду і, як правило, більш прогресивна цифрова обробка зображення..

ІР-камери призначені для передачі зображення через вбудований web сервер на комп'ютер за допомогою Інтернет мережі. Ви можете знаходитися далеко від камери, навіть на іншому континенті, і за зручним web-інтерфейсом через Інтернет спостерігати за тим, що відбувається, наприклад, у вас вдома, або на підприємстві [11].

3.7.3 Вибір устаткування для відео спостереження

Вибір робочої станції для відео спостереження

- Процесор AMD Athlon II X2 245 (Tray) (ADX2450CK23GQ) (2.90 ГГц/AM3/Кэш L2: 2 МБ/Шина: 2.0 МГц/AMD64/0.045 мкм/65 W);
- Материнська плата ASUS P5G41-M LE/C/SI (G41 /ICH7,s775, FSB1333/1066/800, 4DualDDR2_1066 - 800, 1xPCIex16, 1xPCIe;
- Оперативна пам'ять DDR 2 1024 Mb 800 MHz PC-6400 SAMSUNG;
- Жорсткий диск - HITACHI 1,0Tb SATA-II, 7200rpm 32Mb;
- Відео карта- GeForce GT220 512MB DDR2 128bit DVI (550/800) GE;
- Звукова карта Realtek ALC887;
- Монітор TFT 22" Samsung E2220N (CLYSBU) TFT , 22", black, TN, 16:9, 5ms, D-Sub, 300/70000:1(DC), 170/160;
- Корпус- Logispower 4401 - 400w 8cm;

- Клавіатура- SVEN Standard 304, USB;
- Мишка- Logitech B110 Optical Mouse USB.

Вибір плати відео захоплення

Для відеоспостереження на підприємстві було обрано готовий для установки комплект на базі плати відеозахоплення Spotter 2.8. Це готове рішення комплектується зовнішніми кольоровими камерами, внутрішніми кольоровими купольними відеокамерами, а також платою відеозахвату Spotter 2.8. У готовий комплект відео спостереження входить також кабель для відеосигналу і для живлення відеокамер, по 100 метрів кожна бухта. Щоб усе це підключити і живити, в комплект включили блок живлення. Комплект зображено на рисунку 3.16.



Рисунок 3.16 – Комплект обладнання

В комплект входять:

- Плата відео захоплення Avidis Spotter 2.8
- Зовнішня камера TC-520C - чотири штуки
- Внутрішня камера InterVision HP-5540C - чотири штуки

- Блок живлення ІБП 3.5А – одна штука
- Коаксіальний кабель Euro SAT RG-59 – дві бухти по 100 м.
- Коннектор BNC – вісім штук
- F - коннектор RG59 – вісім штук
- Роз'єм живлення 12V MD1620 male – вісім штук
- Кабель сигнальний СЕНК 2х0,22 неекраниваний – дві бухти по 100м.

На рисунку 3.17 зображена Плата відео захоплення Avidis Spotter 2.8



Рисунок 3.17 - Плата відео захоплення Avidis Spotter 2.8

Технічні характеристики:

- швидкість до: 32/50 к/сек;
- кількість відеовходів: 8;
- кількість аудіовходів: 4;
- тип стискування: програмований;
- формат стискування: Wavelet;
- формат кадру: 720x576;
- додаткові характеристики: Avidis Spotter 2.8;
- схема оцифрування: Philips SAA7134;
- кількість плат: 2xDV1.4;
- кількість каналів реального часу: 2;
- швидкість на канал: 4 кб/с.;

- дозвіл: 500 ТВЛ;
- стандарт шини розширення: PCI 2.2, 5V/3.3V, 32bit/33MHz;
- вхідний опір: 75 Ом;
- режим триплекса: огляд відео архіву, запис і спостереження одночасно;
- "кільцевий" запис з обмеженням по вільному місці на жорсткому диску;
- програмна детекція руху;
- програмовані реакції системи на спрацьовування детектора;
- запуск системи в скритому режимі (програма не видна для користувачів ПК);
- розподіл прав доступу.

Найменування по каталогу: Avidis Spotter 2.8, інші назви: Avidis Spotter 2.8, Avidis Spotter-2.8, DV1.4.

Мінімальні системні вимоги:

Операційна система: Windows NT/2000/XP;

Процесор: від 266 МГц;

Оперативна пам'ять: від 64 Мб.

На рисунку 3.18 зображена зовнішня камера TC-520C



Рисунок 3.18 - Зовнішня камера TC-520C

- Виробник: RainBow.
- Об'єктив (мм): 3.6/6/8/12/16.

- ПЗС-матриця: Sony Super HAD CCD.
- Чутливість (кол./чб.): 0 люкс (IR on).
- Кольоровість: кольорова.
- Тип камери: циліндричний.
- Установка: зовнішня.
- Розмір кадру в пікселях: 520.
- Режим "день/ніч": Ні.
- ІК підсвічування: Так.

На рисунку 3.19 зображена внутрішня камера InterVision HP-5540C



Рисунок 3.19 - Внутрішня камера InterVision HP-5540C

- Виробник: InterVision.
- Об'єктив (мм): 3.6/6/8/12.
- ПЗС-матриця: Sony Super HAD HighRes.
- Чутливість (кол./чб.): 0.05.
- Кольоровість: кольорова.
- Тип камери: купольний.
- Установка: внутрішня.
- Розмір кадру в пікселях: 540.
- Режим "день/ніч": Ні.
- ІК підсвічування: Ні.

На рисунку 3.20 зображений блок живлення ИБП 3.5А



Рисунок 3.20 - Блок живлення ИБП 3.5А

Блок живлення імпульсний 12 В, 3,5 А призначений для живлення зниженим (небезпечним) постійним напругою 12 В пристроїв в складі охоронних комплексів і систем відео спостереження.

Технічні характеристики:

- Максимальний вихідний струм – 3,5 А.
- Час виходу на номінальну потужність 1 с.
- Наростання: 30 мс.
- Утримання: 15 мс.
- Робоча температура 0-50 °С.

На рисунку 3.21 зображений коаксіальний кабель Euro SAT RG-59



Рисунок 3.21 - Коаксіальний кабель Euro SAT RG-59

Коаксіальний кабель EuroSAT RG59 з мідним центральним провідником, мідне обплетення 64 %, 0.50Cu+32x0.12Cu, білий, тонкий, бухта 100 м.

На рисунку 3.22 зображений конектор BNC.



Рисунок 3.22 - Конектор BNC

Перехідник BNC під F-конектор для підключення відеокамер до відеореєстратору, платі відео захоплення і іншим пристроям.

На рисунку 3.23 зображений F - конектор RG59



Рисунок 3.23 - F - конектор RG59

Штекер F що накручується, під телевізійний кабель RG-6, EuroSat 3C-2 B. Використовується у теле, відео, радіотехніці.

На рисунку 3.24 зображений роз'єм живлення 12V MD1620 male



Рисунок 3.24 - F - роз'єм живлення 12V MD1620 male

— Роз'єм живлення універсальний "папа".

- Контакти: фосф.бронза, покрита оловом.
- Ізолятор: нейлон 66, посилений скловолокном UL 94V-О.

Електричні характеристики:

- Граничний струм: 2 А.
- Робоча напруга: 250 В.
- Опір ізолятора: не менше 50 МОм.
- Опір контакту: не більше 0,02 Ом.

Експлуатаційні характеристики:

- Допустимі температури: від -35 до +85 °С.

На рисунку 3.25 зображений кабель сигнальний СЕНК 2х0,22 неекраниваний



Рисунок 3.25 - Кабель сигнальний СЕНК 2х0,22 неекраниваний, білий, 100 м

3.7.4 Розміщення обладнання для відео спостереження на підприємстві ТОВ «Терновський хлібзавод»

Система відео спостереження і реєстрації представляє із себе професійний комплекс охоронного призначення, що має можливість контролю об'єктів відео спостереження в реальному часі. Система передбачає підключення 8 відеокамер із сумарним потоком відтворення-запису 100 або 200 кадрів /с. у вікнах розміром до 768х576.

Розміщення камер відео спостереження було прийнято як в середині приміщення так і на зовнішній території об'єкту.

Три камери відео спостереження розташовані на передній під'їзній частині об'єкту (рампі), також ще одна відео камера на задній території об'єкту біля під'їзду до складських воріт.

Для внутрішнього відео спостереження треба прийняти рішення, де розташувати камери щоб було як найкраще охоплення приміщень.

Таким чином встановлено дві відео камери на перегородці головного ЦЕХа, які будуть охоплювати: перша - головний вхід, а друга камера головний ЦЕХ.

Третя відео камера розташована у кондитерському ЦЕХу.

Четверта відео камера розміщена у приміщенні складу.

Всі камери з'єднані коаксіальним кабелем типу Euro SAT RG-59, на кінцях яких вмонтовані: з одного боку F – конектори RG59 для під'єднання до самої відеокамери, а з іншого перехідник BNC під F-конектор для підключення відео камер до плати відео захоплення і іншим пристроям.

Кабелі прокладені в коробі. Переважно прокладати кабелі в коробах і забезпечувати їх, ніж тягнути кабелі безпосередньо до комп'ютера. Відсутність коробів загрожує пошкодженням кабелів в процесі експлуатації, у разі пошкодження доведеться замінити не тільки пошкоджений відрізок, а декілька метрів дорогих кабелів.

Короб захищає кабель від механічних пошкоджень, перепадів температур, пилу і вологи, що благотворно впливає на термін служби кабелів.

Для живлення камер проводиться з'єднання сигнальним неекранованим кабелем СЕНК 2x0,22, на кінцях яких вмонтовані роз'єми живлення 12V MD1620 male.

Живлення камер забезпечує спеціальний блок ІБП 3.5А в який під'єднуються всі відео камери даного об'єкту.

За таким планом буде вестися як найкраще відео спостереження по всій території об'єкта з головного пульта керування який буде знаходитися на першому поверсі у охоронному кабінеті. Також відео картинка буде проходити до комп'ютера який знаходиться у кабінеті директора для зручнішого

спостереження за всіма процесами, які будуть проходити на даному підприємстві.

План-схема розташування системи відео спостереження зображена на рисунку 3.26.

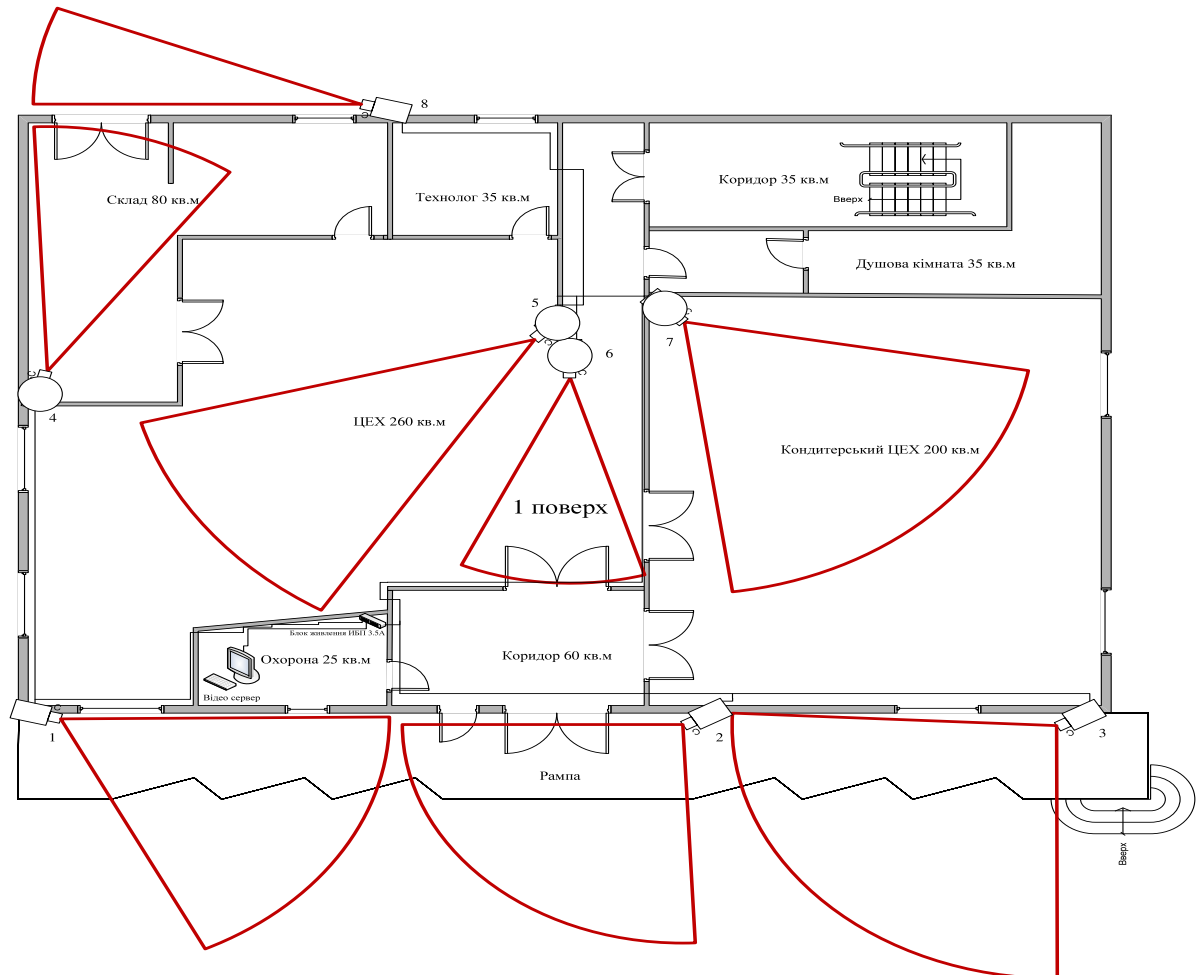


Рисунок 3.26 – План-схема розташування системи відео спостереження

4. ЗАХИСТ ІНФОРМАЦІЇ В МЕРЕЖІ

4.1 Потенційні погрози безпеці інформації

Дослідження і аналіз численних випадків впливу на інформацію і несанкціонованого доступу до неї показують, що їх можна розділити на випадкові і навмисні. Для створення засобів захисту інформації необхідно визначити природу погроз, форми і шляху їх можливого прояву і здійснення в автоматизованій системі. Для вирішення поставленого завдання все різноманіття погроз і шляхів їх дії приведемо до простих видів і форм, які були б адекватні їх множині в автоматизованій системі.

4.1.1 Випадкові погрози

Дослідження досвіду проектування, виготовлення, випробувань і експлуатації автоматизованих систем говорять про те, що інформація в процесі введення, зберігання, обробки, виведення і передачі піддається різним випадковим діям.

Причинами таких дій можуть бути:

- відмови і збої апаратури;
- перешкоди на лінії зв'язку від дій зовнішнього середовища;
- помилки людини як ланки системи;
- системні і системотехнічні помилки розробників;
- структурні, алгоритмічні і програмні помилки;
- аварійні ситуації;
- інші дії.

Частота відмов і збоїв апаратури збільшується при виборі і проектуванні системи, слабкої відносно надійності функціонування апаратури. Перешкоди на лінії зв'язку залежать від правильності вибору місця розміщення технічних засобів АСУ щодо один одного і по відношенню до апаратури сусідніх систем.

До помилок людини як ланки системи слід відносити помилки людини як джерела інформації, людини-оператора, неправильні дії обслуговуючого персоналу і помилки людини як ланки, що приймає рішення.

Помилки людини можуть підрозділятися на логічні (невірні рішення), сенсорні (неправильне сприйняття оператором інформації) і оперативні, або моторні (неправильна реалізація рішення). Інтенсивність помилок людини може коливатися в широких межах: від 1-2% до 15-40% і вище за загальне число операцій при рішеннях задачі.

До погроз випадкового характеру слід віднести аварійні ситуації, які можуть виникнути на об'єкті розміщення автоматизованої системи. До аварійних ситуацій відносяться:

- відмова від функціонування САУ в цілому, наприклад вихід з ладу електроживлення
- стихійні лиха: пожежа, повінь, землетрус, урагани, удари блискавки і т.д.

Вірогідність цих подій пов'язана перш за все з правильним вибором місця розміщення АСУ, включаючи географічне положення.

4.1.2 Навмисні погрози

Навмисні погрози пов'язані з діями людини, причинами яких можуть бути певна незадоволеність своєю життєвою ситуацією, суто матеріальна зацікавленість, або проста розвага з самоствердженням своїх здібностей, як у хакерів, і т.д.

Для обчислювальних систем характерні наступні штатні канали доступу до інформації:

- термінали користувачів;
- термінал адміністратора системи;
- термінал оператора функціонального контролю;
- засоби відображення інформації;
- засоби завантаження програмного забезпечення;
- засоби документування інформації;
- носії інформації;
- зовнішні канали зв'язку.

Маючи на увазі, що за відсутності захисту порушник може скористатися як штатними, так і іншими фізичними каналами доступу, назовемо можливі канали

несанкціонованого доступу (МКНСД) в обчислювальній системі, через які можливо дістати доступ до апаратури, ПЗ і здійснити розкрадання, руйнування, модифікацію інформації і ознайомлення з нею:

- всі перераховані штатні засоби при їх використанні законними користувачами не за призначенням і за межами своїх повноважень
- всі перераховані штатні засоби при їх використанні сторонніми особами;
- технологічні пульти управління;
- внутрішній монтаж апаратури;
- лінії зв'язку між апаратними засобами даної обчислювальної системи;
- побічне електромагнітне випромінювання апаратури системи;
- побічні наведення по мережі електроживлення і заземлення апаратури;
- побічні наведення на допоміжних і сторонніх комунікаціях;
- відходи обробки інформації у вигляді паперових і магнітних носіїв.

Очевидно, що за відсутності законного користувача, контролю і розмежування доступу до терміналу кваліфікований порушник легко скористається його функціональними можливостями для несанкціонованого доступу до інформації шляхом введення відповідних запитів і команд. За наявності вільного доступу в приміщення можна візуально спостерігати інформацію на засобах відображення і документування, а на останніх викрасти паперовий носій, зняти зайву копію, а також викрасти інші носії з інформацією: лістинги, магнітні стрічки, диски і т.д.

Особливо небезпечним є безконтрольне завантаження програмного забезпечення в ЕОМ, в якій можуть бути змінені дані, алгоритми або введена програма "троянський кінь", що виконує додаткові незаконні дії: запис інформації на сторонній носій, передачу в канали зв'язку іншого абонента обчислювальної мережі, внесення в систему комп'ютерного вірусу і т.д. Небезпечною є ситуація, коли порушником є користувач системи, який по своїх функціональних обов'язках має законний доступ до однієї частини інформації, а звертається до іншої за межами своїх повноважень. З боку законного користувача існує багато способів порушити роботу обчислювальної системи, зловживати нею, витягувати, модифікувати або знищувати інформацію. Вільний

доступ дозволить йому звертатися до чужих файлів і банків даних і змінювати їх випадково або навмисно.

При технічному обслуговуванні (профілактиці і ремонті) апаратури можуть бути виявлені залишки інформації на магнітній стрічці, поверхнях дисків і інших носіях інформації. Звичайне стирання інформації не завжди ефективно. Її залишки можуть бути легко прочитані. При транспортуванні носія по території, що не охороняється, існує небезпека його перехоплення і подальшого ознайомлення сторонніх осіб з секретною інформацією. Не має сенсу створення системи контролю і розмежування доступу до інформації на програмному рівні, якщо не контролюється доступ до пульта управління ЕОМ, внутрішнього монтажу апаратури, кабельних з'єднань.

Спрацьовування логічних елементів обумовлене високочастотною зміною рівнів напруг і струмів, що приводить до виникнення в ефірі, ланцюгах живлення і заземлення, а також в паралельно розташованих ланцюгах і соленоїдах сторонньої апаратури, електромагнітних полів і наведень, що несуть в амплітуді, фазі і частоті своїх коливань ознаки оброблюваної інформації. Із зменшенням відстані між приймачем порушника і апаратними засобами вірогідність прийому сигналів такого роду збільшується.

Безпосереднє підключення порушником приймальної апаратури і спеціальних датчиків до ланцюгів електроживлення і заземлення, до каналів зв'язку також дозволяє зробити несанкціоноване ознайомлення з інформацією, а несанкціоноване підключення до каналів зв'язку передавальної апаратури може привести і до модифікації інформації [2].

За останній час в різних країнах проведена велика кількість дослідницьких робіт з метою виявлення потенційних каналів несанкціонованого доступу до інформації в обчислювальних мережах. При цьому розглядаються не тільки можливості порушника, що дістав законний доступ до мережевого устаткування, але і дії, обумовлені помилками програмного забезпечення або властивостями використовуваних мережевих протоколів. Не дивлячись на те, що вивчення каналів НСД продовжується дотепер, вже на початку 80-х років

були сформульовані п'ять основних категорій погроз безпеки даних в обчислювальних мережах:

- 1) Розкриття змісту повідомлень, що передаються.
- 2) Аналіз трафіку, що дозволяє визначити приналежність відправника і одержувача даних до однієї з груп користувачів мережі, зв'язаних загальним завданням.
- 3) Зміна потоку повідомлень, що може привести до порушення режиму роботи якого-небудь об'єкту, керованого з видаленої ЕОМ.
- 4) Неправомірна відмова в наданні послуг.
- 5) Несанкціоноване встановлення з'єднання.

Погрози 1 і 2 можна віднести до просочування інформації, погрози 3 і 5 - до її модифікації, а загрозу 4 - до порушення процесу обміну інформацією.

4.2 Засоби захисту інформації в ЛОМ

Прийнято розрізняти п'ять основних засобів захисту інформації:

- технічні;
- програмні;
- криптографічні;
- організаційні;
- законодавчі.

Розглянемо ці засоби докладніше і оцінимо їх можливості в плані подальшого їх використання при проектуванні конкретних засобів захисту інформації в ЛОМ.

4.2.1 Технічні засоби захисту інформації

Технічні засоби захисту - це механічні, електромеханічні, оптичні, радіо, електронних і інших пристрої, радіолокації, і системи, здатні виконувати самостійно або в комплексі з іншими засобами функції захисту даних. Технічні засоби захисту діляться на фізичні і апаратні. До фізичних засобів відносяться замки, ґрати, охоронні сигналізації, устаткування КРР і інше.; до апаратних -

замки, блокування і системи сигналізації про розтин, які застосовуються на засобах обчислювальної техніки і передачі даних.

4.2.2 Програмні засоби захисту інформації

Програмні засоби захисту - це спеціальні програми, що включаються до складу програмного забезпечення системи, для забезпечення самостійно або в комплексі з іншими засобами, функцій захисту даних. По функціональному призначенню програмні засоби можна розділити на наступні групи:

1) Програмні засоби ідентифікації і аутентифікації користувачів.

- Ідентифікація - це привласнення якому-небудь об'єкту або суб'єкту унікального образу, імені або числа. Встановлення достовірності (аутентифікація) полягає в перевірці, чи є об'єкт (суб'єкт), що перевіряється, тим, за кого себе видає. Кінцева мета ідентифікації і встановлення достовірності об'єкту в обчислювальній системі - допуск його до інформації обмеженого користування у разі позитивного результату перевірки або відмова в допуску інакше. Одним з поширених методів аутентифікації є привласнення персоні унікального імені або числа - пароля і зберігання його значення в обчислювальній системі. При вході в систему користувач вводить свій код пароля, обчислювальна система порівнює його значення із значенням, що зберігається в своїй пам'яті, і при збігу кодів відкриває доступ до дозволеного функціонального завдання, а при неспівпаданні - відмовляє в ньому. Найбільш високий рівень безпеки входу в систему досягається розділенням коду пароля на дві частини, одну, що запам'ятовується користувачем і що вводиться вручну, і другу, розміщену на спеціальному носії - картці, що встановлюється користувачем в спеціальний зчитуючий пристрій, зв'язаний з терміналом.

2) Засоби ідентифікації і встановлення достовірності технічних засобів.

Додатковий рівень захисту по відношенню до паролів користувачів. У ЕОМ зберігається список паролів і інша інформація про користувачів, яким дозволено користуватися певними терміналами, а також таблиця ресурсів, доступних з певного терміналу конкретному користувачу.

3) Засоби забезпечення захисту файлів.

Вся інформація в системі, що зберігається у вигляді файлів ділиться на деяку кількість категорій за різними ознаками, вибір яких залежить від функцій, що виконуються системою. Найчастіше можна зустріти розділення інформації:

- за ступенем важливості;
- за ступенем секретності;
- за виконуваними функціями користувачів;
- за найменуванням документів;
- за типом документів;
- за типами даних;
- за найменуванням томів, файлів, масивів, записів;
- за ім'ям користувача;
- за функціями обробки інформації: читанню, запису, виконанню;
- по областями оперативної і довготривалої пам'яті;
- за часом і т.д.

Доступ посадовців до файлів здійснюється відповідно до їх функціональних обов'язків і повноважень.

4) Засоби захисту операційної системи і програм користувачів.

Захист операційної системи - найбільш пріоритетне завдання. Здійснюється заборонаю доступу у області пам'яті, в яких розміщується операційна система.

Для захисту призначених для користувача програм застосовується обмеження доступу до займаної цими програмами пам'яті.

5) Допоміжні засоби.

До допоміжних засобів програмного захисту інформації відносяться:

- програмні засоби контролю правильності роботи користувачів;
- програмні знищувачі залишків інформації;
- програми контролю роботи механізму захисту;
- програми реєстрації звернень до системи і виконання дій з ресурсами;
- програми формування і друку грифа секретності;
- програмні засоби захисту від комп'ютерних вірусів і інше.

4.2.3 Криптографічні засоби захисту інформації

Криптографічні засоби захисту - це методи спеціального шифрування даних, в результаті якого їх зміст стає недоступним без застосування деякої спеціальної інформації і зворотного перетворення. Суть криптографічного захисту полягає в перетворенні складових частин інформації (слів, букв, складів, цифр) за допомогою спеціальних алгоритмів, або апаратних рішень і кодів ключів, тобто приведенні її до неявного вигляду. Для ознайомлення із закритою інформацією застосовується зворотний процес: декодування (дешифровка). Використання криптографії є одним з поширених методів, що значно підвищують безпеку передачі даних в мережах ЕОМ, даних, що зберігаються у віддалених пристроях пам'яті, і при обміні інформацією між віддаленими об'єктами.

4.2.4 Організаційні засоби захисту інформації

Організаційні засоби захисту - спеціальні організаційно-технічні і організаційно-правові заходи, акти і правила, здійснювані в процесі створення і експлуатації системи для організації і забезпечення захисту інформації.

Організаційні заходи здійснюють подвійну функцію:

- повне або часткове перекриття каналів просочування інформації;
- об'єднання всіх використовуваних засобів захисту в цілісний механізм.

Організаційні заходи захисту інформації повинні охоплювати етапи проектування, виготовлення, випробувань, підготовки до експлуатації і експлуатації системи.

4.2.5 Законодавчі засоби захисту інформації

Законодавчі заходи по захисту інформації від несанкціонованого доступу полягають у виконанні тих, що існують в країні або введенні нових законів, ухвал, положень і інструкцій, регулюючих юридичну відповідальність посадовців - користувачів і обслуговуючого персоналу за витік, втрату або модифікацію довіреної йому інформації, належному захисту, зокрема за спробу

навмисного несанкціонованого доступу до апаратури і інформації. Таким чином мета законодавчих заходів - попередження і заборона потенційних порушників.

4.3 Структура системи захисту інформації

На основі прийнятої концепції засоби захисту інформації діляться на засоби захисту від навмисного НСД (ЗЗІ ННСД) і від випадкового НСД (ЗЗІ ВНСД). Засоби управління захистом інформації (ЗУЗІ) від НСД є об'єднуючими, такими, що дають можливість за допомогою цілеспрямованих і взаємозв'язаних функцій в поєднанні з якнайповнішим охоптом можливих каналів НСД об'єкту окремими засобами захисту створити закінчену і строгу систему захисту в комплексі засобів автоматизації.

ЗЗІ ННСД включає 1-й контур захисту - систему контролю доступу на територію об'єкту (СКДТО), 2-й контур захисту - систему контролю і розмежування доступу в приміщення (СКРДП) і основний контур захисту (ОКЗ). СКДТО, що містить систему охоронної сигналізації (СОС) і контрольно-пропускні пункти (КПП), служить для обмеження доступу осіб на територію об'єкту, а також спільно із спеціальними апаратними рішеннями складає засіб захисту від побічних електромагнітних випромінювань і наведень.

Основний контур захисту перекриває канали доступу по периметру комплексу засобів автоматизації (КЗА). Система контролю відкривання апаратури (СКВА) перекриває доступ до внутрішнього монтажу, технологічних пультів управління і кабельних з'єднань. Система упізнання і розмежування доступу до інформації (СУРДІ) закриває несанкціонований доступ і забезпечує можливість контролю санкціонованого доступу до інформації законних користувачів і розмежування їх повноважень з урахуванням їх функціональних обов'язків.

Засоби виведення апаратури з робочого контура (ЗВАРК) забезпечують блокування НСД до інформації при ремонті і профілактиці апаратури. У числі засобів основного контура застосовуються також засоби захисту ресурсів (ЗЗР) і організаційні заходи. ЗЗР націлені на недопущення блокування користувачем-

порушником роботи інших користувачів, а також для контролю і обмеження доступу користувачів до ресурсів.

Засоби захисту інформації на носіях (ЗЗІН) включають засоби шифрування даних (ЗШД), засобу знищення залишків інформації на носіях (ЗЗЗІ), засобу аутентифікації інформації на носіях (ЗАІН), засоби верифікації програмного забезпечення (ЗВПЗ) і організаційно-технічні заходи. Система контролю відкривання апаратури включає датчики відкривання, встановлені на контрольованій апаратурі, ланцюги збору сигналів (ТЗС) і пристрій контролю відкривання апаратури (ПКВА).

СУРДІ містить термінал служби безпеки інформації (ТСБІ), функціональні завдання програмного забезпечення (ФЗ ПЗ), що реалізують на програмному рівні ідентифікацію і аутентифікацію користувачів, а також розмежування їх повноважень по доступу до інформації. В цілях захисту кодів паролів від НСД для них також повинні бути передбачені засоби захисту (ЗЗКП).

Засоби захисту від випадкового НСД включають засоби підвищення достовірності інформації (ЗПДІ) і засоби захисту інформації від аварійних ситуацій (ЗЗІ АС). ЗПДІ містять систему функціонального контролю (СФК), пристрій захисту від помилок в каналах зв'язку (ПЗП КЗ), засоби контролю цілісності програмного забезпечення (ЗКЦ ПЗ) і спеціальні технічні рішення (СТР). Вони включають засоби захисту від переадресації пам'яті (ЗЗПП), ізоляції функціональних завдань (ЗІФЗ) і інші технічні рішення.

Засоби управління захистом інформації містять автоматизоване робоче місце служби безпеки (АРМ СБ) інформації, ФЗ ПЗ, спеціально розроблені для виконання управління захистом на програмному рівні, включаючи ведення журналу обліку і реєстрації доступу (ЖОРД) і організаційні заходи. АРМ СБ включає термінал безпеки, ПКВА, апаратуру запису кодів у фізичні ключі-паролі (АЗКП), необхідну кількість ключів-паролів і апаратуру реєстрації і документування інформації (АРДІ). Додатково до вказаних засобів, виконаних на апаратному і програмному рівнях, в необхідних випадках застосовуються організаційні заходи.

5. РОЗРАХУНОК НАДІЙНОСТІ МЕРЕЖІ

Однією з найважливіших характеристик комп'ютерної мережі є надійність. Підвищення надійності засновано на принципі запобігання несправностей шляхом зниження інтенсивності відмов і збоїв за рахунок застосування електронних схем і компонентів з високим і надвисоким ступенем інтеграції, зниження рівня перешкод, полегшених режимів роботи схем, забезпечення теплових режимів їх роботи, а також за рахунок вдосконалення методів збірки апаратури.

Відмовостійкість — це така властивість комп'ютерної системи, яка забезпечує їй як логічній машині можливість продовження дій, заданих програмою, після виникнення несправностей. Введення відмовостійкості вимагає надмірного апаратного і програмного забезпечення. Напрями, пов'язані із запобіганням несправностей і відмовостійкістю, основні в проблемі надійності. На паралельних комп'ютерних системах досягається як найвища продуктивність, так і, у багатьох випадках, дуже висока надійність. Наявні ресурси надмірності в паралельних системах можуть гнучко використовуватися як для підвищення продуктивності, так і для підвищення надійності.

Поняття надійності включає не тільки апаратні засоби, але і програмне забезпечення. Головною метою підвищення надійності систем є цілісність збережених в них даних.

Визначення очікуваної надійності проектованої мережі здійснюється розрахунковим способом. Надійність мережі в першу чергу визначається надійністю елементів конструкції і компонентів схеми, що її складають, з урахуванням умов експлуатації.

Для розрахунку надійності необхідно мати логічну модель безвідмовної роботи мережі, яка складається на основі логічного аналізу принципової і функціональної схеми. При її складанні передбачається, що відмови елементів і компонентів незалежні, а елементи, компоненти і система в цілому можуть знаходитися в одному з двох станів: працездатному або непрацездатному. В теорії надійності розрізняють два типи з'єднань елементів на логічній схемі

надійності: послідовне (основне) з'єднання і паралельне (резервне) з'єднання. Послідовним з'єднанням елементів називається таке з'єднання при якому відмова будь-якого елемента приводить до відмови всієї системи в цілому (рисунок 5.1).

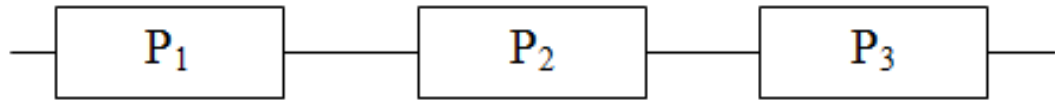


Рисунок 5.1 - Послідовне з'єднання елементів

Якщо вважати первинні пошкодження елементів незалежними подіями, то ймовірність безвідмовної роботи при послідовному з'єднанні може бути виражений на підставі теореми множення ймовірності наступною формулою:

$$P_0(t) = P_1(t) \cdot P_2(t) \dots P_N(t) = \prod_{j=1}^N P_j(t) \quad (5.1)$$

де P_j , $j = 1, 2, 3, \dots, N$ – ймовірність безвідмовної роботи окремих елементів системи.

При експоненціальному законі розподілу $P_j(t) = e^{-\lambda_j t}$, де λ_j – інтенсивність відмов елемента, ймовірність безвідмовної роботи має вигляд:

$$P_0(t) = e^{-\sum_{j=1}^N \lambda_j t} \quad (5.2)$$

Середній час безвідмовної роботи системи при послідовній моделі надійності дорівнює

$$T_{cp} = \frac{1}{\sum_{j=1}^N \lambda_j} \quad (5.3)$$

Паралельним з'єднанням називається таке з'єднання, при якому відмова системи відбувається тільки при відмові всіх елементів входять в нього (рисунок 5.2). Ймовірність безвідмовної роботи при паралельній схемі надійності визначається за формулою:

$$P_{пар} = 1 - \prod_{j=1}^m (1 - e^{-\lambda_j t}) \quad (5.4)$$

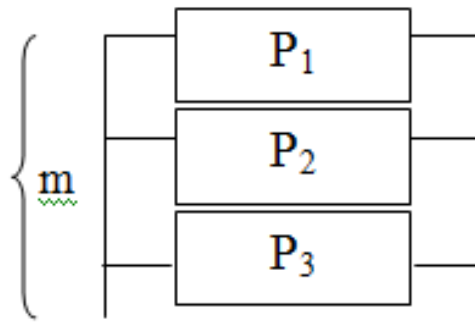


Рисунок 5.2 - Паралельна схема надійності

При паралельному з'єднанні елементів надійність всієї системи завжди більше надійного елемента. Паралельне з'єднання елементів використовується з метою підвищення надійності системи для забезпечення резервування. Для виконання розрахунку надійності проектованої системи необхідно проаналізувати передбачувані умови і режими експлуатації виробу, сформулювати поняття відмови для даної системи. Початковими даними для розрахунку надійності системи є: кількість елементів кожного типу входять в проектовану систему N_j ; інтенсивності відмов складових елементів системи λ_j ; розрахунковий час для визначення характеристик надійності t_p (середній час розрахунку, період експлуатації і т.д.).

Для розрахунку надійності мережі треба розбити всю проектовану мережу на групи. Групи повинні складатися, так щоб при відмові хоча б однієї групи не відмовила б уся мережа. В даному проекті комп'ютерна мережа вважається непрацездатною у разі неможливості всіма співробітниками використовувати ресурси мережі. Це може відбутися у разі збою хоча б однієї з наступної групи: сервер, робочі станції, концентратори, кабелі, роз'єми. Це все зображено на схемі надійності мережі (рисунок 5.3).

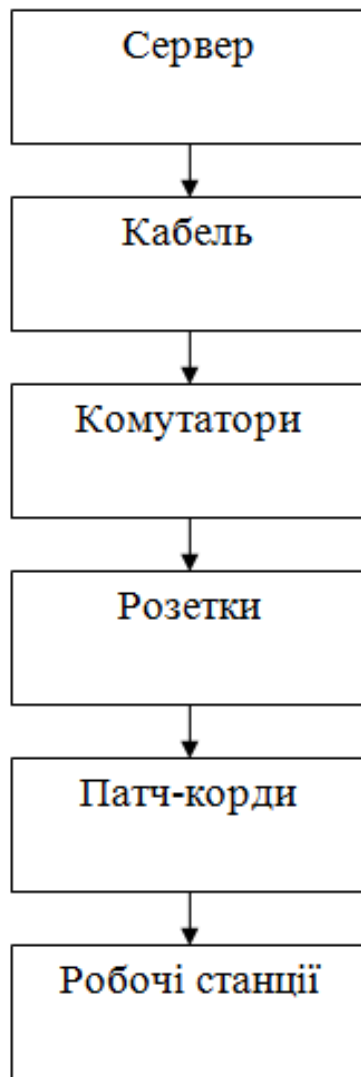


Рисунок 5.3 – Структурна схема надійності мережі

Далі потрібно скласти таблицю характеристик надійності елементів мережі (таблиця 5.1). У цю таблицю повинна увійти кожна група, кількість її елементів, інтенсивність відмов елементів λ_j , математичний добуток $N_j \lambda_j$.

Таблиця 5.1 - Характеристики надійності елементів

Номер групи	Найменування елементів	Число елементів	$\lambda \cdot 10^{-6}, 1/\text{год.}$	$N_j \lambda_j$
1	Сервер	1	0,065	$0,065 \cdot 10^{-6}$
2	Робочі станції	12	0,065	$2,15 \cdot 10^{-6}$
3	Комутатори	2	0,073	$0,22 \cdot 10^{-6}$
4	Один кабельний фрагмент (з врахуванням роз'ємів)	15	0,023	$17,78 \cdot 10^{-6}$
5	Розетки	12	0,025	$0,85 \cdot 10^{-6}$
6	Патч-корд	12	0,042	$1,43 \cdot 10^{-6}$

Результуюча інтенсивність відмов системи розраховується за формулою:

$$\lambda_0 = \sum_{j=1}^k N_j \cdot \lambda_j, \quad (5.5)$$

де k – кількість груп; $N_j \lambda_j$ – математичний добуток кількості елементів групи та інтенсивності відмов.

$$\lambda_0 = (0,065 + 2,15 + 0,22 + 17,78 + 0,85 + 1,43) = 22,49 \cdot 10^{-6}.$$

Час безвідмовної роботи визначається за формулою:

$$T_0 = \frac{1}{\lambda_0}, \quad (5.6)$$

Тому $T_0 = 0,044 \cdot 10^6$ годин.

Ймовірність безвідмовної роботи знаходиться за формулою:

$$P_0 = e^{-\lambda_0 \cdot T_{cp}}, \quad (5.7)$$

де T_{cp} – середній час безвідмовної роботи.

Для побудови залежності ймовірності безвідмовної роботи мережі від часу проведено розрахунки для різних моментів часу, результати яких представлено у таблиці 5.2.

Таблиця 5.2 – Результати розрахунків ймовірності безвідмовної роботи

Час роботи, год.	Ймовірність безвідмовної роботи
1000	0,9777
5000	0,8935
10000	0,7985
20000	0,6376
30000	0,5092

На рисунку 5.4 наведено графічну інтерпретацію результатів розрахунків, що відображає зменшення ймовірності безвідмовної роботи мережі з тривалістю часу її функціонування.

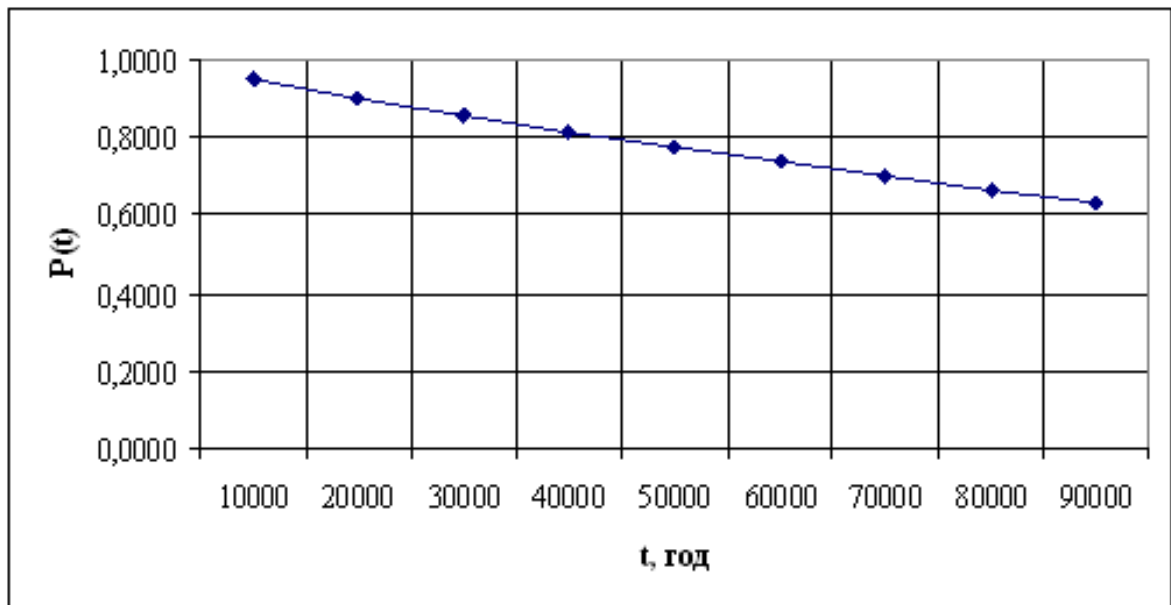


Рисунок 5.4 – Залежність ймовірності безвідмовної роботи від часу функціонування мережі

Середній час безвідмовної роботи:

$$T_0 = \frac{1}{\lambda_0} = \frac{1}{5,089 \cdot 10^{-6}} = 19650 \text{ годин} \approx 27 \text{ місяців.}$$

Ймовірність безвідмовної роботи системи для 10000 годин:

$$P_0 = e^{-\lambda_0 \cdot T_{cp}} = e^{-5,089 \cdot 10^{-6} \cdot 10000} = 0,9504.$$

Згідно розрахунків $P_{\text{розрахункове}} > P_{\text{задане}}$, це свідчить проте, що дана комп'ютерна мережа надійна.

6. ЕКОНОМІЧНИЙ РОЗРАХУНОК ЛОКАЛЬНОЇ МЕРЕЖІ ТОВ «ТЕРНОВСЬКИЙ ХЛІБЗАВОД»

При техніко-економічному обґрунтуванні впровадження нової комп'ютерної мережі та системи відео спостереження необхідною частиною проекту повинен бути розрахунок капітальних вкладень. Кошторисна вартість розробки обчислювальної мережі - це сума грошових коштів, визначуваних кошторисними документами, необхідних для її здійснення відповідно до проекту. Кошторисна вартість обчислювальної мережі, затверджена підрядником і замовником, виконує роль ціни на дану мережу. Локальний кошторис є первинним документом і складається на монтажні роботи, придбання і монтаж устаткування. Кошторисна вартість устаткування і матеріалів визначається на підставі відомостей на придбання устаткування і матеріалів. Локальний кошторис є первинним документом, на підставі якого визначається вартість окремих видів робіт і витрат, що входять в об'єктний кошторис. Локальні кошториси складаються на будівельні і монтажні роботи, придбання і монтаж устаткування і на інші цілі. Кошторисна вартість устаткування, матеріалів і виробів визначається на підставі відомостей на придбання устаткування, матеріалів і виробів і оптових цін, які вказані в прейскурантах цін на промислову продукцію, а також тимчасових, лімітних і договірних цін. Крім того, можуть використовуватися каталоги цін різних фірм і інформаційні списки зайвих і невживаних матеріальних цінностей, що пред'являються до реалізації підприємствами. Кошторисна вартість устаткування, окрім оптових цін, включає вартість запасних частин, тари і упаковки, комплектації устаткування, транспортних і заготовчо-складських витрат. Кошторисна вартість монтажних і пусконаладжувальних робіт визначається на підставі об'єму або кількості відповідних видів робіт по монтажу. Спираючись на розроблений проект з технічного забезпечення мережі, проводяться розрахунки матеріальних витрат (таблиця 6.1, 6.2, 6.3, 6.4, 6.5, 6.6).

Таблиця 6.1 – Загальні витрати на обладнання мережі та системи відео спостереження

Назва		Кількість	Вартість, грн.	Сума, грн.
Кабель UTP		350 м	3,00	1050,00
Коннектор для UTP		28	1,00	28,00
ADSL модем D-Link DSL-300L		1	350,00	350,00
Комутатор D-Link 8-портовий 10/100 (DES-1008D)		1	185,00	185,00
Блок безперебійного живлення Mustek Power Must 650 Office		1	475,00	475,00
Система відео спостереження		1	7574,00	7574,00
Програмне забезпечення		12	1276,00	17990,00
Ком-п'ютери	Робочі станції	12	30063,00	30063,00
	Сервер	1	3350,00	3350,00
	Відео сервер	1	3288,00	3288,00
Загальна сума				64353,00

Таблиця 6.2 – Розрахунок елементів серверу

Назва	Кількість, шт.	Вартість, грн.	Сума, грн.
Корпус- CoolerMaster CMP 350	1	530,00	530,00
Материнська плата- Intel (G41) 6 USB / 1 x PCI-Ex16 / 1 x PCI-Ex1 / 2 x PCI / 1 x COM / 1 x LPT / RJ-45 (LAN) / VGA / DVI / HDMI / Audio	1	740,00	740,00
Процесор- Intel Core 2 Quad, частота 2.66 ГГц	1	1105,00	1105,00
Оперативна пам'ять - 4 Гб DDR3 1333 МГц	1	470,00	470,00
Жорсткий диск - Samsung HD322GJ, 500 GB 7200 rpm 16Mb cache SATA II-300;	1	415,00	415,00
Мережева карта - D-Link DFE-520TX 1-port UTP 10/100Mbps PCI, OEM	2	45	90,00
Загальна сума			3350,00

Таблиця 6.3 – Розрахунок елементів робочих станцій

Назва	Кількість, шт.	Вартість, грн	Сума, грн
Процесор - Intel Pentium Dual Core E5500 (2.8 ГГц)	11	452,00	4,972
Материнська плата - ASUS P5KPL-AM IN/ROEM/SI 4 USB / 1 x PCI- Ex16 / 1 x PCI-Ex1 / 2 x PCI / 1 x COM / 1 x LPT / RJ-45 (LAN) / VGA / DVI / Audio	11	421,00	4,631
Оперативна пам'ять - DDR3-1333 1 ГБ	11	220,00	2,420
Жорсткий диск - ATA 250 GB WD WD2500AVJB 8MB 7200rpm	11	320,00	3,520
Відео карта Інтегрована Intel GMA 4500	11	-	-
Корпус - Logispower 4401 - 400w 8cm	11	295,00	3,245
Монітор - 18.5" Samsung E1920N	11	875,00	9,625
Клавіатура - SVEN Standard 304, USB	11	65,00	715,00
Мишка Logitech B110 Optical Mouse USB	11	60,00	660,00
Мережевий фільтр	12	25,00	275,00
Загальна сума			30063,00

Таблиця 6.4 - Розрахунок елементів системи відео спостереження

Назва	Кількість, шт.	Вартість, грн	Сума, грн
Плата відео захоплення Spotter 2.8	1	1600,00	1600,00
Вулична кольорова відеокамера RainBow TC-520C	4	604,00	2416,00
Купольна кольорова відеокамера InterVision HP-5540C	4	437,00	1748,00
Блок живлення ІБП 3.5А	1	470,00	470,00
Коаксіальний кабель Euro SAT RG-59 100 м.	2	280,00	560,00
Коннектор BNC	8	7,00	56,00
F - коннектор RG59	8	5,00	40,00
Роз'єм живлення 12V MD1620 male	8	8,00	64,00
Кабель сигнальний СЕНК 2x0,22 неекранований 100 м.	2	310,00	620,00
Загальна сума			7574,00

Таблиця 6.5 – Розрахунок елементів робочої станції відео спостереження

Назва	Кількість, шт.	Вартість, грн	Сума, грн
Процесори-AMD Athlon II X2 245 (Tray) (ADX2450CK23GQ) (2.90 ГГц/AM3/КешL2:2МБ/Шина: 2.0 МГц/AMD64/0.045 мкм/65W)	1	452,00	452,00
Материнська плата-ASUS P5G41-M LE/C/SI (G41 /ICH7,s775, FSB1333/1066/800, 4DualDDR2_1066 - 800, 1xPCIex16, 1xPCIe	1	431,00	431,00
Оперативна пам'ять-DDR 2 1024 Mb 800 MHz PC-6400 SAMSUNG	1	230,00	230,00
Жорсткий диск - HITACHI 1,0Tb SATA-II, 7200rpm 32Mb	1	320,00	320,00
Відео карта - GeForce GT220 512MB DDR2 128bit DVI (550/800) GE	1	560,00	560,00
Корпус- Logicpower 4401 - 400w 8cm	1	295,00	295,00
Монітор TFT 22" Samsung E2220N (CLYSBU) TFT , 22", black, TN, 16:9, 5ms, D-Sub, 300/70000:1(DC), 170/160	1	875,00	875,00
Клавіатура- SVEN Standard 304, USB	1	65,00	65,00
Мишка- Logitech B110 Optical Mouse USB	1	60,00	60,00
Загальна сума			3288,00

Таблиця 6.6 – Програмне забезпечення

Назва	Кількість, шт.	Ціна за одиницю, грн.	Вартість, грн.
Windows Server 2003	1	2678,00	2678,00
Windows XP Professional Rus (Service Pack 3)	12	1276,00	15312,00
Загальна сума			17990,00

Розрахунок кошторисної вартості комп'ютерної системи.

1) Матеріальні витрати становлять загальну суму витрат на устаткування, які приведені в таблицях 6.1, 6.2, 6.3, 6.4, 6.5 і 6.6 містить 64353,00 грн., далі буде визначатися, як коефіцієнт C_m .

2) Витрати на основну й додаткову заробітну плату представлені в таблиці 6.7. Враховуючи, що на підприємстві працює системний адміністратор як

штатний співробітник, він буде виконувати роботи по організації мережі та її налагоджуванню.

Таблиця 6.7 – Витрати на основну й додаткову заробітну плату

Основна заробітна плата системного адміністратора за 1 місяць	ЗП	1500,00
Додаткова заробітна плата системному адміністратора за 1 місяць	дод. ЗП	487,00
Нарахування на ЗП:		
Відрахування до фонду соціального страхування	(осн. ЗП + дод. ЗП)*1,4 %	36,78
Відрахування до пенсійного фонду	(осн. ЗП + дод. ЗП)*33,2 %	800,64
Відрахування до фонду зайнятості	(осн. ЗП + дод. ЗП)*1,6 %	44,32
Всього		2868,74

3) Амортизація мережі визначається за формулою:

$$C_a = K_{\sigma} \cdot H_a, \quad (6.1)$$

де C_a – амортизації комп'ютерної системи; K_{σ} – балансова (первинна) вартість системи – 64353,00 грн; H_a – норма амортизації 0,25.

$$C_a = 64353,00 \cdot 0,25 = 16088,25 \text{ грн.}$$

4) Собівартість визначається як сума всіх витрат і визначається за формулою:

$$C = C_m + C_{zn} + C_a, \quad (6.2)$$

$$C = 64353,00 + 16088,25 + 2868,74 = 83309,99 \text{ грн.}$$

Розрахунковий прибуток визначається за формулою:

$$\Pi_p = (C - C_n) \cdot P, \quad (6.3)$$

де Π_p – розрахунковий прибуток; C – собівартість; C_n – вартість купувальних матеріалів; P – рентабельність продукції 0,5 (дані підприємства).

$$\Pi_p = (83309,99 - 64353,00) \cdot 0,5 = 9478,50 \text{ грн.}$$

5) Витрати на комп'ютерну систему K_c визначається за формулою:

$$K_c = C + P_p, \quad (6.4)$$

де C – витрати на систему; P_p – розрахунковий прибуток.

$$K_c = 83309,99 + 9478,50 = 92788,49 \text{ грн.}$$

6.1 Економічна ефективність розробки й впровадження системи

Основним показником економічної ефективності функціонування системи є підвищення ефективності керування інформацією у вигляді зниження витрат на керування при одночасному збільшенні швидкості і якості одержання потрібного результату.

Крім багатьох інших негативних ефектів, ручна обробка інформації спричиняє наступні негативні економічні ефекти: високі витрати по складуванню паперових документів і відео файлів (сейфи, шафи, папки диски й ін.); підвищені витрати на канцтовари; витрати, зв'язані з роботою виявлення раніше допущених помилок (людський фактор).

До числа основних факторів, що визначають приріст прибутку у зв'язку з упровадженням програми, відносяться: підвищення продуктивності праці й скорочення робочого часу.

Крім того, не піддається прямій грошовій оцінці підвищення оперативності керування, якості одержуваних результатів, поліпшення організації праці й т.д.

Обов'язковою умовою визначення економічної ефективності системи є порівнянність усіх показників у часі, за цінами й іншими нормами, які використовуються для визначення показників, по змісту й колі елементів витрат.

Визначення прямої економічної ефективності ґрунтується на тому, що впровадження системи вивільняє 3,7 працівника.

Час за який система себе окупає визначається за формулою:

$$T = \frac{K}{\Delta C}, \quad (6.5)$$

де T – час, за який система себе окупає; K – витрати на розробку системи, які визначаються за формулою:

$$K = C_n + Z_i \cdot M, \quad (6.6)$$

де C_n – витрати на купівельні матеріали; Z_i – заробітна плата системного адміністратора; M – час проектування мережі – 2 місяця.

$$K = 64353,00 + (1500 \cdot 2) = 67353,00 \text{ грн.}$$

Зарплата ΔC за рік робітників, яких звільнили визначається за формулою:

$$\Delta C = Z_p \cdot K_z, \quad (6.7)$$

де ΔC – зарплата за рік робітників яких звільнили; Z_p – за рік робітників 24300 грн; K_z – коефіцієнт робітників, яких звільнили дорівнює 1,4.

$$\Delta C = 24300 \cdot 1,4 = 34020 \text{ грн.}$$

Тоді час, за який система себе окупає, буде дорівнювати:

$$T = \frac{64353,00}{34020} \approx 1,8 \text{ роки.}$$

Виходячи з розрахунків можна зробити висновок, що впровадження цієї мережі в підприємство є доцільним. Разом з розрахованим економічним ефектом впровадження даної системи забезпечить появу непрямого економічного ефекту, який не підлягає прямому розрахунку. Це свідчить про те що впровадження системи забезпечить значну економію, що виражено в наступних показниках:

- вивільнення робочого часу;
- збільшення продуктивності роботи працівників;
- оперативний доступ до актуальної інформації про поставку і найменування товару;
- наявність надійного й швидкого каналу зв'язку з іншими відділами;
- мінімізація документообігу між підрозділами ТОВ «Терновський хлібзавод».

Так як час, за який мережа себе окупає становить приблизно 1,8 роки, цю систему можна вважати рентабельною.

7. ОХОРОНА ПРАЦІ

7.1 Аналіз умов праці

Локальна мережа, що проектується, буде встановлена у приміщеннях на першому та другому поверхах.

При монтажі, випробуваннях, експлуатації і всіх видах технічного обслуговування системи можуть виникнути наступні види небезпеки:

- електробезпека;
- шум, вібрація.

Силові ланцюги 220 В є джерелом небезпеки. Напруга 220 В, при замиканні людським тілом з опором 1000 Ом, збуджує струм 220 мА, що є смертельним для людини.

Робота ЕОМ є джерелом шуму і вібрації. Дія шуму виявляється при тривалому перебуванні поблизу працюючого устаткування. Це може привести до погіршення слуху і розладу нервової системи. Тривала дія технологічної вібрації приводить до погіршення самопочуття, нервовим розладам, головнуболлю і т.д. Тому найбільш шумний пристрій – сервер локальної мережі.

7.2 Оздоровлення повітряного середовища

Для здоров'я людини і для охорони його праці велике значення має якість повітря у приміщенні офісу.

Температура, відносна вологість, швидкість руху повітряного потоку, ГДК шкідливих речовин нормуються по ГОСТ 12.1.005 –76 ССБТ «Повітря робочої зони».

При оцінці допустимих значень температури і вологості повітря враховується категорія тяжкості робіт відповідно до загальних енергетичних витрат.

Таблиця 7.1 – Оптимальні норми мікроклімату для приміщень з ЕОМ

Період року	Категорія робіт	Температура повітря, 0С не більше	Відносна вологість повітря, %	Швидкість руху повітря, м/с
Холодний	легка - 1а	22 – 24	40 – 60	0,1
	легка - 1б	21 – 23	40 – 60	0,1
Теплий	легка - 1а	23 – 25	40 – 60	0,1
	легка - 1б	22 – 24	40 – 60	0,2

По характеру робіт наше підприємство можна віднести до 1 категорії.

Визначаються оптимальні норми температури, відносної вологості і швидкості руху повітря в офісі. Для холодного і перехідного періодів року температура 23⁰С, відносна вологість 40-60 %, швидкість руху повітря не більше 0,1 м/с. Для теплого періоду року температура повітря 22-25⁰С, а решта параметрів такі ж.

Таблиця 7.2 – Оптимальні та допустимі параметри температури і вологості

Оптимальні параметри		Допустимі параметри	
Температура, 0С	Відносна вологість, %	Температура, 0С	Відносна вологість, %
19	62	18	39
20	58	22	31
21	55		

Для температурного контролю використовується кондиціонер, що забезпечує замкнений цикл циркуляції повітря в приміщенні, яке при необхідності можна підігрівати, зволожувати або, навпаки, осушувати. Для вентиляції та подачі в приміщення зовнішнього повітря, використовується механічна вентиляція за допомогою вентиляторів.

Таблиця 7.3 – Рівні іонізації повітря приміщень при роботі з ЕОМ

Рівні	Кількість іонів в 1 см ³ повітря	
	n^+	n^-
Мінімально необхідне	400	600
Оптимальні	1500 – 3000	300 – 5000
Максимально допустимі	50000	50000

7.3 Електробезпека

Приміщення, в якому буде встановлена дана мережа, відноситься до приміщень по ГОСТ 12.1.006-84 з особливою електробезпекою, де не виключається можливість дотику людини до з'єднаних із землею металоконструкцій.

Живлення електроустаткування проводиться від мережі 220 В, частотою 50 Гц.

На вимогу до електробезпеки система відноситься до 1 класу ГОСТ 12.1.002-84.

Як система захисту від небезпек переходу напруги на конструктивні частини устаткування у разі пробією ізоляції вибираємо захисне заземлення корпусів пристроїв.

Проводимо розрахунок захисного заземлення.

Вибираємо контурний вид захисного заземлення.

Як вертикальні штучні заземлення застосуємо кутову сталь розміром 60х60 мм завдовжки 2,5 м. Для зв'язку вертикальних заземлень і як заземлюючих провідників використовуємо смугову сталь перетином 4х12 мм. Устаткування, що заземляється, приєднуємо до магістралей заземлення через стандартні розетки типу «EURO». Визначимо розрахунковий питомий опір ґрунту ρ .

$$\rho = \rho_{изм} \cdot \varphi.$$

7.4 Захист від шуму і вібрації

При виконанні основної роботи на моніторах і ПЕОМ (диспетчерські, операторські, розрахункові, кабіни і пости управління, зали обчислювальної техніки і ін.) 12.1.012-78, ГОСТ 12.1.034-81, ГОСТ 12.1.042-84, ГОСТ 12.1.043-84 де працюють інженерно-технічні працівники, що здійснюють лабораторний, аналітичний або вимірювальний контроль, рівень шуму не повинен перевищувати 60 дБ.

У приміщеннях операторів ЕОМ (без дисплеїв) рівень шуму не повинен перевищувати 65 дБ.

На робочих місцях в приміщеннях для розміщення шумних агрегатів обчислювальних машин (АЦПУ, принтери і ін.) рівень шуму не повинен перевищувати 75 дБ.

Найбільш шумливе устаткування (АЦПУ, принтери і ін.), рівні шуму якого перевищують нормовані, повинне знаходитися поза приміщенням з монітором і ПЕОМ.

Понизити рівень шуму в приміщеннях з моніторами і ПЕОМ можна використанням звукопоглинальних матеріалів з максимальними коефіцієнтами звукопоглинання області частот 63 – 8000 Гц для обробки приміщень, підтверджених спеціальними акустичними розрахунками.

Додатковим звукопоглинанням служать однотонні завіси з щільної тканини, що гармонують із забарвленням стін і підвішені в складку на відстані 15 – 20 см від огорожі. Ширина завіси повинна бути в два рази більше ширини вікна.

Таблиця 7.4 – Рівні звуку, еквівалентні рівні звуку та рівні звукового тиску в октавних смугах частот

Рівні звукового тиску, дБ									Рівні звуку, еквівалентні рівні звуку дБ
Середньгеометричні частоти октавних смуг, Гц									
31,5	63	125	250	500	1000	2000	4000	8000	
	59	48	40	34	30	27	25	23	35
	63	52	45	39	35	32	30	28	40
	67	57	49	44	40	37	35	33	45
86	71	61	54	49	45	42	40	38	50
93	79	70	63	58	55	52	50	49	60
96	83	74	68	63	60	57	55	54	65
103	91	83	77	73	70	68	66	64	75

Таблиця 7.5 – Санітарні норми вібрації категорії «три» технологічного типу «В»

Середньоггеометричні частоти смуг, Гц	Допустимі значення по осям X0, Y0, Z0							
	Віброприскорення				Віброприскорення			
	2 м/с		дБ		2 м/с ¹⁰		дБ	
	1/3окт	1/1окт	1/3окт	1/1окт	1/3окт	1/1окт	1/3окт	1/1окт
1,6	0,0125	0,02	31	36	0,13	0,18	88	91
2	0,112		32		0,089		85	
2,5	0,01		30		0,063		82	
3,15	0,009	0,014	29	33	0,0445	0,063	79	82
4	0,008		28		0,032		76	
5	0,008		28		0,025		74	
6,3	0,008	0,014	28	33	0,02	0,032	72	76
8	0,008		28		0,016		70	
10	0,01		30		0,016		70	
12,5	0,0125	0,028	35	39	0,016	0,028	70	75
16	0,016		34		0,016		70	
20	0,0196		36		0,016		70	
25	2,025	0,056	38	45	0,016	0,28	70	75
31,5	0,04		40		0,016		70	
40			42		0,016		70	

Таблиця 7.6 – Допустимі норми вібрації на всіх робочих місцях з ЕОМ

Середньоггеометричні частоти смуг, Гц	Допустимі значення			
	По віброприскоренню		По віброшвидкості	
	Осі X, Y			
	мс - 2	дБ	мс - 1	дБ
2	5,3 x 10	25	4,5 x 10	79
4	5,3 x 10	25	2,2 x 10	73
8	5,3 x 10	25	1,1 x 10	67
16	1,0 x 10	31	1,1 x 10	67
31,5	2,1 x 10	37	1,1 x 10	67
63	4,2 x 10	43	1,1 x 10	67
Кориговані значення та їх рівні в дБ	9,3 x 10	30	2,0 x 10	72

7.5 Вимоги до моніторів та ЕОМ

Конструкція монітора повинна забезпечувати можливість фронтального спостереження екрану шляхом повороту корпусу в горизонтальній площині навколо вертикальної осі в межах плюс мінус 30° і у вертикальній площині навколо горизонтальної осі в межах плюс мінус 30° з фіксацією в заданому положенні. Дизайн моніторів повинен передбачати забарвлення в спокійні м'які

тони з дифузним розсіюванням світла. Корпус монітора і ПЕОМ, клавіатура повинні мати матову поверхню одного кольору з коефіцієнтом віддзеркалення 0,4 – 0,6 і не мати блискучих деталей, здатних створювати відблиски.

Конструкція монітору повинна передбачати наявність ручок регулювання яскравості і контрасту, забезпечуючи можливість регулювання яскравості і контрасту, забезпечуючи можливість регулювання цих параметрів від мінімальних до максимальних значень.

Монітори і ПЕОМ повинні забезпечувати потужність експозиційної дози рентгенівського випромінювання в будь-якій крапці на відстані 0,05 м від екрану і корпусу монітора при будь-яких положеннях регулювальних пристроїв не повинна перевищувати $7,74 \times 10^{-4}$ А/кг, що відповідає еквівалентній дозі, рівній 0,1 мбэр/год (100 мкР/год).

Таблиця 7.7 – Візуальні ергономічні параметри моніторів, та межі їх змінення

Найменування параметру	Межі значень параметру	
	<i>min</i> (не менше)	<i>max</i> (не більше)
Яскравість знака (яскравість фону), кд/м ² (зміряна в темряві)	35	120
Зовнішня освітленість екрана, лк	100	250
Кутовий розмір знака, кут. хв.	16	60

Примітки:

1) Оптимальним діапазоном значень візуального ергономічного параметра називається діапазон, в межах якого забезпечується безпомилкове прочитування інформації при часі реакції людини - оператора, що перевищує мінімальне, встановлене експериментально для даного типа монітору, не більше, ніж в 1,2 разу.

2) Допустимим діапазоном значень візуального ергономічного параметра називається діапазон, при якому забезпечується безпомилкове прочитування інформації, а час реакції людини-оператора перевищує мінімальне, встановлене експериментально для даного типа монітору, не більше, ніж в 1,5 разу.

3) Кутовий розмір знаку – кут між лініями, що сполучають крайні точки знаку по висоті і око спостерігача. Кутовий розмір знаку визначається по

формулі: $a = \arctg(h/2l)$, де h – висота знаку, l – відстань від знаку до ока спостерігача.

4) Дані, приведені в справжній таблиці, підлягають коректуванню у міру введення в дію нових стандартів, що регламентують вимоги і норми на візуальні параметри моніторів.

Таблиця 7.8 – Нормовані візуальні параметри моніторів

Контраст (для монохромних моніторів)	Від 3 : 1 до 1,5 : 1
Нерівномірність яскравості елементів знаків, %	Не більш ± 25
Нерівномірність яскравості робочого поля екрану, %	Не більш ± 20
Формат матриці знаку: для прописних букв і цифр (для відображення діакритичних знаків і рядкових букв з нижніми виносними елементами формат матриці повинен бути збільшений зверху або знизу на 2 елементи зображення)	Не менше 7 * 9 елементів зображення Не менше 5 * 7 елементів зображення
Відношення ширини знаку до його висоти для прописних букв	від 0,7 до 0,9 (припускається від 0,5 до 1,0)
Розмір мінімального елементу відображення (пікселя) для монохромного монітору, мм	0,3
Кут нахилу лінії спостереження, град.	Не більш 60 град нижче горизонталі
Кут спостереження, град.	Не більш 40 град. від нормалі до будь-якої точки екрану дисплея
Допустимий горизонтальний зсув однотипних знаків % від ширини знаку	не более 5
Допустимий вертикальний зсув однотипних знаків % від висоти матриці	не более 5
Відхилення форми робочого поля екрану монітора від правильного прямокутника не повинне перевищувати: - по горизонталі - по вертикалі - по діагоналі де $B1$ і $B2$ - значення довжин верхнього і нижнього рядків тексту на робочому полі екрану, мм; $H1$ і $H2$ - значення довжин крайніх стовпців на робочому полі екрану, мм; $D1$ і $D2$ значення довжин діагоналей робочого поля екрану, мм;	$\frac{B1 - B2}{B1 + B2} < 0,02$ $\frac{H1 - H2}{H1 + H2} < 0,02$ $\frac{D1 - D2}{D1 + D2} < 0,04 \text{ (H1 - H2)}$

Продовження таблиці 7.8

Допустима просторова нестабільність зображення (тремтіння по амплітуді зображення) при частоті коливань в діапазоні від 0,5 до 30 Гц, мм	- 4 Не більше 2 x L10 е (L-відстань спостереження мм)
Допустима тимчасова нестабільність зображення (мерехтіння)	не повинна бути зафіксована 90 % спостерігачів
Відбивна здатність, дзеркальне і змішане віддзеркалення (відблиски) % (допускається виконання вимоги при використанні приєктранного фільтру	Не більше 1

Примітки:

1) Дані, приведені в таблиці, підлягають коригуванню в міру введення в дію нових стандартів, що регламентують вимоги і норми на візуальні параметри моніторів.

2) Під нерівномірністю яскравості розуміються відносини:

$$U^{+} = (L_{\max} - L) / L_{cp} \text{ (позитивна нерівномірність)}$$

$$U^{-} = (L_{\min} - L) / L_{cp} \text{ (від'ємна нерівномірність)}$$

$$L_{cp} = \sum_{i=1}^n \frac{L_i}{N},$$

де n – число зміряних значень яскравості, $L_{\max}$ – максимальне значення яскравості, $L_{\min}$ – мінімальне значення яскравості.

3) Розмір елементу зображення (пікселя) визначається фотометрично на рівні 50% максимальної яскравості.

8. ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

8.1 Вступна частина

У наш час захист навколишнього середовища висувається на перший план. Наслідки недостатньої уваги до проблеми можуть бути катастрофічними. Мова йде не тільки про добробут людства, а про його виживання. Особливо тривожно те, що деградація природного середовища і може виявитися необоротною.

Під охороною навколишнього середовища розуміють сукупність міжнародних, державних і регіональних правових актів, інструкцій і стандартів, які доводять загальні юридичні вимоги до кожного конкретного забруднювача і забезпечують його зацікавленість у виконанні цих вимог, конкретних природоохоронних заходів по втіленню в життя цих вимог.

Тільки якщо всі ці складові частини відповідають один одному за змістом і темпами розвитку, тобто складаються в єдину систему охорони навколишнього природного середовища, можна розраховувати на успіх.

Оскільки не була вирішена вчасно завдання охорони природи від негативного впливу людини, тепер все частіше постає завдання захисту людини від впливу змінилася природного середовища. Обидва ці поняття інтегруються в терміні "охорона навколишнього (людини) природного середовища".

Охорона навколишнього природного середовища складається з:

- правової охорони, що формулює наукові екологічні принципи у вигляді юридичних законів, обов'язкових для виконання;
- матеріального стимулювання природоохоронної діяльності з ціллю зробити її економічно вигідною для підприємств;
- інженерної охорони, що розробляє природоохоронну та ресурсозберігаючу технологію і техніку.

Основними принципами охорони навколишнього природного середовища є:

- пріоритет забезпечення сприятливих екологічних умов для життя, праці та відпочинку населення;
- науково обґрунтоване поєднання екологічних і економічних інтересів

суспільства;

- облік законів природи і можливостей самовідновлення і самоочищення її ресурсів;
- недопущення незворотних наслідків для охорони природного середовища і здоров'я людини;
- право населення та громадських організацій на своєчасну і достовірну інформацію про стан навколишнього середовища та негативному впливі на неї і на здоров'я людей різних виробничих об'єктів;
- невідворотність відповідальності за порушення вимог природоохоронного законодавства.

8.2 Забруднення навколишнього середовища підприємствами

Забруднення навколишнього середовища – надходження в природне середовище будь-яких твердих, газоподібних речовин, мікроорганізмів або енергій (у вигляді звуків, шумів, електромагнітного й радіоактивного випромінювання) у кількостях, що викликають зміну складу й властивостей компонентів природи й (або) чинять шкідливий вплив на людину, флору й фауну.

Види забруднень навколишнього середовища різні й різноманітні: викиди в атмосферу хімічних сполук і сумішей; надходження у водне середовище всіляких виробничих і комунально-побутових відходів, влучення в неї нафтових продуктів; засмічування ландшафтів сміттям і пакувальними матеріалами; забруднення полів, луків, лісів і водних об'єктів пестицидами; підвищення рівня іонізуючої радіації, виробничих і побутових шумів, вібрацій, а також нагромадження тепла в атмосфері.

У результаті господарської діяльності людини в атмосфері з'являється велика кількість забруднюючих речовин. Взаємодія атмосферного повітря з водою і ґрунтом призводить до якісних і кількісних змін усієї біосфери в цілому, підсилюючи і прискорюючи небажані зміни складу і структури атмосферного повітря, клімату Землі. Найбільш сильні зміни клімату і якості атмосферного повітря спостерігаються у великих містах. Якщо кисень в атмосферному повітрі

буде дуже сильно забруднений усілякими речовинами, то поступово у всього живого на Землі буде скорочуватися термін життя, доки не зменшиться до винищення всіх і всього.

Різноманітне втручання людини в природні процеси в біосфері можна згрупувати за наступними видами забруднень, розуміючи під ними будь-які небажані для екосистем антропогенні зміни:

- інгредієнтне (інгредієнт – складова частина складного з'єднання або суміші) забруднення як сукупність речовин, кількісно або якісно далеких природнім біогеоценозам;
- параметричне забруднення (параметр навколишнього середовища – одне з його властивостей, наприклад рівень шуму, освітленості, радіації і т.д.), пов'язане зі зміною якісних параметрів навколишнього середовища;
- біоценотичне забруднення, що полягає у впливі на склад і структуру популяції живих організмів;
- стаціонально-деструкційне забруднення (стація – місце проживання популяції, деструкція – руйнування), яке являє собою зміну ландшафтів екологічних систем у процесі природокористування.

Відомо більше 200 забруднюючих атмосферу речовин, причому в міру освоєння нових технологічних процесів і створення нових продуктів виробництва число забруднюючих речовин зростає. Цьому сприяють також реакції в атмосфері й інших середовищах між забруднюючими речовинами під впливом сонячного світла, окислювально-відновних процесів і інших реакцій. Стрімкий розвиток усіх галузей промисловості, енергетики, транспорту, збільшення чисельності населення й урбанізація, хімізація всіх сфер діяльності людини привели до визначених змін навколишнього природного середовища, у тому числі несприятливих, що полягають головним чином у забрудненні біосфери. Вплив шкідливих речовин антропогенного походження на природне середовище, а так само відгук середовища на ці впливи стають глобальними, всеосяжними.

У великих містах до числа основних джерел забруднення атмосферного повітря відноситься автотранспорт. Гази двигунів, що відходять, містять

складну суміш, їх більш ніж двісті компонентів, серед яких чимало канцерогенів. Найбільш значимі фактори негативного впливу автомобільного транспорту на людину і навколишнє середовище наступні:

- забруднення повітря;
- забруднення навколишнього середовища;
- шум, вібрація;
- виділення тепла (розсіювання енергії).

Основна причина забруднення повітря полягає у неповному і нерівномірному згорянні палива. Всього 15% його витрачається на рух автомобіля, а 85% "летить на вітер". До того ж камери згорання автомобільного двигуна – це своєрідний хімічний реактор, що синтезує отруйні речовини і викидає їх в атмосферу.

Рухаючись зі швидкістю 80-90 км/год в середньому автомобіль перетворює на вуглекислоту стільки ж кисню, скільки 300-350 чоловік. Але справа не тільки в вуглекислоті. Річний вихлоп одного автомобіля – це 800 кг окису вуглецю, 40 кг окислів азоту і більше 200 кг різних вуглеводнів. У цьому наборі дуже підступна окис вуглецю. Через високу токсичність її допустима концентрація в атмосферному повітрі не повинна перевищувати 1 мг/м³.

Рівень загазованості магістралей залежить від інтенсивності руху автомобілів, ширини і рельєфу вулиці, швидкості вітру, частки вантажного транспорту та автобусів в загальному потоці і інших факторів. При інтенсивності руху 500 транспортних одиниць на годину концентрація окису вуглецю на відкритій території на відстані 30-40 м від автомагістралі знижується в 3 рази і досягає норми.

Ускладнене розсіювання викидів автомобілів на тісних вулицях. У результаті практично всі жителі міста відчувають на собі шкідливий вплив забрудненого повітря.

Чадний газ і окиси азоту, настільки інтенсивно виділяються на перший погляд безневинним голубуватим димком глушника автомобіля – ось одна з основних причин головних болів, втоми, невмотивованого роздратування, низькою працездатності. Сірчистий газ здатний впливати на генетичний апарат,

сприяючи безпліддя і природженої потворності, а всі разом ці чинники ведуть до стресів, нервовим проявам, прагненню до усамітнення, байдужості до найближчих людей. У великих містах також більш широко поширені захворювання органів кровообігу і дихання, інфаркти, гіпертонія і новоутворення. За розрахунками фахівців, "внесок" автомобільного транспорту в атмосферу становить до 90% по окису вуглецю і 70% по окису азоту. Автомобіль також додає в ґрунт і повітря важкі метали та інші шкідливі речовини.

В умовах сильного міського шуму відбувається постійна напруга слухового аналізатора. Це викликає збільшення порогу чутності (10 дБ для більшості людей з нормальним слухом) на 10-25 дБ.

Високі рівні шуму в міському середовищі є одним з агресивних подразників центральної нервової системи. Міський шум справляє негативний вплив і на серцево-судинну систему. Ішемічна хвороба серця, гіпертонічна хвороба, підвищений вміст холестерину в крові зустрічаються частіше в осіб, що проживають у гучних районах.

Найбільші рівні шуму 90-95 дБ відзначаються на магістральних вулицях міст з середньою інтенсивністю руху 2-3 тис. і більше транспортних одиниць на годину.

Рівень вуличних шумів обумовлюється інтенсивністю, швидкістю і характером (складом) транспортного потоку. Крім того, він залежить від планувальних рішень (поздовжній і поперечний профіль вулиць, висота і щільність забудови) і таких елементів благоустрою, як покриття проїзної частини та наявність зелених насаджень. Кожен з цих факторів здатний змінити рівень транспортного шуму в межах до 10 дБ.

Шум, що виникає на проїжджій частині магістралі, поширюється не тільки на при магістральну територію, але і вглиб житлової забудови. Так, в зоні найбільш сильного впливу шуму знаходяться частини кварталів і мікрорайонів, розташованих уздовж магістралей загальноміського значення (еквівалентні рівні шуму від 67,4 до 76,8 дБ). Рівні шуму, заміряні в житлових кімнатах при відкритих вікнах, орієнтованих на зазначені магістралі, всього на 10-15 дБ

нижче.

8.3 Основні заходи щодо зниження забруднення атмосферного повітря викидами автомобільного транспорту

Увага вчених, інженерів, агрономів, інших фахівців і громадськості зосереджено на усуненні всіх видів забруднюючих речовин, що представляють найбільшу небезпеку для здоров'я людей. Способи й шляхи боротьби із забрудненнями навколишнього середовища різноманітні: пристрої очисних споруджень, установка фільтрів, створення й впровадження безвідхідних технологій, замкнутих циклів водокористування, заміна хімічних способів боротьби зі шкідниками й хворобами сільськогосподарських і лісових рослин біологічними, звукопоглинаючі пристрої, використання відходів для одержання корисної продукції, пошуки нових видів палива, використання для технічних і побутових потреб тепла геотермальних джерел, сили вітру, морських припливів, сонячного тепла, установлення режиму користування автомобільним і авіаційним транспортом

Проблема забруднення навколишнього середовища автомобільним транспортом цілком очевидно є глобальною. По всьому світу кількість автомобілів з кожним днем збільшується в геометричній прогресії. Все більше і більше людей мають свою власну машину. Але багато хто зовсім не замислюється про те, до чого все це врешті-решт приведе. Для того, щоб зберегти людству автомобіль, необхідно якщо не виключити, то звести до мінімуму шкідливі викиди. Робота в цьому напрямі ведеться в усьому світі і дають певні результати. Автомобілі випускаються в даний час в промислово розвинених країнах, викидають шкідливих речовин у 10-15 разів менше, ніж 10-15 років тому. У всіх розвинених країнах відбувається посилення нормативів на шкідливі викиди при роботі двигуна. У 2000 р. введені більш суворі норми. Відбувається не тільки кількісне посилення норм, але і їх якісна зміна. Постійно розширюється перелік речовин, зміст яких має знаходитися під контролем.

В даний час йде боротьба з автомобільною небезпекою. Конструюються фільтри, розробляються нові види пального, що містять менше свинцю.

Загальні шляхи зниження екологічних збитків від транспорту полягають в наступному:

- оптимізація руху міського транспорту
- розробка альтернативних енергетичних джерел;
- опалювання і очищення органічного палива;
- створення (модифікація) двигунів, що використовують альтернативні палива;
- захист від шуму;
- економічні ініціативи з управління автомобільним парком і рухом.

8.4 Заходи запобігання забруднення навколишнього середовища застарілою комп'ютерною технікою підприємства

Природоохоронною є будь-яка діяльність, спрямована на збереження якості навколишнього середовища на рівні, що забезпечує стійкість біосфери. До неї відноситься як великомасштабна, здійснювана на загальнодержавному рівні діяльність, так і діяльність окремих підприємств.

Існують два основних напрямки природоохоронної діяльності підприємств. Перший – очищення шкідливих викидів. Цей шлях "у чистому вигляді" малоефективний, тому що з його допомогою далеко не завжди вдається цілком припинити надходження шкідливих речовин у біосферу. До того ж скорочення рівня забруднення одного компонента навколишнього середовища веде до посилення рівня забруднення іншого.

Другий напрямок – усунення самих причин забруднення, що вимагає розробки маловідходних, а в перспективі й безвідходних технологій виробництва, які дозволяють комплексно використовувати вихідну сировину й утилізувати максимум шкідливих для біосфери речовин.

Однак далеко не для всіх галузей знайдені прийнятні техніко-економічні рішення по різкому скороченню кількості відходів, що утворюються, і їхньої утилізації, тому в цей час доводиться працювати по обох зазначених напрямках.

Людство знаходиться в постійній залежності від процесу модернізації і

заміни електронної техніки. Виробництво офісного устаткування, комп'ютерів і мобільних пристроїв з кожним роком нестримно збільшується. Проте є в прогресу і неприваблива сторона – застарілу апаратуру, що вийшла з використання, необхідно кудись дівати – виникає поняття "електронне сміття", і про його об'єми можна лише здогадуватися.

На відміну від органічних відходів, техногенне сміття неможливо утилізувати, використовуючи природні процеси регенерації. Більш того, враховуючи присутність в багато компонентах важких металів і отруйних речовин, спалювати його подібно до побутових відходів теж не можна. Переробка застарілої електроніки вимагає значних зусиль і є чималою проблемою. Ігнорувати її неможливо, тому що вона несе серйозну загрозу для екології.

Навіть по приблизним оцінках з 1991 р. до України було завезено більше 10 млн. одиниць персональної і оргтехніки загальною масою понад 400 тис. т і ще порядку 20 млн мобільних телефонів (близько 2400 т). Причому в сучасній електроніки є своя специфіка – вона в набагато більшій мірі складається з неліквідних матеріалів. Так, один комп'ютер класу 286 або 386 в комплекті з ЕПТ-монітором орієнтування містить від 10 до 20 кг скла, 3 кг АВС-пластика, приблизно стільки ж чорних металів, по 200 г міді і алюмінію, всього 1 г срібла і не більше 10 міліграма золота. Тобто в основному йдеться про матеріали, вторинне використання яких неможливе, і тому вартість переробки значно перевищує вартість отримуваних металів.

Окрему проблему утилізації представляють кінескопи моніторів – із-за вмісту отруйних речовин їх не можна навіть розібрати – як і ядерні відходи, їх слід лише ховати в спеціальних могильниках. Розвинені країни задихаються від електронного сміття, оскільки одних лише неробочих кінескопів і моніторів в них скупчилося більше 100 млн. Те ж саме відноситься і до батарей живлення і акумуляторів, що містять такі метали, як свинець, кадмій, цинк і нікель.

У Японії, США і країнах ЄС останніми роками активно розвивається напрям утилізації старих комп'ютерів. У США компанія Dell почала переробку застарілої техніки восени 2002 р. У Німеччині щорік викидається 2,2 млн

комп'ютерів, принтерів і моніторів. Середньостатистичний німець повністю або частково оновлює свій ПК кожні 2–3 роки і вимушений платити за утилізацію старого (залежно від моделі) від 15 до 30 євро.

В наш час німецький концерн Siemens і японська компанія Fujitsu мають намір створити спільне підприємство по утилізації персональних комп'ютерів – вони планують побудувати заводи в п'яти містах Німеччини. Є в намірах також створення аналогічних виробництв у Великобританії, Франції і Скандинавських країнах. На думку ініціаторів проекту, централізована переробка ПК поліпшить екологічну обстановку і сприятиме збільшенню попиту на нові моделі.

У Японії Sony організувала службу по утилізації застарілих персональних комп'ютерів своєї марки. Компанія створила спеціальну мережу по їх збору і доставці, а вартість переробки одного ПК складає 4–5 тис. ієн (\$40).

У нашій державі, на відміну від індустріально розвинених країн, проблема переробки електронного сміття практично пущена на самоплив – утилізація застарілої техніки є турботою виключно її власників, тому найчастіше устаткування закінчує свої дні на звалищі.

Згідно із законом для списання і утилізації ПК і офісного устаткування юридична особа повинна звернутися до одного із спеціалізованих підприємств, які займаються виробництвом, ремонтом і обслуговуванням персональної техніки, з проханням про проведення експертизи, і отримати висновок про те, що дана модель морально застаріла, знята з виробництва і ремонту не підлягає. Лише після цього можна укласти договір з відповідною організацією про утилізацію відходів.

Ліцензію на утилізацію відходів, що містять дорогоцінні метали, видає Міністерство фінансів, кольорові і чорні – Міністерство промислової політики, а полімери і отруйні матеріали – Міністерство екології і природних ресурсів. Але, як ми вже з'ясували, персональні комп'ютери містять всі ці речовини. Тому в їх відношенні діє такий порядок: устаткування необхідно здати підприємству, що має дозвіл на роботу з дорогоцінними металами. Там здійснюються розбирання техніки і сортування матеріалів, які потім передаються компаніям, на законних підставах що займається переробкою певного вигляду відходів.

Утилізація застарілої офісної техніки вимагає грошей, проте такі витрати неминучі. У силах же законодавчих органів зробити цей процес по можливості простим і ефективним. При розумній організації переробка "електронного сміття" може стати економічно вигідною діяльністю і сприяти створенню додаткових робочих місць.

ВИСНОВКИ

Ціль даного дипломного проекту полягала у освітленні й рішенні практичних проблем побудови локальної обчислювальної мережі підприємства ТОВ «Терновський хлібзавод».

У будинку вимагають прокладки кабелю системи, такі як комп'ютерна мережа, система відео спостереження. Для раціональної їхньої реалізації необхідне єдине середовище передачі даних, якою буде структурована кабельна система.

В Україні на сьогоднішній день, на жаль, немає національного стандарту, що визначає розробку комп'ютерної мережі, тому була опора на міжнародні стандарти (ANSI/TIA/ EIA-568-A та ISO/IEC11801).

Розроблена ЛОМ відповідає прийнятим міжнародним стандартам і забезпечує передачу всіх видів інформації (дані, голос, відео й т.п.) з урахуванням перспектив розвитку сучасних інформаційних технологій. Крім того, дана ЛОМ забезпечує інтеграцію й працездатність всіх елементів та систем.

В ході проектування було розглянуто кілька варіантів архітектури, та обраний варіант як оптимальний за вартістю, так і найбільш зручний з погляду подальшого адміністрування.

В проекті реалізована традиційна топологія зірки на основі неекранованих 4-х парних кабелів UTP категорії 5е, крім того, використовується архітектура однокрапкового керування, тобто все комутаційне обладнання перебуває в одному місці - у приміщенні серверної. Відстань від серверної до будь-якого робочого місця не перевищує максимально можливу довжину кабелю, дозволена стандартом для даного рівня ієрархії.

Як корпоративний стандарт операційної системи для серверів була обрана ОС Windows 2003 Server SP2 корпорації Microsoft. Ця версія

підтримує роботу з більшим обсягом оперативної пам'яті й більшою кількістю процесорів. Вона містить у собі засоби організації кластерів та механізми розподілу навантаження.

У проекті надані необхідні розрахунки й креслення, специфікація встаткування й матеріалів, необхідних для побудови ЛОМ та відео спостереження. Дано рекомендації з адміністрування й. Крім того, у рамках проекту розглянута реалізація системи резервного копіювання й методів забезпечення інформаційної безпеки. Виконано економічний розрахунок локальної мережі ТОВ «Терновський хлібзавод».

Як додаткові розділи в дипломному проекті присутні глави, присвячені безпеці та охороні праці.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Косенко, І. О. Основи відеонагляду: навчальний посібник. — Київ: Академвидав, 2018. — 320 с.
2. Шевчук, В. І. Технології відеонагляду: принципи, пристрої, застосування. — Львів: Вища школа, 2020. — 240 с.
3. Дмитрієв, Ю. В. Відеонагляд та системи безпеки: основи та сучасні технології. — Харків: ХНУ, 2019. — 250 с.
4. Горєв, С. М. Системи відеонагляду в охоронних технологіях. — Одеса: Одеський університет, 2017. — 180 с.
5. Федоров, В. І., & Шевченко, В. М. (2007). Основи широкосмугових технологій передачі даних. Київ: Наукова думка.
6. Кравченко, В. О. (2011). Технології та методи цифрової передачі інформації в телекомунікаціях. Харків: ХНУРЕ.
9. Косов, С. П. (2005). Цифрові технології в телекомунікаціях: DSL, ADSL, та інші рішення. Київ: НТУУ "КПІ".
10. Шинкаренко, О. В. Локальні мережі: підручник для вищих навчальних закладів. — Київ: Кондор, 2020. — 312 с.
11. Дем'яненко, О. І. Основи побудови локальних мереж: навчальний посібник. — Харків: Фоліо, 2019. — 265 с.
12. Миколайчук, Ю. В. Основи проектування локальних мереж. — Львів: Наукова думка, 2021. — 348 с.
13. Петренко, В. М., Мельник, С. О. Сучасні тенденції розвитку локальних мереж в умовах технологій 5G. // Технічні науки. — 2023. — Т. 29, № 2. — С. 45-55.
7. Hecht, H. (2006). Broadband: History, Technology, and Applications. Wiley.
Книга дає огляд розвитку широкосмугових технологій, таких як ADSL, їх основні переваги, обмеження та перспективи.
8. Gulati, V. (2003). DSL and ADSL Technologies. New York: McGraw-Hill.
14. Sommerville, I. Software Engineering. — 10th ed. — Boston: Addison-Wesley, 2015. — 1005 p. (Розділ "Системи локальних мереж та архітектура").

15. Tanenbaum, A. S., Wetherall, D. J. Computer Networks. — 5th ed. — Upper Saddle River: Pearson, 2011. — 600 p.

Конфігурація сервера доступу до Internet на базі FreeBSD 8.1

etc/rc.conf - Файл основних налаштувань

```
gateway_enable="YES"          # Дозволяє сервера бути шлюзом
pf_enable="YES"               # Запуск pf
pflog_enable="YES"            # Можливість писати логи pf
pf_rules="/etc/pf.conf"       # Шлях до правил pf
pf_program="/sbin/pfctl"      # Шлях до програми управління pf
pf_flags=""                   # Необхідно для pfctl
defaultrouter="xx.xx.xx.xx"   # Шлюз провайдера
named_enable="YES"            # Запуск DNS
ifconfig_r10="inet 192.168.1.1 netmask 255.255.252.0" # Внутрішній
інтерфейс
ifconfig_r11="inet xx.xx.xx.xx netmask 255.255.252.0" # Зовнішній
інтерфейс
```

/etc/pf.conf - Конфігурація Packet Filter , брандмауер

```
ext_if="r11"                  # Зовнішній інтерфейс (дивиться до провайдера WAN)
int_if="r10"                  # Внутрішній інтерфейс (дивиться в нашу мережу LAN)
```

```
table <pf-allow-pc> file "/etc/pf-allow-pc"
set skip on lo0              # пропускаємо перевірку на петлі
scrub in all                 # збираємо всі частини пакета перед відправкою
nat on $ext_if from <pf-allow-pc> to any -> ($ext_if) # список ПК яким
потрібен Internet
block all                   # заборонимо всі звідусіль
pass in on $int_if from any to any # дозволити все з локальної мережі
pass out on $ext_if from $ext_if to any # дозволити серверу доступ в
Internet
pass in on $ext_if proto tcp from any to $ext_if port ssh # дозволяємо
SSH
pass in inet proto icmp all icmp-type echoreq # дозволяємо ping
```

/etc/pf-allow-pc - Список ПК яким потрібен Internet

```
192.168.1.5
```

```
192.168.1.6
192.168.1.10
192.168.1.yy
```

/etc/namedb/named.conf

```
listen-on { 127.0.0.1; 192.168.1.1; };
forwarders { 127.0.0.1; 192.168.1.1; };
```

/etc/dhcpd.conf - Конфігурація DHCP сервера

```
option domain-name "example.com";
option domain-name-servers 192.168.1.1;
option subnet-mask 255.255.255.0;
```

```
default-lease-time 3600;
max-lease-time 86400;
ddns-update-style none;
```

```
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.5 192.168.1.254;
    option routers 192.168.1.1;
}
```

```
host Director { # Визначення того, що хосту завжди буде видаватися один і той же IP-адрес
    hardware ethernet 02:03:04:05:06:07;
    fixed-address 192.168.1.10;
}
```

```
host name {
    hardware ethernet 01:02:03:04:05:06;
    fixed-address 192.168.1.YY;
}
```