Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет прикладних інформаційних технологій та електроінженерії
(повна назва факультету)
Кафедра приладів та контрольно-вимірювальних систем
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістра
(назва освітнього ступеня)

на тему: Інформаційне забезпечення комп'ютерної мережі ТОВ «TV-4»

Виконав: студент 6 курсу, групи РНм-61
спеціальності 153 Мікро- та наносистемна техніка
(шифр і назва спеціальності)

(підпис) Лизун В. І.
(прізвище та ініціали)

Керівник (підпис) Пастернак Ю. В.
(прізвище та ініціали)

Нормоконтроль (підпис) Апостол Ю. О.
(прізвище та ініціали)

Завідувач кафедри (підпис) Паламар М. І.
(прізвище та ініціали)

Рецензент (підпис) Дедів Л. Є.
(прізвище та ініціали)

Тернопіль 2020

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет Факультет прикладних інформаційних технологій та електроінженерії
(повна назва факультету)

Кафедра Кафедра приладів та контрольно-вимірювальних систем
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри

(підпис) (прізвище та ініціали)

« » 20___ р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня магістр
(назва освітнього ступеня)

за спеціальністю 153 Мікро- та наносистемна техніка
(шифр і назва спеціальності)

студенту Лизуну Валерію Ігоровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Інформаційне забезпечення комп'ютерної мережі ТОВ «TV-4»

Керівник роботи Пастернак Юрій Володимирович
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «___» _____ 2020_ року № _____

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи

4. Зміст роботи (перелік питань, які потрібно розробити)
1 Аналітична частина. 2 Основна частина. 3 Науково-дослідна частина. 4 Спеціальна частина.
5 Охорона праці та безпека в надзвичайних ситуаціях.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. План приміщень 2 поверх. 2. План приміщень 3 поверх. 3. Фізична топологія 2 поверх.
4. Фізична топологія 3 поверх. 5 Таблиця IP адрес. 6. Логічна топологія.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Затвердження теми кваліфікаційної роботи		
2	Аналіз літературних джерел		
3	Обґрунтування актуальності дослідження		
4	Аналіз предмету дослідження та предметної області		
5	Проведення дослідження методів та засобів аналітичного опрацювання даних		
6	Оформлення розділу «Аналітична частина»		
7	Оформлення розділу «Основна частина»		
8	Оформлення розділу «Науково-дослідна частина»		
9	Оформлення розділу «Спеціальна частина»		
10	Оформлення розділу «Охорона праці та безпека в надзвичайних ситуаціях»		
11	Нормоконтроль		
12	Попередній захист роботи		
13	Захист кваліфікаційної роботи		

Студент _____ _____
(підпис) (прізвище та ініціали)

Керівник роботи _____ _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Розробка інформаційного забезпечення комп'ютерної мережі ТОВ «TV-4». // Магістерська атестаційна робота // Лизун Валерій Ігорович // Тернопільський національний технічний університет, група РНм - 61// Тернопіль, 2020 // с. – 97 , рис. – 36, таблиці – 10, кресл. – 6 .

Ключові слова: ЛОКАЛЬНА КОМП'ЮТЕРНА МЕРЕЖА, ДОСТУП ДО ІНТЕРНЕТ, CISCO.

Тема кваліфікаційної роботи розробка інформаційного забезпечення комп'ютерної мережі ТОВ «TV-4». Мета роботи в розробці проекту створення надійної і високошвидкісної мережі для обміну великими обсягами інформації.

Дипломний проект містить пояснювальну записку, додатки і графічну частину.

Пояснювальна записка складається з п'яти розділів.

В першому розділі описано і проаналізовано завдання, виконано постановку задачі та наведено характеристики приватного підприємства.

В другому розділі дається загальний опис задачі та її специфічні особливості. Здійснюється розробка схем фізичного розташування кабелів та вузлів. Також тут здійснено обґрунтування вибору операційних систем, програмного забезпечення та обладнання для мережі.

В третьому розділі міститься модель мережі, інструкції з інсталяції та налаштування відповідного обладнання.

В четвертому розділі проведено математичне моделювання середнього часу функціонування системи без збоїв на основі журналу спостережень даної мережі.

В п'ятому розділі описані питання охорони праці та техніки безпеки при роботі з обчислювальним обладнанням.

ANNOTATION

Development of information support for the computer network of TV-4 LLC. // Master's certification work // Lyzun Valeriy Ihorovych // Ternopil National Technical University, group RNm - 61 // Ternopil, 2020 // p. - 97, fig. - 36, tables - 10, chair. - 6.

Keywords: LOCAL COMPUTER NETWORK, INTERNET ACCESS, CISCO.

The topic of the qualification work is the development of information support of the computer network of TV-4 LLC. The purpose of the project is to create a reliable and high-speed network for the exchange of large amounts of information.

The diploma project contains an explanatory note, appendices and a graphic part.

The explanatory note consists of five sections.

In the first section the task is described and analyzed, the problem is set and the characteristics of a private enterprise are given.

The second section gives a general description of the problem and its specific features. Schemes of physical arrangement of cables and knots are developed. The selection of operating systems, software and equipment for the network is also substantiated here.

The third section contains the network model, installation instructions and configuration of the relevant equipment.

In the fourth section the mathematical modeling of the average time of system operation without failures on the basis of the log of observations of this network is carried out.

The fifth section describes health and safety issues when working with computer equipment.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

VLAN (англ. Virtual Local Area Network — віртуальна локальна комп'ютерна мережа).

NAT - (від англ. Network Address Translation — перетворення (трансляція) мережних адрес) — це механізм зміни мережної адреси в заголовках IP датаграм, поки вони проходять через маршрутизуючий пристрій з метою відображення одного адресного простору в інший.

FDDI – Fiber Distributed Data Interface (укр. розподілений волоконний інтерфейс даних) — специфікація, що описує високошвидкісні мережі з методом доступу із передачею маркера на основі оптоволокна.

FTP - Протокол передачі файлів (англ. File Transfer Protocol, FTP) — дає можливість абоненту обмінюватися двійковими і текстовими файлами з будь-яким комп'ютером мережі, що підтримує протокол FTP.

VPN скор. від (англ. Virtual Private Network — віртуальна приватна мережа) — загальна назва віртуальних приватних мереж, що створюються поверх інших мереж, які мають менший рівень довіри.

ATM - (англ. Asynchronous Transfer Mode - асинхронний спосіб передачі даних) – мережева високопродуктивна технологія комутації та мультиплексування, заснована на передачі даних у вигляді комірок (cell) фіксованого розміру (53 байти), з яких 5 байтів використовується під заголовок.

ВСТУП

Персональний комп’ютер став невід’ємною частиною будь-якого роду людської діяльності. Проте інформацію, яка міститься на одному комп’ютері, досить важко, особливо при великих об’ємах інформації, перенести з одного на другий для майбутньої обробки. Також коли на кожному пристрої є свої версії документів, важко організувати спільну роботу над ними та синхронізацію. Складно знайти сферу діяльності людини, яка б не використовувала комп’ютери. Вони використовуються практично у всіх галузях, таких як: науково-дослідницька, проектно-конструкторська, виробнича, торгівельна, фінансова, освітня та в адміністративних установах; міжнародні корпорації та малий бізнес усі вони потребують надійної та ефективної роботи комп’ютерних мереж.

Комп’ютерні мережі відкрили зовсім нові і значно ширші можливості використання ПК. Тепер ПК – це не тільки засоби для обробки інформації, це – також засоби для отримання та обміну інформацією.

Метою даної дипломної роботи було розробити проект інформаційного забезпечення комп’ютерної мережі ТОВ «TV-4».

Об’єднання персональних комп'ютерів в єдину мережу у вигляді внутрішньої інформаційної системи мережі отримуються такі переваги, як:

– розподіл ресурсів дозволяє керувати периферійними пристроями, такими як принтери чи сканери, з усіх підключених до мережі робочих станцій.

– розподіл даних дозволяє отримати спільний доступ до інформації з будь яких робочих станцій.

– розподіл програмних засобів дозволяє використовувати програмне забезпечення яке не встановлено безпосередньо на робочі станції а є спільним ресурсом мережі.

1. АНАЛІТИЧНА ЧАСТИНА

1.1 Призначення розробки

У даному дипломному проекті буде розроблено інформаційне забезпечення комп'ютерної мережі ТОВ «TV-4». У мережі буде задіяно 1 сервер для зберігання даних і сервер для інших цілей. Також мережу розподілено на кілька сегментів, які мають різні рівні доступу.

Оскільки прогрес не стоїть на місці, то при розробці мережі враховується можливість модернізації. Для цього вибиралось обладнання, яке підлягає удосконаленню (оновленню), а саме комутатори на 24 порти та 16 портів, у яких залишаються вільними по кілька портів (3-5), сервер з можливістю використання новішого програмного забезпечення і доданням потужніших комплектуючих.

Також ПК з можливістю додавання потужнішого обладнання і встановленням новішого ПЗ.

До мережі потрібно підключити такі відділи:

- відділ по роботі з клієнтами;
- відділ маркетингу (аналітичний відділ);
- креативний відділ;
- виробничий відділ;
- відділ медіапланування;
- pr-відділ;
- відділ btl-акцій;
- юридичний відділ;
- бухгалтерія;
- апаратна;
- гостьова кімната;
- кімната відпочинку.

1.2 Аналіз вимог до апаратного та програмного забезпечення

В якості фізичного середовища передачі даних повинні бути використані кабельні з’єднання.

При необхідності використати екрановану виту пари в разі наявності в мережі великих завад з зовнішньої сторони. Відповідно, оскільки зростає ціна, необхідне обґрунтування використання такого виду кабелю.

Використовуваний комутатор повинен відповідати таким експлуатаційним ознакам:

– наявність світлодіодних індикаторів, що вказують на стан портів (Port Status), наявність колізій (Collisions), активність передачі даних (Activity), наявність несправності (Fault) і наявність живлення (Power), утилізацію портів (Utilization), що забезпечує відображення стану та етапи, в яких перебуває комутатор в даний момент роботи, статус використання портів;

– можливість бути змонтованими і введеним в дію на протязі декількох хвилин;

– мати стандартний розмір по ширині – 19U;

– бути прозорим для програмних засобів мережевої операційної системи;

– підтримувати стандарт IEEE 802.1d – Spanning Tree Protocol;

Мережева операційна система надає можливість користувачам спільно користуватися такими ресурсами:

– дорогими апаратними ресурсами мережі – потужні принтери(heavy duty), сканери, файлові сервери, а також іншим мережевим обладнання;

– інформаційними ресурсами і базами даних;

– забезпечити спільну роботу великої кількості користувачів з високою пропускною здатністю.

Вимоги до апаратного забезпечення для локальних мереж: потрібен Web-сервер, робочі станції клієнтів, Ethernet-карти і кабелі.

Потужний сервер повинен мати високопродуктивний процесор з достатнім запасом потужності для роботи віртуальної машини веб-сайту та інших необхідних засобів, наприклад популярний intel i7 8700, який працює на частоті до 5,1 ГГц, 16 ГБ ОЗУ та жорсткий диск об’ємом не менше 10 ТБ. Для роботи з сервером не тільки по мережі, але й безпосередньо з консолі, потрібно до переліченого додати відеокарту PCI з 512 Мбайт VRAM чи більше, яка забезпечує середню роздільну здатність.

Комп’ютери клієнтів мають бути обладнані відео-адаптерами середньої і високої потужності, оскільки на ПК багато роботи проводиться саме з відео та фотоматеріалами. Для цього необхідний центральний процесор, що працює на частоті більше 2,2 ГГц. Крім того, на продуктивність комп’ютера відчутно впливає об’єм оперативної пам’яті, кожний комп’ютер повинен мати ОЗУ з об’ємом пам’яті не менше 8 Гбайт в 2 канальному режимі, а на комп’ютерах які будуть використовуватися безпосередньо для роботи з графікою відео та фото матеріалами об’єм оперативної пам’яті повинен бути не менше 16 Гбайт. Для швидкої роботи в якості пристрою запам’ятовування необхідно використати ssd накопичувачі так як вони, порівняно з hdd, мають значно більшу швидкість запису і зчитування інформації, що значно прискорює роботу операційної системи та програм. На робочі станції можна встановлювати відео-карти з 4 ГБ VRAM, із високою продуктивністю.

Також важливим є вибір мережевого адаптера. Оскільки планується створення швидкісної мережі, то доцільно обрати мережевий адаптер стандарту не нижче Gigabit Ethernet. Для економії коштів можна обирати інтегрований мережевий адаптер, але обов’язково враховувати слот для ще одного адаптера, оскільки, якщо виникне потреба замінити його то у інтегрованому варіанті це буде неможливо.

1.3 Вимоги до документації

Потрібно вказати вимоги до документування мережі, на основі єдиних стандартів. Також потрібно розробити (адаптувати) стандартний бланк(и) для документування мережі.

Під час проектування ЛОМ, повинно бути створено наступну документацію:

– інженерний журнал;
– логічна топологія;
– описи виходів і трас кабелю;
– характеристики пристроїв.

Після цього, можна приступити до монтажу системи.

1.4 Стадії та етапи розробки

При організації мережі, всі роботи можна поділити на 4 етапи:

1. Збір інформації.
2. Створення і затвердження проекту.
3. Фізична реалізація мережі.
4. Експлуатація та моніторинг мережі.

При зборі інформації, необхідно визначитись у наступних питаннях:

– який тип організації і чи планується її зростання;
– побажання керівництва;
– яке програмне забезпечення буде використовуватись в мережі;
– визначити тип мережі, топологію, провідники та інше обладнання;
– визначити необхідність повторювачів, концентраторів для робочих груп;
– визначити кількість і потребу магістралей;
– кількість і потреба в головному та проміжних комутаційних вузлах;

– визначити необхідність встановлення мостів, комутаторів або заміни іншого обладнання на них;
– визначити необхідність встановлення маршрутизаторів;
– тип підключення до глобальної мережі;
– необхідний захист і процедури керування.

1.5 Порядок контролю та прийому

При прийомі мережі необхідно виконати перевірку функціонування усіх існуючих мережевих вузлів . Наявність відповідного маркування на кабелях та їх відповідність таблицям. Перевірка функціонування мережі виконується за допомогою утиліт ping та tracert, або пакетів, здатних замінити дані утиліти.

1.6 Постановка задачі на розробку проекту. Характеристика підприємства, для якого створюється проект мережі

Завданням проектування є розробка інформаційного забезпечення комп'ютерної мережі ТОВ «TV-4». Підприємство складається з таких відділів:
– PR-відділ;
– апаратна;
– бухгалтерія;
– виробничий відділ;
– відділ BTL-акцій;
– відділ маркетингу (аналітичний відділ);
– відділ по роботі з клієнтами;
– гостьова кімната;
– кімната відпочинку;
– креативний відділ;
– серверна;

- директор;
- технічний відділ;
- юридичний відділ.

Для роботи підприємства необхідна надійна мережа з високою пропускною здатністю тому, що підприємство займається виробництвом відео-роликів, сюжетів і телевізійних програм. Також в підприємства має бути власний сайт, тому потрібний сервер для web-сайту, окрім цього потрібен і сервер для зберігання відеоматеріалів, фото документів та інших необхідних файлів для роботи. Так як відео-файли за об’ємом є достатньо великі і можливий варіант коли одразу 2 або більше користувачів мережі будуть завантажувати на комп’ютер чи відправляти на сервер файли великого об’єму, тому швидкість зв’язку між комутатором і комп’ютером має бути не менше 1 Gb\s, а зв’язок між маршрутизатором і комутатором виробничих відділів 10 Gb\s.

2 ОСНОВНА ЧАСТИНА

2.1 Опис та обґрунтування логічного типу мережі

Топологія комп’ютерної мережі відображає структуру зв’язків між її основними функціональними елементами. В залежності від компонентів, що розглядаються, розрізняють фізичну і логічну структури локальних мереж. Фізична структура визначає топологію фізичних з’єднань між комп’ютерами. Логічна структура визначає логічну організацію взаємодії комп’ютерів між елементами мережі. Доповнюючи одна одну, фізична та логічна топології дають найбільш детальне уявлення про структуру комп’ютерної мережі.

Для локальної мережі було обрано логічну топологію розширена зірка тому, що це найбільш надійна і продуктивна топологія із всіх існуючих на сьогоднішній день.

Переваги топології розширена зірка:

– весь мережевий трафік локальної мережі проходить через центральний маршрутизатор. Використовуючи технологію Port Mirorring є можливість застосовувати мережевий аналізатор для виявлення та усунення проблем в роботі локальної мережі та мережевих додатків;

– комутатор може відігравати роль інтелектуального фільтра інформації, що поступає в мережу з різних станцій в мережу, і при необхідності створювати правила навіть для різних протоколів передачі даних, встановлювати обмеження швидкості і блокувати небажані ресурси;

– використовуючи засоби ОС центрального маршрутизатора можна проводити моніторинг кількості пакетів, що передаються через нього, а також проводити моніторинг завантаженості сегментів мереж;

– до мережі легко підключити новий комп’ютер, комутатор, принт-сервер чи WiFi-роутер;

– пошкодження кабелю призведе до проблем з мережею тільки у того комп’ютера, до якого цей кабель приєднаний.

На рисунку 2.1 наведено фізичну топологію «Зірка».

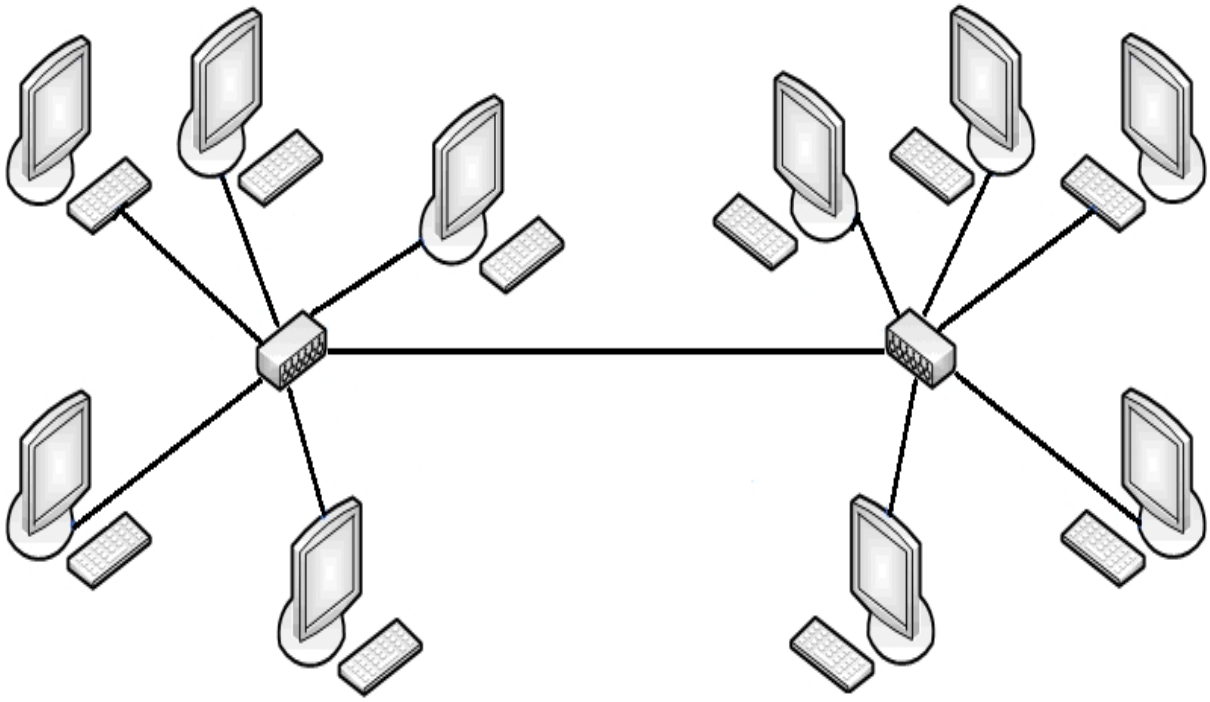

Рисунок 2.1 - Фізична топологія «Розширена зірка»

Слабким місцем обраної топології є центральний маршрутизатор, при виході з ладу якого вся мережа перестає функціонувати. Даний недолік не є суттєвим, або ймовірність його виникнення є невеликою, оскільки гарантовано, що він буде працювати на відмову приблизно 80000 годин.

В результаті аналізу завдання та плану розташування ПК в мережі розроблено логічну топологію яка представлена на листі КРМ 000.00.00 ПЗ 6. Розроблена топологія мережі є гібридною, оскільки включає в себе маршрутизатор, точку доступу, сервер та комутатори.

IP адресація в мережі клас С. Вона представлена на листі КРМ 000.00.00 ПЗ 5. Існуюча мереже буде сегментована за допомогою VLAN стандарту IEEE 802.1Q.

Логічна адресація в ЛОМ та таблиця конфігурування VLAN представлені в таблиці 2.1 та таблиці 2.2.

Таблиця 2.1 – Логічна адресація в ЛОМ

Діапазон позначення вузлів	Робоча група/Кіль-кість вузлів		Назва кабінету та його номер**		Номер VLAN	Адреса підмережі/ Маска
1	2	3	4	5	6	7
WS_1	workgroup1	1	Юрист	-	21	192.168.1.0/24
WS_2 – WS_7	workgroup2	6	Креативний відділ	-	22	192.168.122.0/24
WS_8 – WS_10	workgroup3	3	Директор, Замісник директора, бухгалтер		27	192.168.27.0/24
WS_11 – WS_13	workgroup4	3	Апаратна		210	192.168.210.0/24
WS_14- WS_16	workgroup5	3	Відділ маркетингу		211	192.168.211.0/24
WS_17	workgroup6	1	Тех. відділ	-	214	192.168.214.0/24
WS_18– WS_19	workgroup7	2	PR - Відділ		315	192.168.115.0/24
WS_20– WS_23	workgroup8	4	відділ BTL-акцій		317	192.168.117.0/24
WS_24– WS_27 WS_30– WS_32	workgroup9	7	виробничий відділ		320	192.168.120.0/24

Продовження таблиці 2.1

1	2	3	4	5	6	7
WS_28– WS_29 AP_2	workgroup1 0	2	Гостьова кімната, кімната відпочинку		324	192.168.124.0/24
WS_33	-	1	Серверна			192.168.22.0/24
S_1	-					192.168.4.0/24
S_2	-					192.168.5.0/24

Таблиця 2.2 - Таблиця конфігурування VLAN

№ п/п	Позначення вузла	Назва мережевого пристрою	Номер порту**	Тип порту*	Номер VLAN
1	2	3	4	5	6
1	WS_1	SW_1	1	Untagged	21
2	WS_2– WS_7	SW_1	2-7	Untagged	22
3	WS_8 – WS_10	SW_1	8-10	Untagged	27
4	WS_11 – WS_13	SW_2	1-3	Untagged	210
5	AP_1	SW_2	4	Untagged	202
6	WS_14 –WS_16	SW_2	5-7	Untagged	211
7	WS_17	SW_2	8	Untagged	214
8	WS_18 - WS_19	SW_3	1-2	Untagged	315
9	WS_20– WS_23	SW_3	3-6	Untagged	317
10	WS_24– WS_27 WS_30– WS_32	SW_3	7-10 13-15	Untagged	320
11	WS_28– WS_29 AP_2	SW_3	11-13	Untagged	324
12	SW_1	R_1	3	Tagged	-
13	SW_2	R_1	4	Tagged	-

Продовження таблиці 2.2

1	2	3	4	5	6
14	SW_3	R_1	1	Tagged	-
15	R_1	WS_33	5	Tagged	-
16	R_1	S_1	6	Tagged	-
17	R_1	S_2	2	Tagged	-

2.2 Розробка схеми фізичного розташування кабелів та вузлів

2.2.1 Типи кабельних з'єднань та їх прокладка

Використовуватися буде кабель типу «вита пара» і оптичне волокно в деяких випадках, максимальна відстань між комп'ютером і мережевими пристроями не повинна бути більша ніж 100 метрів. Під'єднання до кабелю здійснюється через стандартний роз'єм типу RJ-45.

Основними перевагами кабелів «вита пара» є висока швидкодія, простота прокладання і низька вартість. Недолік неекрановані кабелі «витої пари» є вразливі до зовнішніх електромагнітних полів, що вирішується використанням екранованих кабелів.

Оптичне волокно – найбільш ефективне середовище передачі сигналів, що забезпечує швидкість десятків Гбіт/с. Сигнали передаються використовуючи оптичне волокно (світловід), яке являє собою тонку скляну (або пластикову) нитку, що поміщена в гнучку оболонку. Сигнал генерується світлодіодом або лазером і по оптоволоконному кабелю передається за допомогою світлових променів, приймається сигнал з допомогою світлочутливих елементів і конвертується в електричний сигнал.

Оптичне волокно в порівнянні з попередниками має суттєві переваги такі як: стійкість до електромагнітного і радіочастотного випромінювання, захищеність інформації, висока швидкодія. Основний недолік – висока вартість встановлення і обслуговування мережі на базі оптичного волокна.

Отже, враховуючи всі переваги і недоліки наведених типів кабелів в якості

середовища передачі інформації вибрано кабель типу "скручена пара" категорії 6. Він дозволить побудувати мережу з швидкістю передачі інформації 1000 Мбіт/с (Стандарт Gigabit Ethernet).

Згідно стандарту EIA/TIA 568A максимальна відстань в підсистемі робочого місця (між ПК і розеткою) не повинна перевищувати 3м, отже спроектуємо розміщення розеток на плані будівлі з дотриманням цієї вимоги, і помітимо їх на схемі.

Прокладка кабелю може здійснюватися кількома способами: вмонтовані в стіну, прокладання по існуючих системах, встановлення в коробах.

В проектованій мережі сукупність кабелів не надто велика, проте в приміщенні є підвісна стеля, тому виходячи з економічних міркувань вибираємо метод встановлення кабелю – над підвісною стелею.

Розміщення кабелів та комунікаційних розеток наведено на фізичній топології мережі.

2.2.2 Будова вузлів та необхідність їх застосування

Враховуючи те, що приміщення фірми займають 2 поверхи буде використовуватися вертикальна і горизонтальна мережа.

Комутатори потрібно встановити так, щоб забезпечити мінімальні відстані від комутатора до мережевих розеток. Маршрутизатор в серверній кімнаті в серверній стійці за допомогою кріпильних елементів.

Головний комутаційний вузол потрібно розмістити в серверній кімнаті, що забезпечить:

- можливість розмежування фізичного доступу до активного обладнання і серверу;
- забезпечення робочим простором адміністратора мережі;
- створення правильного температурного режиму для роботи обладнання;

– фільтрування повітря, що дозволить працювати довше без зупинки обладнання для технічного обслуговування і очистки від пилу.

В мережі буде створено один головний комутаційний вузол, який розташовано в серверній кімнаті, доступ до якої обмежений, а в середині встановлено кондиціонер, що дозволяє підтримувати потрібну температуру і запобігає перегріву обладнання.

В приміщенні серверної також розміщуємо блок безперебійного живлення, який забезпечить роботу обладнання до 3 годин потужністю 5 кВт. В серверній буде встановлено головний комутаційний вузол маршрутизатор R_1 і 2 сервера. В якості проміжних комутаційних вузлів будуть встановленні комутатори 2 рівня. Комутатор SW_1 знаходиться на другому поверсі в кабінеті №5, SW_2 на другому поверсі кабінет №10, комутатор SW_3 буде знаходитися на третьому поверсі в кабінеті №19.

2.3 Обґрунтування вибору обладнання для мережі (пасивного та активного)

В результаті аналізу логічної та фізичної топології необхідно виконати вибір наступного обладнання, яке представлено в таблиці 2.3.

Таблиця 2.3 - Потреби в обладнанні для мережі

№ п.п.	Назва	Кількість, шт
1	Комутатори 24 портові	3
3	Сервери	2
4	Маршрутизатори	1
5	Точки доступу	2

Характеристика активного та пасивного комунікаційного обладнання локальної комп’ютерної мережі.

Для локальної мережі буде використано таке пасивне та активне мережеве обладнання:

- мережевий кабель;
- екранована вита пара;
- оптичний кабель;
- мережеві розетки;
- комутаційні шафи;
- комутатори другого рівня моделі OSI;
- маршрутизатори;
- сервер для роботи віртуальної машини;
- сервер зберігання даних;
- точки доступу WiFi;

В якості сервера на якому буде встановлено віртуальну машину для Active Directory Domain Services, веб-сайту, програми «фабрики новин», сервера для прийому відео-сигналу було обрано ARTLINE Business R27 v10 (див. рис 2.3) тому, що він найкраще підходить для завдань які будуть виконуватись, також за необхідності є можливість покращити характеристики сервера. Для порівняння вибираєм 3 сервера Сервер Dell poweredge, T440 ARTLINE, Business R27 v10, Lenovo thinkserver RD450 порівняльні характеристики представленні в таблиці 2.4.

Рисунок 2.3 - Сервер ARTLINE Business R27 v10 (R27v10)

Таблиця 2.4 - Порівняльна характеристика серверів

№ п.п.	Характеристики обладнання	Модель вибраного пристрою (Сервер ARTLINE Business R27 v10	Аналог Сервер Dell PowerEdge T440	Аналог Сервер Lenovo ThinkServer RD450
1	2	3	4	5
1	Процесор	Восьмиядерний Intel Xeon Silver 4110 3.0 ГГц	Восьмиядерний Intel Xeon Silver 4110 3.0 ГГц	Восьмиядерний Intel Xeon E5-2620 3.0 ГГц
2	Оперативна пам'ять	Kingston DDR4-2400 PC4-19200	Kingston DDR4-2400 PC4-19200	RDIMM 16 ГБ
3	Обсяг оперативної пам'яті	32 Гб	16 Гб	16 ГБ
4	Контролер HDD	RAID 0, 1, 5, 10 для SATA 3 (6 портів)	RAID 0, 1, 5, 10	RAID 0/1/5/10/50
5	Жорсткий диск	2 x Seagate ST100-0NM0033 4 ТБ, 128 МБ, 7200 об/хв, Serial ATA 6 Гбіт/с	Hitachi (HGST) Ultrastar 7K2 1TB 7200rpm 128MB SATA III	Можливість встановлення HDD SAS/SATA 3.5"
7	Мережений адаптер	2 x Gigabit Ethernet media over LAN і KVM-over-LAN і 10GBe SFP+.	2 мережеві адаптери LOM, 1GbE	HP NC362i Integrated Dual Port Gigabit Server Adapter
8	Форм-фактор	3U Rackmount	Tower	3U Rackmount
9	Вартість	47520 грн.	61 793 грн.	68 995 грн

В якості маршрутизатора буде обрано Cisco ASR1001-X (див. рис 2.4) тому, що він має потрібні нам порти і є можливість доставити до 2-ох додаткових модулів, які збільшать кількість оптичних портів, та значно збільшать пропускну здатність. Порівняльні характеристики Cisco ASR1001-X і Mikrotik Cloud Core Router CCR1036-8G-2S+ представлені в таблиці 2.5.

Таблиця 2.5 - Порівняльний аналіз технічних характеристик маршрутизаторів Cisco ASR1001-X та Mikrotik CCR1036-8G-2S+EM.

№ п.п.	Характеристики обладнання	Cisco ASR1001-X	Mikrotik Cloud Core Router CCR1036-8G-2S+
1	2	3	4
1	Процесор	Quad-core 2.00GHz	Tilera Tile-Gx36 CPU 1.2 ГГц
2	Інтерфейси	1 слот x NIM + 1 слот x SPA 6 x SFP 1 Gb 2 x SFP + 10 Gb 2 x USB 2.0	1x10/100/100 Ethernet 8xSFP+ 10GE 2xMicroSD 1xUSB 2.0
3	Брандмауер (Firewall):	+	+
4	NAT	+	+
5	Веб-інтерфейс	+	+
6	Telnet	+	-
7	Підтримка SNMP	+	+
8	Полоса пропускання	20 Gbit / s	20 Gbit / s
9	Вартість	272 329 грн	76218 грн

Рисунок 2.4 – Маршрутизатор локальної мережі Cisco ASR1001-X

Для з’єднання маршрутизаторів Cisco 2921-SEC/K9 (див.рис. 2.5) обрано оптичний модуль Cisco SFP-10G-SR, його основні характеристики вказані в таблиці 2.6.

Таблиця 2.6 - Технічні характеристики SFP Cisco GLC-LH-SM

Стандарт	1 х мережі - Ethernet 10GBASE-SR - LC / PC багато-режимний х 2
Відстань передачі даних	300 м
Швидкість передачі даних	10 Gbps
Роз’єм для оптичного кабелю	подвійний LC
вихідна потужність передавача	-9.5 ~ -3 dBm
чутливість приймача м	-22 dBm

Рисунок 2.5 - модуль SFP Cisco GLC-LH-SM

Для локальної мережі буде використано комутатор Cisco Catalyst 2960S-24TS-L (див. рис 2.6) на 24 порти. Вигляд комутатора представлено на рисунку 2.6. Порівняльні характеристики комутаторів представлено в таблиці 2.7.

Таблиця 2.7 – Порівняльна характеристика комутаторів Cisco Catalyst WS-C2960S-24TD-L і Mikrotik CRS328-24P-4S+RM.

№ п.п.	Модель/Параметри	Комутатор Cisco Catalyst WS-C2960S-24TD-L	Mikrotik CRS328-24P-4S+RM
1	2	3	4
1	Кількість портів Fast Ethernet (10/100)	-	-
2	Кількість портів Gigabit Ethernet (10/100/1000)	24	24
3	Додаткові слоти SFP	2 x 10G	4 x 10G
4	Швидкість комутаційної шини	88 Гбіт/с	64 Гбіт/с
5	Підтримка протоколів	VLAN, Spaning Tree, Jumbo packet, QoS	VLAN, Spaning Tree, Jumbo packet, QoS
6	Статична маршрутизація	+	+
7	Моніторинг	RMON, SNMP, PortMirroring	SNMP, PortMirroring, MON
8	Фільтр трафіку	+	+
9	Вартість	45 000 грн	10 971 грн

Рисунок 2.6 – Комутатор Cisco Catalyst WS-C2960S-24TD-L

В проекті передбачено використання 2 точок доступу. Маршрутизатор вибираємо виходячи із порівняльної таблиці 2.8.

Таблиця 2.8 - Порівняльна характеристика точок доступу

N п.п.	Характеристики обладнання	Обрана модель (D-Link DIR-825/AC/G1)	Аналог 1 TP-LINK Archer C2	Аналог 2 Netis WF2681
1	2	3	4	5
1	WAN-порт	Ethernet	Ethernet	Ethernet
2	Безпровідні можливості	802.11b, 802.11g, 802.11n 802.11ac 802.11a	802.11n 802.11g 802.11b 802.11ac 802.11a	802.11n 802.11g 802.11b 802.11ac 802.11a
3	Інтерфейси	1 x WAN 10/100/1000BASE-T, 4 x LAN 10/100/1000BASE-T, 1 x USB 2.0	4 x LAN 10/100/1000 Мбіт/с 1 x WAN 10/100/1000 Мбіт/с	1 x WAN 10/100/1000M 4 x LAN 10/100/1000M
4	Підтримка протоколів	PPTP, L2TP, IPsec, PPPoE,	PPPoE, IPsec, L2TP, PPTP,	PPPoE, IPsec, L2TP, PPTP,
5	Кількість антен	4	2	4
6	Функції безпеки	WEP WPA/WPA2 (Personal/Enterprise) MAC-фільтр WPS (PBC/PIN)	WEP, WPA / WPA2, WPA-PSK / WPA2-PSK	WEP / WPA-PSK / WPA2-PSK Фільтр MAC-адрес безпровідної мережі
9	Вартість	966 грн	900 грн	1 369 грн

В результаті аналізу в якості точки доступу вибрано маршрутизатор D-Link DIR-825/AC/G1 (див. рис 2.7) даний маршрутизатор було вибрано через невелику ціну, достатні для потреб мережі характеристики, високу продуктивність та надійність.

Рисунок 2.7 – Точок доступу D-Link DIR-825/AC/G1

Для зберігання інформації обрано мережеве сховище Qnap TS-832XU-RP-4G (див. рис. 2.8) тому, що на ринку на даний час він є найбільш продуктивним і надійним сервером зберігання даних. Для порівняння обрано сервер Synology RS1219, їх характеристики можна подивитися в таблиці 2.9. Особливістю сервера Qnap TS-832XU є можливість гарячої заміни жорстких дисків, тому при виході з ладу чи необхідності збільшити об’єм пам’яті його не потрібно відключати, що дає змогу не припиняти його роботу в будь-якій ситуації.

Таблиця 2.9 - Порівняльна характеристика точок доступу.

№ п/п	Характеристики обладнання	Обрана модель Qnap TS-832XU-RP-4G	Аналог Synology RS1219+
	2	3	4
1	Процесор	Annapurna Labs Alpine AL-324, 1,7 ГГц, 4 ядра	Intel Atom C2538
2	Пам'ять	4 ГБ DDR4 (можливість розширення до 16 ГБ)	2 ГБ DDR3

Продовження таблиці 2.9

	2	3	4
3	Слоти для дисків	8x2.5" SATA, 3.5" SATA	8x2,5 "/ 3,5" SATA3
4	Керування дисками	Single disk, JBOD, RAID 0, RAID 5, RAID 6, RAID 10	Synology Hybrid RAID, Basic, JBOD, RAID 0, RAID 5, RAID 6, RAID 10
5	Файл-сервер	CIFS / SMB, AFP	CIFS / AFP / NFS / FTP / WebDAV
6	Web-сервер	HTTP / HTTPS	HTTP / HTTPS
7	Автономне завантаження	FTP, HTTP	CalDAV, iSCSI, Telnet, SSH, SNMP, VPN (PPTP, OpenVPN, L2TP)
8	Інші мережі та протоколи	CIFS/SMB, AFP, NFS, FTP, SFTP, TFTP, WebDAV, HTTP, HTTPS, iSCSI, DHCP, Bonjour, Telnet, SSH, SNMP, DDNS	CIFS / AFP / NFS / FTP / WebDAV
9	LAN	2xGigabit Ethernet, 2x10Gigabit SFP+	4 (GbE)
10	Ціна	45000 грн	35230 грн

Рисунок 2.8 сервер Qnap TS-832XU

Підсистема робочого місця. Включає мережеву розетку, яка розміщується біля коробу та патч-корд, яким ПК під’єднується до мережевої розетки. Для забезпечення високої швидкості використовується мережева розетка категорії 6. Зовнішній вигляд мережевої розетки показано на рисунку 2.9.

Рисунок 2.9 - Мережева розетка UTP кат. 6

Горизонтальна підсистема являє собою сегменти кабелів, які з’єднують мережеві розетки певного сегменту з комутатором робочої групи. Кабельні сегменти будуть розміщуватися у коробах, які розміщуватимуться на відстані 70 см від підлогового покриття. Комутатор робочої групи розміщується в настінній комутаційній шафі Pleolan 6U (див.рис.2.9).

Рисунок 2.10 - Шафа настінна Pleolan 6U

Для розміщення серверів та головного маршрутизатора використовується комутаційна стійка, яка розміщується в серверній. На рисунку 2.10 наведено зовнішній вигляд комутаційної стійки.

Рисунок 2.10 Комутаційна стійка 32U 400 Rackmount

До головного комутаційного вузла буде підведено зовнішні магістралі (підключення до мережі Інтернет по локальній мережі).

Кабельна інфраструктура побудована на базі витої пари категорії 6. Кабель симетричний категорії 6 призначений для швидкісної передачі інформації в структурованих кабельних системах.

Кабель категорії 6 широко застосовується в мережах Fast Ethernet і Gigabit Ethernet, складається з восьми попарно скручених провідників і здатний передавати дані на швидкості до 10 Гбіт/с і пропускає сигнали частотою до 200МГц.

В таблиці 2.10 показано обране обладнання для побудови мережі.

Таблиця 2.10 - Зведена таблиця обраного обладнання для мережі

№ п/п	Найменування матеріальних ресурсів	Од. виміру	Факт. витрач. матеріалів	Ціна 1-ці, грн.	Загальна сума витрат, грн.
1	Маршрутизатор	шт.	1	272 329	272 239
2	Оптоволокно Finmark UT016-SM-15 LSZH	м	130	17	2 210
3	Короб 15*10	м	200,8	9,36	1881,36
4	Кабель вита пара 6 категорії	м	750,5	20	15 020
5	Шурупи з дюбелем	шт.	180	0,87	156,6
6	Сервер	шт.	1	47520	47520
	Qnap TS-832XU	шт.	1	45200	45200
7	Комутатор	шт.	3	45563	136689
8	Точка доступу	шт.	2	966	1932
9	Комутаційна стійка 32U	шт.	1	2 931	2931
10	Шафа настінна Pleolan 6U	шт.	3	2 156	6468
11	Мережева розетка UTP кат. 6	шт.	32	65	2080
12	Модуль SFP Cisco GLC-LH-SM	шт.	10	1004	10 040
13	Разом				544367

2.4 Особливості монтажу мережі

Під час розробки системи слід дотримуватися вимог, які встановлені стандартом EIA/TIA-569.

Оскільки будинок багатоповерховий, тому на кожному з поверхів організовано проміжні комутаційні вузли (ПКВ або IDF - Intermediate Distribution Facility) до яких зводиться усе комутаційне обладнання та канали даного поверху.

На всю організацію один головний комутаційний вузол (ГКВ або MDF – Main Distribution Facility) , який знаходиться на другому поверсі. Відстані між ГКВ та ПКВ, а також горизонтальними кабелями не більше 90 – 100 метрів, згідно обраного стандарту.

Розміри головного і проміжного комутаційних вузлів 5,5х5,25м.

Приміщення відповідають технічним стандартам і пожежній безпеці. Температура в середині становить 21 градус по Цельсію. Вологість 30-50 відсотків. Освітлення 500 люкс на висоті 2.6м над номіналом. Електричні розетки подвійні, заземлені кожні 1.8 м.

Забезпечений вільний доступ до кабелів і вузлів. В ПКВ та ГКВ двері шириною 90см і відкриваються на зовні, забезпечується блокування дверей з середини.

Обладнання встановлено від стіни на відстані 50см(19”) , виходячи із мінімальної відстані 15см та 30-40 см робочого простору.

Монтажні шафи стандартні (розміри : висота 180см, ширина – 74см, глибина – 66 см), забезпечено достатньо простору для робіт перед монтажною шафою (80см диспетчерського простору).

Кабелі захищені кабелепроводом, прокладеними по плінтусу.

Після монтажу всі кабельні виходи були марковані згідно стандарту (кожні 60см 3 рази).

2.5 Обґрунтування вибору операційних систем та програмного забезпечення для серверів та робочих станцій в мережі

Для сервера було обрано операційну систему Microsoft Windows Server Essentials 2016 Single Multilanguage OPEN No Level (G3S-01015) – це зручна мережева операційна система для швидкого створення надійних рішень.

Microsoft Windows Server Essentials 2016 Single Multilanguage OPEN No Level (G3S-01015) заснована на підвищеній надійності, масштабованості і керованості Windows 2000 Server, у такий спосіб вона є інфраструктурною платформою високої продуктивності для підтримки зв'язаних додатків, мереж, і веб-служб XML у будь-якому масштабі - від робочої групи до центру даних.

Microsoft Windows Server Essentials 2016 Single Multilanguage OPEN No Level (G3S-01015) — перша із операційних систем, що постачається користувачам з встановленою оболонкою NET Framework. Це дає системі виступати у ролі сервера застосунків для платформи Microsoft NET без необхідності встановлення додаткового програмного забезпечення.

Компанія Microsoft, у Microsoft Windows Server Essentials 2016 Single Multilanguage OPEN No Level (G3S-01015) збільшено ефективність системи безпеки. Тепер система інсталюється в мінімальній комплектації, без додаткових служб, що зменшує можливості атаки, що позитивно впливає на безпеку. У Windows Server 2016 входить програмний фаєрвол Internet Connection Firewall. Далі до системи було випущено пакет оновлення, який повністю зосереджений на підвищення безпеки системи і містить декілька додаткових функцій, які посилять захист від атак. Відповідно до американського стандарту безпеки Trusted Computer System Evaluation Criteria (TCSEC) система Windows Server 2016 відноситься до класу безпеки C2 — Controlled Access Protection.

У Windows Server 2016 доступна служба тіньового копіювання, яка автоматично записує старі версії файлів користувача, даючи змогу при необхідності повернутись до іншої версії того чи іншого документу. Робота з тіньовими копіями можлива тільки якщо встановлена «функція тіньових копій» на комп’ютері користувача, документи якого треба відновити.

Також в цій версії операційної системи було додано нові утиліти для адміністрування, які викликаються з допомогою командного рядка, що допомагає автоматизувати керування системою. Введено «ролі», на них базується керування сервером. Тому, наприклад, щоб створити файл-сервер, необхідно додати роль – «файл-сервер».

Окрім ОС для серверів обрано наступне ПЗ:

1. Plesk – комерційний програмний пакет для автоматизації Веб-хостингу. Plesk дозволяє адміністратору сервера налаштовувати нові веб-сайти, акаунти електронної пошти і записи DNS через Веб-інтерфейс . Адміністратор може створити шаблони клієнта і сайту, які будуть контролювати виділення ресурсів для домену та / або клієнта.
2. Веб-сервер Apache – відкритий веб-сервер Інтернет для UNIX-подібних, Microsoft Windows, Novell NetWare та інших операційних систем. На сьогодні є найуживанішим веб-сервером мережі Інтернет.
3. Веб-додатки: phpMyAdmin, Squirrellmail, Rouncube, Horde
4. Пошта: Postfix, Exim, Spamassassin, ClamAV;
5. Сервер DNS: Bind;
6. Сервер баз даних: MySQL, PostgreSQL, MS SQL Server;
7. Сервер IMAP: Dovecot, Courier IMAP;
8. Сервер FTP: PureFTP, vsFTP, proftpd;
9. Статистика: Awstats, Webalizer.

Для робочих станцій було обрано операційну систему Windows 10, яка розроблена компанією «Microsoft» для багатьох пристроїв таких як: комп'ютери, ноутбуки, планшети і смартфони. Ця версія називається останньою так як надалі вона надаватиметься за моделлю «програмне забезпечення як послуга» і періодично оновлюватиметься. Windows 10 має вдосконалену функцію Snap Assist, яка допомагає розподіляти простір екрана між вікнами, що дозволяє зручно працювати одразу з кількома програмами. Вона дозволяє розташувати на робочому столі до чотирьох вікон одночасно. Водночас Windows 10 підказує, які ще додатки запущені в системі і як їх можна розмістити. В цій ОС стала доступна функція створення кількох робочих столів (схожу функцію можна побачити в Ubuntu та Apple OS X).

Служба для входу до системи за допомогою біометричних даних Windows Hello дає змогу входити в систему за допомогою свого обличчя в тих застосунках і сайтах, котрі її підтримують.

Паралельно із Windows Hello Microsoft запустили систему, що називається Microsoft Passport, що дозволяє змінити пароль з допомогою особистих пристроїв, таких як смартфони, для того щоб можна було пройти авторизацію в корпоративних системах і інших сервісах компанії Microsoft.

Окрім ОС робочих станцій обрано наступне ПЗ:

1. Microsoft Office;
2. Антивірус Avast;
3. КОМПАС-3D;
4. Skype;
5. Viber;
6. Adobe Photoshop;
7. Adobe Illustrator;
8. Adobe Premiere Pro;
9. Adobe After Effects;
10. VLC media player;
11. File zilla client;
12. Ccleaner;
13. Any desk ;

У списку перераховані основні програми для роботи в офісі. При потребі на ПК буде встановлене додаткове ПЗ, яке потрібне для покращення виконуваної роботи.

2.6 Захист мережі

Для захисту мережі використовується Avira Server Security.

Установка Avira Server Security.

У першому вікні програми установника необхідно обов’язково прийняти ліцензійну угоду тиснемо «Далі» (див. рис. 2.11).

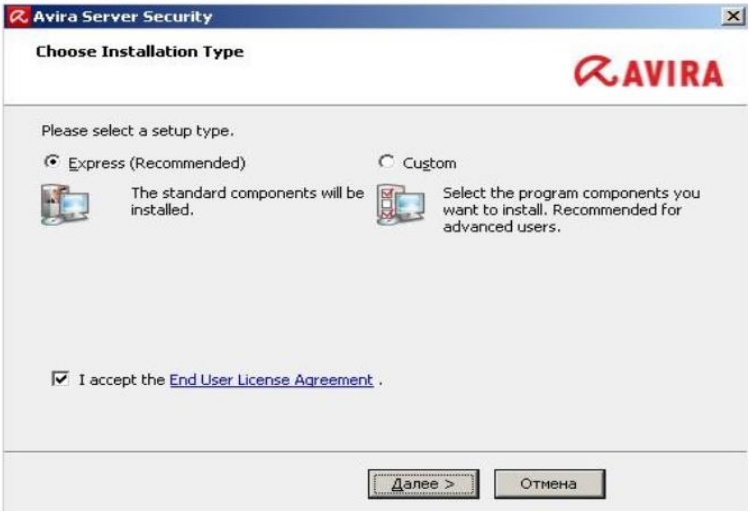

Рисунок 2.11 - Вікно вибору ліцензійної угоди

Антивірусна програма запропонує вибрати діючий файл ключа, який необхідно встановити, тиснемо «Browse» (див. рис. 2.12).

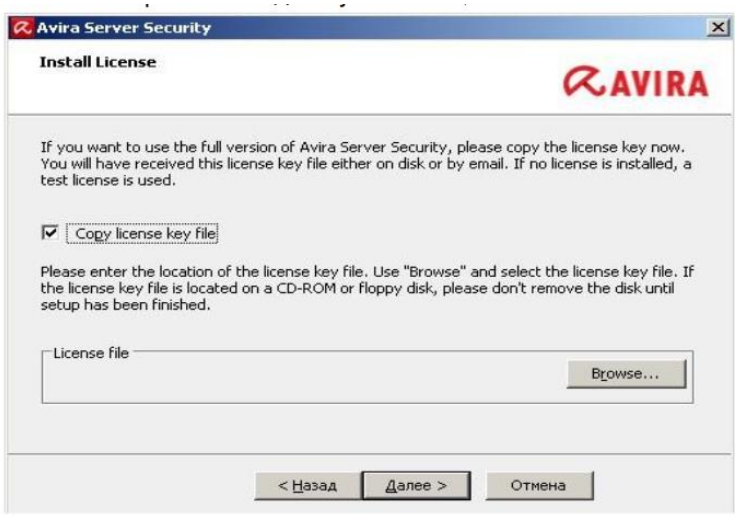

Рисунок 2.12 - Вікно вибору файла діючого ключа

Після цього з'явиться вікно провідника (див. рис. 2.13) в якому слід вибрати чинний файл ліцензії (hbedv.key) і натиснути «Відкрити».

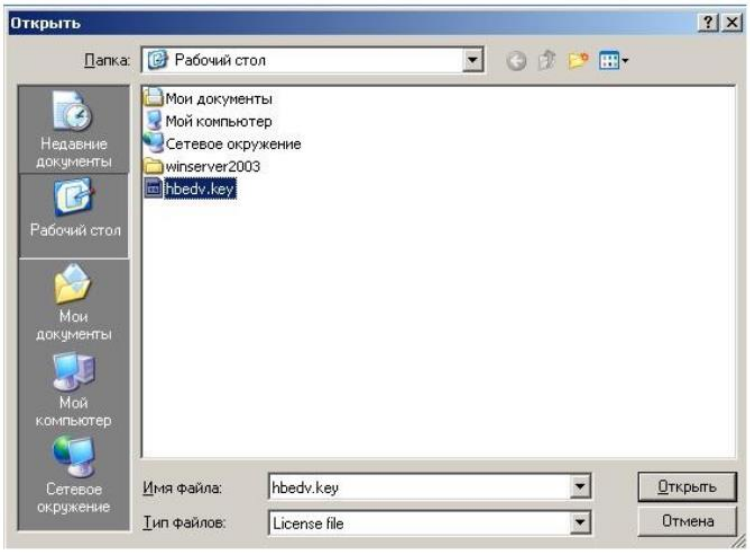

Рисунок 2.13 - Вікно вибору файлу ліцензії

Після цього відкриється вікно в якому необхідно натиснути кнопку «Далі» Далі відбудеться процес копіювання файлів (див. рис. 2.14)

Рисунок 2.14 - Вікно процесу копіювання файлів

Далі відбудеться процес копіювання файлів. По завершенню копіювання буде виконана перевірка системи (див. рис. 2.15) (за замовчуванням).

Рисунок 2.15 - Вікно перевірки системи

Для настройки потрібно натиснути на зірочку напроти потрібного нам меню. Після нажаття на зірочку буде активовано експертний режим розширених настройок. System Scanner – настройка дозволяє налаштувати сканування. Обираєм сканування всіх файлів, в додаткових настройках налаштовуєм сканування в середньому режимі. Налаштування дій при виявленні віруса: лікувати, якщо лікування неможливо тоді перемістити в карантин. Щоб не збільшувати час сканування обираєм сканувати архіви тільки з заданого списку.

Avira ProActiv- Активуємо. Таким чином, програми перевіряються Avira Internet Security 2012 на підозрілі дії. При виявленні подібної програми буде запропоновано її заблокувати або ігнорувати. Підозрілі програми (вірніше їх виконувані файли) будуть відправлені в вірусну лабораторію Avira Malware Researh Center для додаткової перевірки, якщо файл виявиться шкідливим, то відразу ж буде додано до антивірусних баз.

Firewall - Призначений для забезпечення контролю над усіма мережевими з'єднаннями, як вхідними так і вихідними. Рекомендується перевести в високий

рівень виявлення - це дозволяє зробити невидимим комп'ютер для зовнішнього несанкціонованого впливу. В установці доступу активуємо всі web-фільтри.

2.7 Тестування та налагодження мережі

Тестування і діагностика є обов’язковим аспектом при розробці, експлуатації й обслуговуванні мереж. Для тестування даної мережі будуть використані програми і утиліти компанії Fluke Networks.

Програмні й апаратні рішення для тестування, аналізу й моніторингу LAN/WAN мереж надають повну інформацію про роботу всієї мережі, усунення неполадок і керування. Портативні аналізатори дозволяють одержувати докладні дані про роботу локальних, бездротових, віртуальних і глобальних мереж. Серія портативних тестерів мережі дозволяє швидко усувати проблеми в лінії, кабелях і з'єднанні.

Приклади програм і приладів для тестування та налагодження мережі:

EtherScope II Network Assistant – портативний прилад для усунення неполадок у мережах стандартів 10, 100 і Gigabit, мідних, волоконно-оптичних і бездротових локальних мережах.

За допомогою аналізатора можна легко знайти й вирішити проблеми ще поки вони не торкнулися продуктивності якої-небудь частини або всієї мережі в цілому.

Мережевий тестер дозволяє здійснювати діагностику будь-яких обчислювальних мереж, що комутують, Ethernet - 10/100/1000Мбіт побудованих на "скрученій парі" з підтримкою віртуальних локальних обчислювальних мереж (VLAN), чи навіть бездротових мереж WiFi стандартів 802.11 /g/i/n. Також мережевий тестер дозволить здійснювати моніторинг всіх пристроїв підключених до мережі, а також надати необхідну статистику про роботу мережі і одержати відповідь на такі питання як: хто з користувачів більше всіх завантажує мережу - статистика про найбільш активних користувачів (Top Senders), який протокол, найбільш використовуваний у мережі (Protocol Mix), в кого є проблеми з великою

кількістю помилкових (Error Sources) або широкомовних пакетів (Top Broadcasters).

OptiVie Series III – портативний інтегрований мережевий аналізатор, що забезпечує огляд всієї корпоративної мережі.

В аналізаторі OptiView™ Integrated Network Analyzer, дуже насиченому ручному інструменті, закладені можливості всіх видів мережевого контролю й пошуку всіляких несправностей. Високоефективний аналізатор протоколів. Швидкодіючий кабельний тестер RMON2 зонд.

Повне візуальне подання мережі за секунди. Поєднує аналіз протоколів семи рівнів, виявлення активних компонентів, аналіз SNMP пристроїв, RMON2 аналіз трафіка й контроль пристроїв фізичного рівня в одному мобільному рішенні.

Дистанційний аналіз через Web. Доступ семи користувачів одночасно до одного приладу.

AnalyzeAir™ Wi-Fi Spectrum Analyzer – виявлення, ідентифікація й знаходження джерел радіочастотних перешкод у бездротових мережах 802.11

Спектроаналізатор AnalyzeAir надає повний огляд фізичного рівня бездротової мережі. Він швидко визначає, ідентифікує й знаходить радіо-випромінюючі пристрої, які можуть викликати перешкоди в бездротових мережах 802.11. Функція виявлення пристроїв AnalyzeAir дозволяє користувачам швидко виявляти проблемні або неавторизовані пристрої.

InterpretAir™ WLAN Survey Software – візуалізація покриття й оптимізація продуктивності бездротової мережі до й після її розгортання. Планування, розгортання, перевірка й розширення бездротової локальної мережі. Візуалізація характеристик продуктивності радіочастот і забезпечення покриття бездротової мережі. Документування даних про продуктивність для їхнього зберігання й створення звітів.

3 НАУКОВО-ДОСЛІДНА ЧАСТИНА
ЗАСОБИ МОНІТОРИНГУ РІВНЯ НАДІЙНОСТІ СИСТЕМИ

Підвищення ефективності інформаційної системи як комплексу апаратно-програмних засобів в значній степені залежить від регулярної її діагностики на безвідмовність. Створення ефективних систем діагностування дозволяє проводити моніторинг рівня надійності як окремих підсистем, так і системи в цілому, а значить, приймати правильні рішення про їх експлуатацію та обслуговування.

3.1 Математичний апарат для оцінки надійності роботи системи

Основними методами розрахунку надійності є метод інтегрально-диференційних рівнянь та метод диференційних рівнянь. Перший метод можна застосовувати для будь-яких законів розподілу напрацювання на відмову, але розв’язок отриманих рівнянь досить часто передбачає значні труднощі. Другий метод можна застосовувати лише для експоненційного закону розподілу напрацювання до відмови та часу відновлення, що в більшості випадків характерно для періоду нормальної експлуатації. Для того, щоб скласти систему диференційних рівнянь, необхідно перерахувати всі стани системи, скласти її логічну модель у вигляді схеми станів, що представляє собою орієнтований граф, кожна вершина якого відповідає певному стану системи, а ребра - можливі напрями переходів із стану в стан. Диференційні рівняння складаються на основі наступних правил:

– в лівій частині кожного рівняння стоїть похідна по часу від ймовірності знаходження системи в j-му стані в момент часу t;

– кількість членів в правій частині дорівнює кількості стрілок, які з’єднують даний стан з іншими;

– кожний такий член рівний добутку інтенсивності переходу на ймовірність того стану, з якого виходить стрілка;

– знак добутку додатній, якщо стрілка входить в стан, що розглядається, і від'ємний, якщо виходить з нього;

– кількість рівнянь дорівнює кількості станів системи.

Загальний принцип запису ІС диференційного рівняння для довільної вершини і, в яку система може прийти із m вершин і із якої переходить в одну із n вершин відображений в (3.1):

$$\frac{dP_i(t)}{t} = \sum_{j=1}^{m} \Lambda_{ji} P_j(t) - P_i(t) \sum_{z=1}^{n} \Lambda_{iz}. \tag{3.1}$$

Отримана система рівнянь доповнюється рівнянням:

$$\sum_{j=0}^{m} P_j(t) = 1, \tag{3.2}$$

де *Pj(t)* –ймовірність знаходження системи в *j*-му стані; *(m+1)* –кількість можливих станів системи. В результаті розв'язку системи диференційних рівнянь (за допомогою перетворення Лапласа) отримуємо ймовірності знаходження системи в кожному стані. Для того, щоб знайти функцію готовності, необхідно просумувати ймовірності знаходження системи в усіх робото-здатних станах:

$$K_Г(t) = \sum_{j=1}^{n} P_j(t), \tag{3.3}$$

де *n*–кількість робото-здатних станів

Функція простою визначається, як:

$$K_П(t) = 1 - K_Г(t). \tag{3.4}$$

Для отримання коефіцієнта готовності або простою необхідно розглянути режим експлуатації при $t \to \infty$, в цьому випадку всі похідні будуть рівні нулю і система диференційних рівнянь перетвориться в систему алгебраїчних рівнянь. При розрахунку надійності резервованих систем з врахуванням відновлення може бути всього декілька варіантів, які залежать від обмеження на відновлення. Відновлення називається необмеженим, якщо елемент, що відмовив починає відновлюватися відразу після відмови. Відновлення називається повністю обмеженим, якщо незалежно від кількості елементів, що відмовили, відновитися може тільки один з них. При частково обмеженому відновленні кількість ремонтних місць обмежена числом $m<k$ (k–кількість елементів в резерві).

3.2 Математична модель для оцінки надійності роботи досліджуваної системи

Стосовно конкретної системи, граф станів якої показано на рис. 3.1, система диференційних рівнянь (3.1) набуде вигляду (3.2)

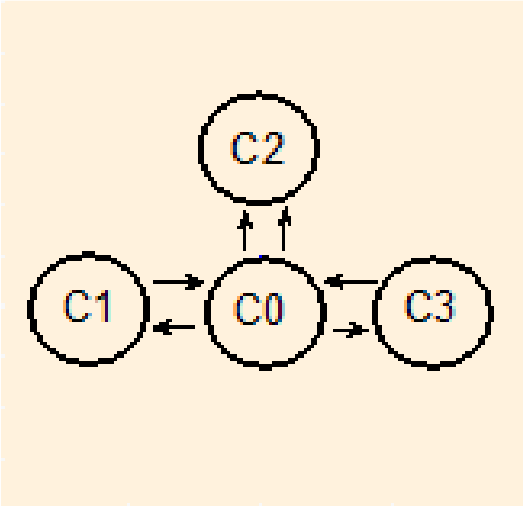

Рисунок 3.1 Граф станів досліджуваної інформаційної системи

$$\frac{dP0}{dt} = l\frac{dP0}{dt} - m\frac{dP1}{dT} - m\frac{dP2}{dt} - m\frac{dP3}{dt}$$

$$\frac{dP1}{dt} = l\frac{dP0}{dt} - m\frac{dP1}{dT}$$
$$\frac{dP0}{dt} = l\frac{dP0}{dt} - m\frac{dP2}{dt}$$
$$\frac{dP0}{dt} = l\frac{dP0}{dt} - m\frac{dP3}{dt}$$

(3.2)

Коефіцієнти безвідмовного напрацювання та інтенсивності відмови *l i m* в даній системі диференційних рівнянь (3.2) є величинами оберненими до середнього часу безвідмовної роботи роботи *Tvcep* та середнього часу простою конкретної ланки *Tfcep*:

$$l=1/Tvcep,$$
$$m=1/Tfcep.$$

Розв'язки *P1, P2,P3* системи (3.2) за конкретних початкових умов задаватимуть імовірності збою ланок 1,2,3, а *P0* – імовірність безвідмовної роботи системи. для їх знаходження визначимо *Tfcep i Tvcep* за даними журналу спостережень над роботою системи.

3.3 Оцінки середнього часу функціонування системи без збою на основі журналу спостережень.

З робочого журналу, де зафіксовані відомості про роботу досліджуваної системи вибираємо часові інтервали протягом яких складові системи працювали без збоїв, а також часові інтервали необхідні для приведення їх до робочого стану у випадку аварійних зупинок, на основі цих даних будуємо гістограми (див. рис 3.2, рис. 3.3), з яких можна зробити висновок, що розподіл часових інтервалів в обидвох випадках близький до нормального.

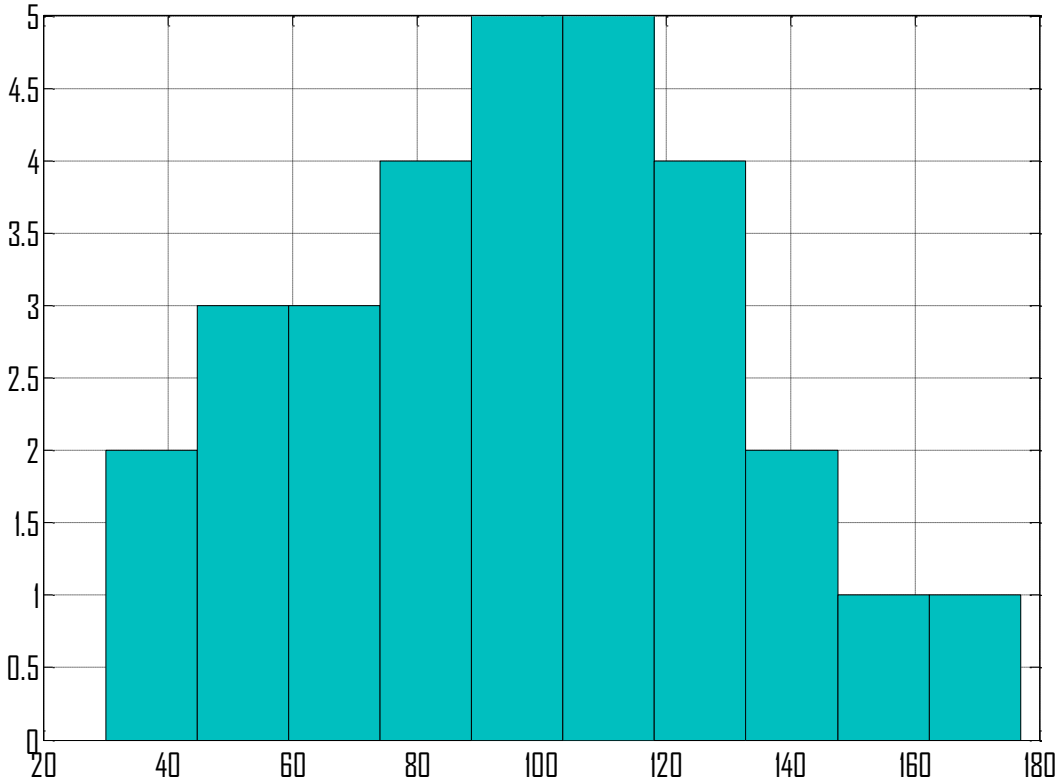

Рисунок 3.2 Гістограма часових інтервалів роботи системи без збоїв.

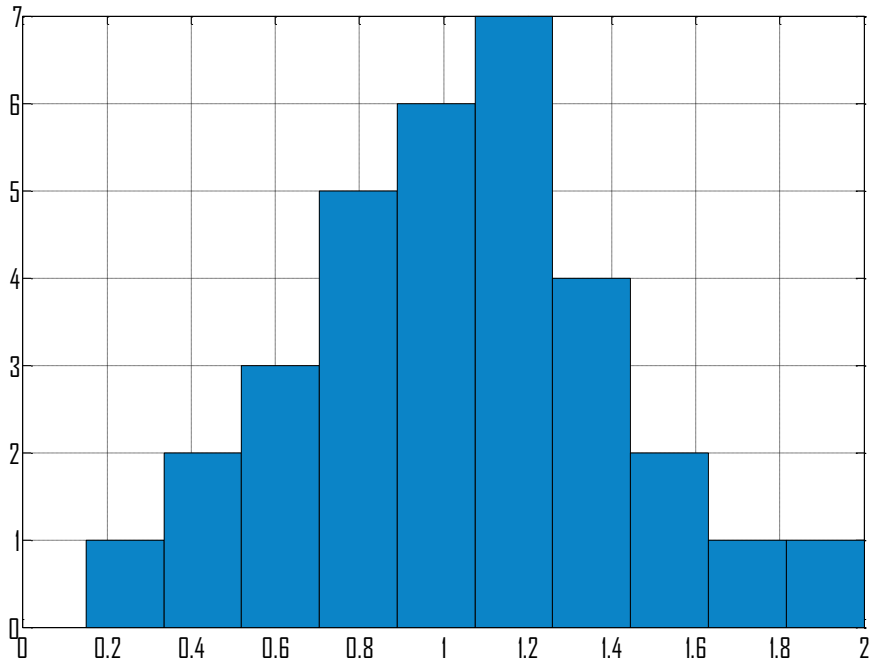

Рисунок 3.3 Гістограма часової послідовності простою вузла

Для знаходження середнього значення параметри нормального розподілу знаходимо за допомогою пакету Statistics (Distribution Fitting Tool) в matlab.

Результат опрацювання даних показано на рисунках 3.4 і 3.5.

Distribution: Normal

Log likelihood: -148.418

Domain: -Inf < y < Inf

Mean: 95.6

Variance: 1199.9

Parameter Estimate Std. Err.

mu 95.6 6.3243 Отже **Tvcep.= 95.6 год.**

sigma 34.6396 4.58813

Estimated covariance of parameter estimates:

	mu	sigma
mu	39.9968	-5.85011e-015
sigma	-5.85011e-015	21.0509

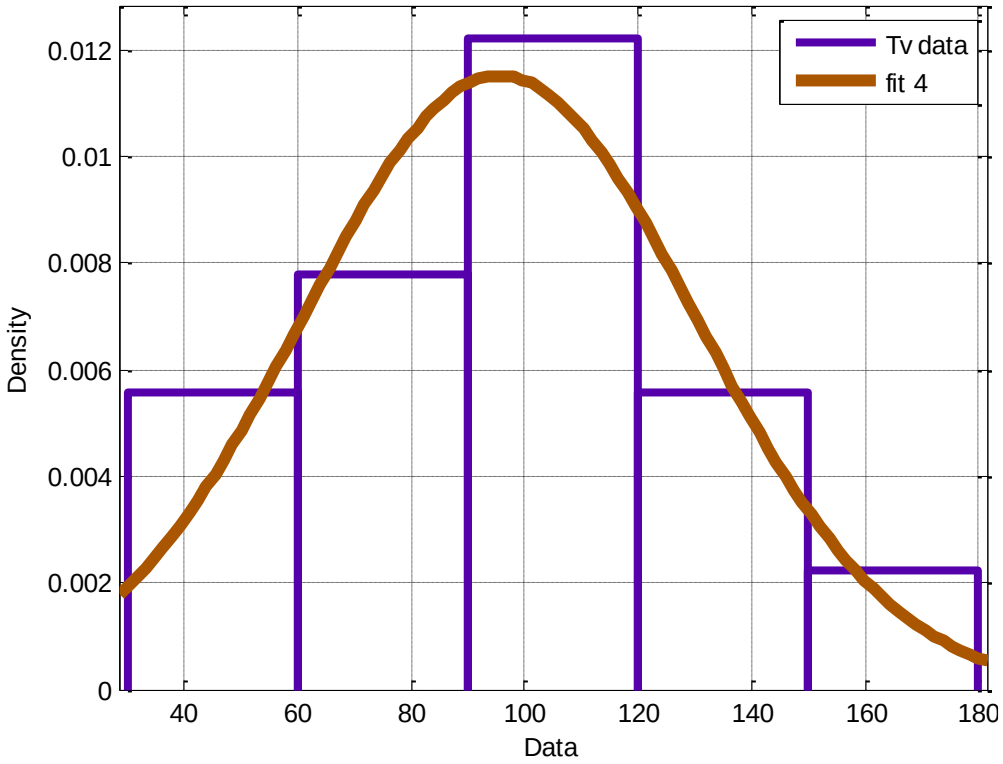

Рисунок 3.4 Підбір параметрів нормального розподілу

Таким чином математичне сподівання даного розподілу дає нам середній час роботи без збоїв конкретного вузла *Tvcep*=**mu=95.6 6.3243год.**

Аналогічні розрахунки проводим для оцінки часу середнього простою даного вузла.

Distribution: Normal

Log likelihood: -14.2879

Domain: -Inf < y < Inf

Mean: 1.03719

Variance: 0.147543

Parameter Estimate Std. Err.

mu 1.03719 0.0679024, отже Tf=1.03год.

sigma 0.384114 0.0491807

Estimated covariance of parameter estimates:

	mu	sigma
mu	0.00461073	4.26299e-018
sigma	4.26299e-018	0.00241875

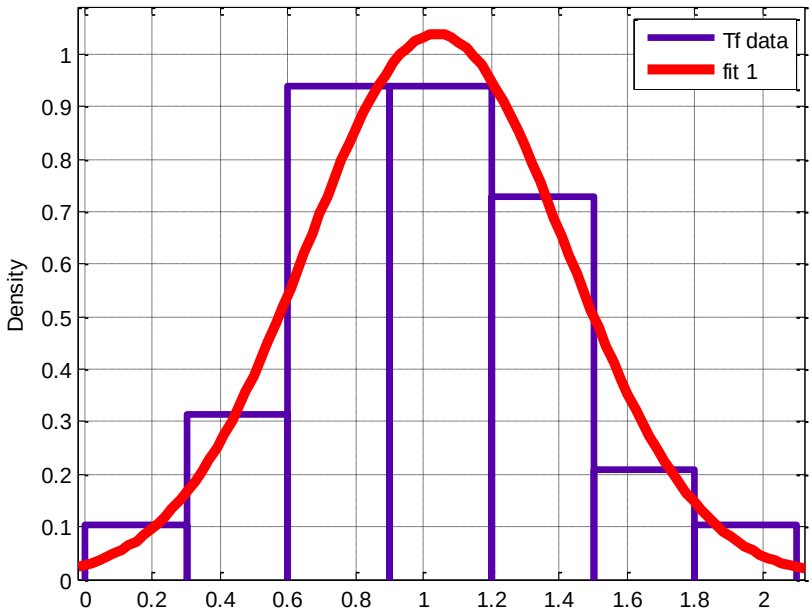

Рисунок 3.5 Результати обробки часової послідовності Tool statistik

Звідси отримаєм середній час вимушеного простою

Tfcep = **mu =1.03719год**

Програму для опрацювання даних часових послідовностей приведено нижче, побудова гістограми заданих масивів Tv і Tf (часу безперебійної роботи і часу (в год.)простою на основі спостережень за роботою системи):

```
clear all
Tv=[122 30 35 45 68 72 80 98 90 97 113 150 135 177 78 120 110 115 128 135
117 63 56 49 77 86 98 109 119 96];
hist(Tv)
Tf=[1 1.1 .9 .8 2 1.0 .80 .8 .50 .65 1.1 .50 1.35 1.0 .8 1.20 1.10 1.05 1.25 1.3 .15
1.6 1.3 .9 .8 .6 1.25 1.09 1.75 1.35 1.5 .7];
figure
hist(Tf)
```

3.4 Побудова S-моделі для моделювання динаміки показників надійності системи

S-модель для оцінки динаміки надійності досліджуваного об’єкта відображає систему диференційних рівнянь, побудовану за графом стану даної інформаційної системи засобами MATLAB SIMULINK. Вихідними параметрами є усереднені значення часу безвідмовної роботи та часу простою кожної із підсистем – величин, отримуваних в результаті статистичного опрацювання результатів спостережень протягом деякого періоду в п.3.4. Оскільки взаємодію підсистем можна відобразити графом станів (рис.1), на основі якого побудовано систему диференційних рівнянь (3.2) то дану систему можна представити S –моделлю, зображеною на рис. 3.6.

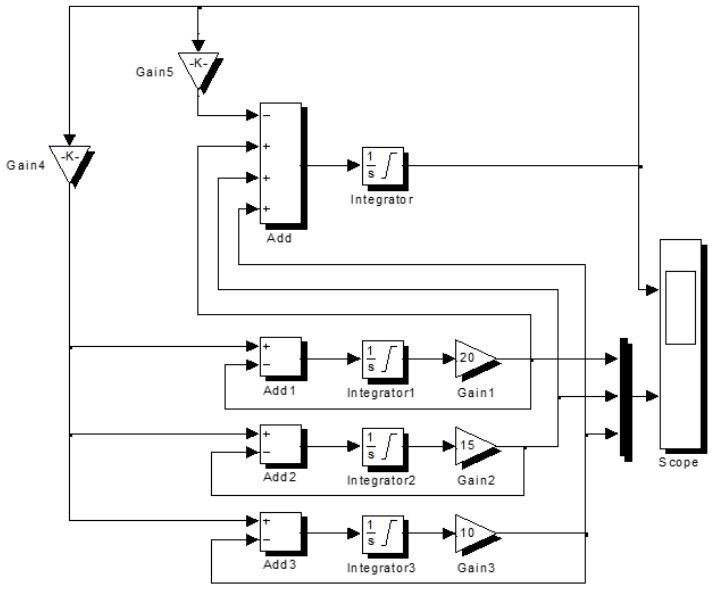

Рисунок 3.6 S-модель ІС, представленої графом станів на рис.4.5. $P_{00} = 0.95;\ P_{10} = 0.005;\ P_{20} = 0.008;\ P_0 = 0.95;\ P_{30} = 0.010;\ \mu = 0.008;\ \lambda_1 = 0.20;\ \lambda_2 = 0.15;\ \lambda_{13} = 0.15.$

Рисунок 3.6 S-модель ІС, представленої графом станів на рис.4.5. $P_{00} = 0.95;\ P_{10} = 0.005;\ P_{20} = 0.008;\ P_0 = 0.95;\ P_{30} = 0.010;\ \mu = 0.008;\ \lambda_1 = 0.20;\ \lambda_2 = 0.15;\ \lambda_{13} = 0.15.$

Результати спостерігаємо на блоках візуалізації моделі. Нижче приведено динаміку зміни імовірності безвідмовного функціонування системи (*P0*) (рис.3.7) та імовірностей відмови окремих підсистем (*P1, P2, P3*) (рис. 3.8) в залежності від часу експлуатації за конкретних характеристик надійності і початкових станів підсистем.

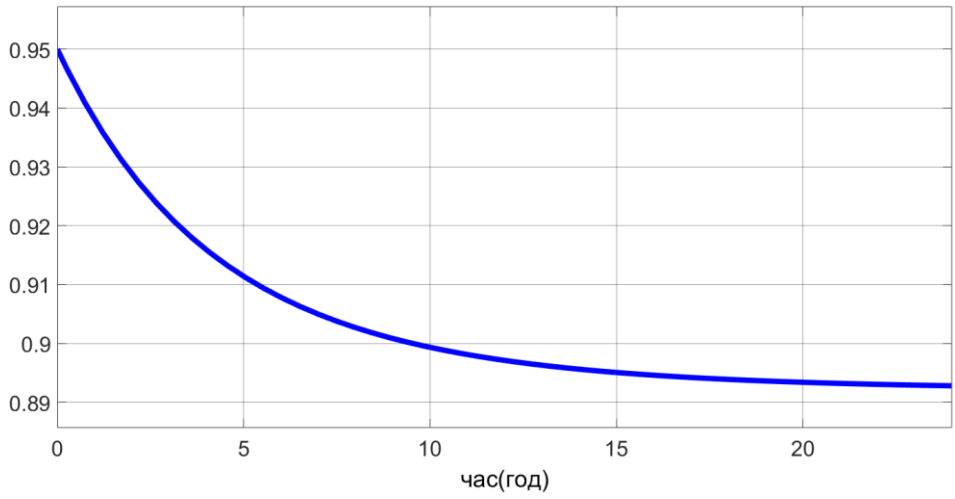

Рис.3.7 Зміна імовірності *P0* безвідмовного функціонування системи

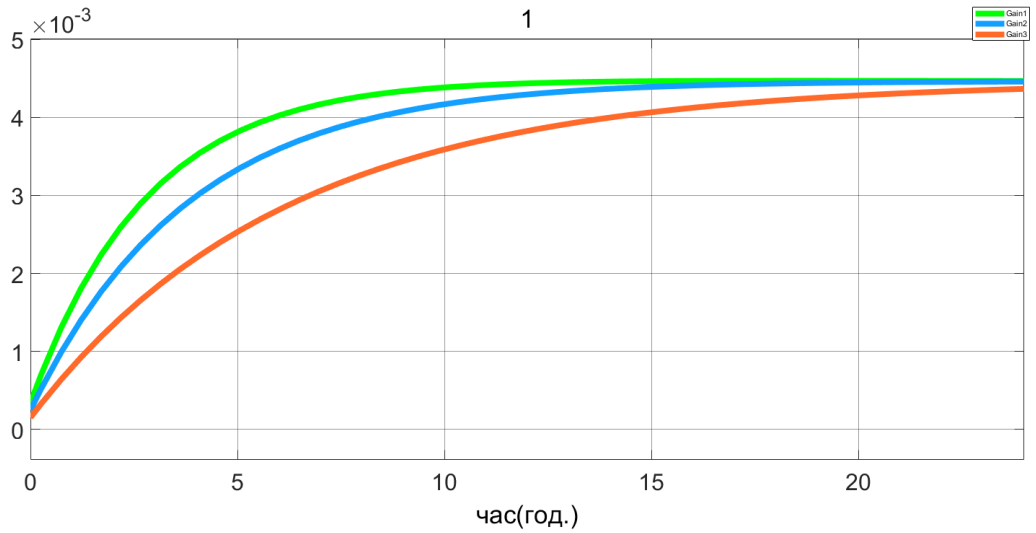

Рис.3.8 Зміна імовірності *P1, P2, P3* збоїв у ланках системи

3.5 Ідентифікація S-моделі

Паралельно для ідентифікації даної моделі розв'язок (3.2) знайдено в режимі роботи із символьними змінними в matlab. Програмне забезпечення для якого приведене нижче.

Результат динаміки зміни імовірності безвідмовного функціонування системи (*P0*) та імовірностей відмови окремих підсистем (*P1, P2, P3*) в залежності від часу експлуатації за конкретних характеристик надійності і початкових станів підсистем подано на рис 3.8, 3.10.

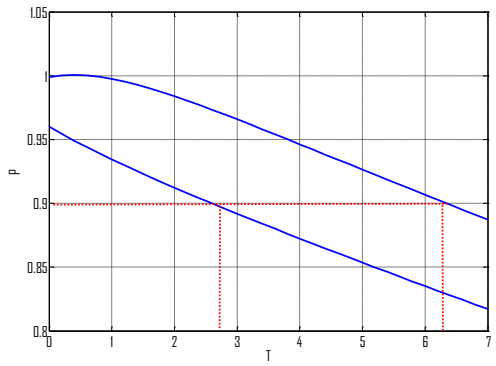

Рисунок 3.9 зміна імовірністі безперебійної роботи ситстеми з часом за різних початкових умов

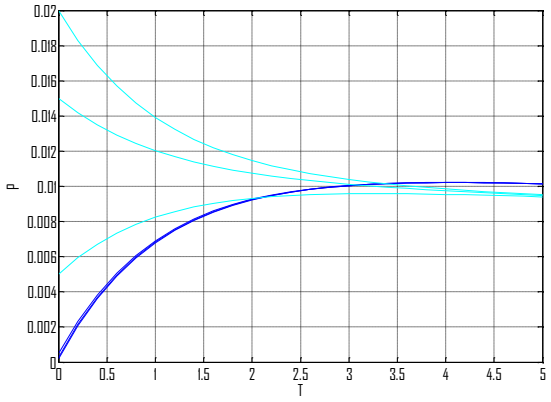

Рисунок 3.10 імовірності простою ланок за різних початкових умов

З порівняння результатів моделювання на аналітичній моделі та S-моделі слідує що дана S-модель адекватно відображає результати моделювання

Програмне забезпечення для знаходження розв’язку рівняння (3.2) засобами символьних обчислень в матлаб:

```
clear all
T=[0:.2:5];
sys='Dp0=.0105*p0-.971*p1-.971*p2-.971*p3,  Dp1=.0105*p0-.971*p1, Dp2=.0105*p0-.971*p2, Dp3=.0105*p0-.971*p3';
cnd={'p0(0)=.9990,p1(0)=.0002,  p2(0)=.0005, p3(0)=.0003','p0(0)=0.960,p1(0)=0.02,p2(0)=0.005,p3(0)=0.015'};
 %,...
%  'x(0)=0.9,y(0)=0.05, z(0)=0.05',...
%  'x(0)=0.99,y(0)=0.01,z(0)=0','x(0)=0.9,y(0)=0, z(0)=0.1'};
 for k=1:2
 [p0,p1,p2,p3]=dsolve(sys,char(cnd(k)))
 P0=subs(p0,'t',0:.2:7);
 P1=subs(p1,'t',0:.2:5)
 P2=subs(p2,'t',0:.2:5);
 P3=subs(p3,'t',0:.2:5);
%plot(T,P0),grid
```

```
%figure
 plot(T,P1)
 hold on
 plot(T,P2)
 plot(T,P3)
 end
 hold off;
 grid
```

Висновок

Запропонована - S-модель (рис. 3.5) для оцінки надійності інформаційної системи (рис.3.6) дозволяє прогнозувати тривалість безвідмовного функціонування (P_0) системи, імовірності збоїв в окремих підсистемах (P_1,P_2,P_3) а також часові інтервали між завчасними профілактичними оглядами для запобігання аварійних зупинок. Структура моделі легко піддається модифікації при зміні конфігурації досліджуваної системи

4 СПЕЦІАЛЬНИЙ РОЗДІЛ

4.1 Інструкції з налаштування програмного забезпечення серверів

Інсталяція Windows server буде проводитися з usb накопичувача, для цього потрібно вставити флешку в будь-який з роз'ємів материнської плати, далі потрібно натиснути кнопку включення і при завантаженні bios натиснути кнопку del. Після цього відкриється меню bios в якому потрібно знайти пункт завантаження і вибрати там наш завантажувальний usb накопичувач, зберегти настройки і вийти, сервер при цьому перезавантажиться і запуститься завантажувальна флешка, в першу чергу при інсталяції windows server буде запропоновано обрати мову локалізації в якому обираєм необхідну нам мову, після цього тиснем кнопку далі. Наступним кроком йде вибір редакції Windows Server 2016, далі приймаємо ліцензійну угоду, ставлячи відповідну галочку і тиснемо кнопку далі. Тепер потрібно вибрати тип установки - вибіркова установка Windows.

Останній етап це вибір диска на який буде установлено windows server 2016. Тут буде розпакування установочних файлів на жорсткий диск і подальше їх застосування, по завершенні чого буде кілька перезавантажень. Через деякий час з'явиться вікно налаштування параметрів, тут буде потрібно для облікового запису адміністратор задати пароль і підтвердити його. Чим менше на сервері запущено служб і ролей, тим він більш безпечний, менша кількість служб дозволяє зменшити фронт атаки на нього і як наслідок, він більш продуктивний. У даній редакції з'явився ще більш захищений режим у порівнянні з core і називається він Nano Server. У ньому немає так само графічного інтерфейсу GUI немає підтримки 32 розрядних додатків і мінімальну кількість компонентів. Ставлять його логічно, що для Hyper-V і кластерів зберігання з Scale-out File Server підійде для DNS сервера або хостингу на базі IIS. Локально на нього зайти не можна і можна управляти тільки за допомогою Windows PowerShel 5 і MMC консолі.

Заміна мережевої карти і оперативної пам'яті в Hyper-V налаштуваннях віртуальної машини> взагалі не минуло й року, як Microsoft таки реалізував це, ще

один пункт по наближенню до Vmware, завдяки цьому вийти не зупиняючи віртуальну машину.

Екрановані віртуальні машини (Shielded Virtual Machines)> свіжий механізм захисту віртуальної машини Hyper-V, в ньому присутня механізм шифрування томів в гостьовій системі, все тим же BitLocker, захист від шкідливого коду, так і для доступу адміністратора вузла Hyper-V.

Безпечне завантаження Linux (Linux Secure Boot)> Windows Server 2016 для ролі Hyper-V зробив можливість включати опцію безпечного завантаження (Secure Boot), для операційний систем CentOS 7, Red Hat 7 і вище, Ubuntu 14 і вище. Сенс Secure Boot в захисті віртуальної машини від rootkit.

PowerShell Direct> Щоб керувати через powershell віртуальною машиною віддалено, Windows Server 2016 має функціонал PowerShell Direct, він запускає команди PowerShell в VM. Доступ до гостьової операційної системи по мережі не потрібен, PowerShell Direct функціонує між віртуальною машиною і хостом. Це альтернатива Remote PowerShel і VM Connec.

Cluster OS Rolling Upgrade> даний функціонал, дозволяє поетапно перекинути вузли кластера з Windows Server 2012 R2 на 2016, без необхідності вимикати Hyper-V.

Дискретне призначення пристроїв (Discrete Device Assignment)> Windows Server 2016 Hyper-V завдяки функції Discrete Device Assignment, ви можете зробити перехід в гостьову операційну систему деяких пристроїв, які ви підключили до хосту віртуалізації Hyper-V через PCI Expres. Сенс цього, що віртуальна машина отримує прямий доступ до пристрою, прикладом може бути raid контролер або відео-карта.

Вкладена віртуалізація Hyper-V (Nested virtualization Hyper-V) в Windows Server 2016 Hyper-V, так само реалізована вкладена віртуалізація, це коли ви всередині віртуальної машини створюєте ще одну віртуальну машину VMCX і VMRS це свіжий формат файлу зберігання конфігурації для віртуальних машин, покликаний знизити ймовірність пошкодження даних у разі збою зберігання.

Контейнери Windows Server і Hyper-V технологія контейнерів в Windows Server 2016 дає можливість ізоляції додатків від ОС, і як наслідок забезпечити надійність і поліпшити його розгортання. У Windows Server 2016 таких два види контейнерів: Hyper-V Containers і Windows Server Containers. Контейнери Windows Server забезпечують ізоляцію через простір імен та ізоляцію процесів. Контейнери Hyper-V відрізняються більш надійною ізоляцією завдяки їх запуску в віртуальній машині.

Storage Replica - нова функція Windows Server 2016, робить реплікацію томів в Windows, на блочному рівні через SMB протокол, зручно для аварійного відновлення томів між серверами, через синхронну реплікацію. Роль сервера MultiPoint (MultiPoint Services Role) роль MPS в Windows Server 2016 дає розширену функціональність віддалених робочих столів. Сенс MultiPoint Services Role в тому, що у вас є слабке робоче місце, або тонкий клієнт (необхідна можливість підключення до MPS через USB або LAN), ви підключаєтеся до сервера і отримуєте недорогі призначені для користувача станції підключені до віддалених робочих столів.

Покращення Active Directory Domain Services (AD DS)> Windows Server 2016 приніс новий функціонал привілейоване управління доступом і Microsoft Passport все це відноситься до авторизації.

Storage Spaces Direct> функція дозволяє створити зі звичайних серверів, систему зберігання даних (СЗД) з високим ступенем доступності і масштабованості. З дисків підтримуються як і HDD так і SSD і дискові пристрої NVMe.

Remote Desktop Protocol (RDP) Graphics Compression> в Windows Server 2016 поліпшили і RDP технологію, що дозволило знизити пропускну здатність і збільшило швидкість роботи.

Credential Guard> цей компонент Windows Server 2016, робить захист облікових даних, щоб тільки привілейоване системне ПО могло отримувати доступ до цих даних. Якщо у вас є вірусні програми, які працюють з правами адміністратора, отримати доступ до облікового запису не зможуть, завдяки

Credential Guard, що працює в захищеному середовищі, ізольованій від ОС, у всіх інших версіях використовувалася система LSA.

Оскільки у даній мережі буде утворено кілька незалежних груп, то на серверах потрібно встановити відповідні налаштування.

Для розмежування прав доступу налаштуємо службу каталогів (Active Directory). Це LDAP-сумісна реалізація інтелектуальної служби каталогів корпорації Microsoft для операційних систем родини Windows NT. Active Directory дозволяє використовувати групові політики (GPO) для забезпечення подібного налаштування користувацького робочого середовища, розгортати ПЗ на великій кількості комп'ютерів (через групові політики або за допомогою Microsoft Systems Management Server 2016 (або System Center Configuration Manager)), встановлювати оновлення ОС, прикладного та серверного ПЗ на всіх комп'ютерах в мережі (із використанням Windows Server Update Services (WSUS); Software Update Services (SUS) раніше). Active Directory зберігає дані і налаштування середовища в централізованій базі даних. Мережі Active Directory можуть бути різного розміру: від кількох сотень до кількох мільйонів об'єктів.

Служба доменних імен (DNS) є показником Active Directory в операційній системі Windows Server 2016. Клієнти Active Directory і програми, які виконуються на клієнтських комп'ютерах, використовують службу DNS для пошуку контролерів домену під час входу до системи та під час виконання адміністративних функцій. Для правильної роботи служби Active Directory і клієнтських програм потрібна наявність інстальованого й настроєного DNS-сервера.

На першому етапі потрібно призначити серверу статичну конфігурацію протоколу IP. DNS-сервери не повинні використовувати динамічні IP-адреси, оскільки динамічне змінення IP-адреси може призвести до втрати клієнтськими комп'ютерами зв'язку із DNS-сервером.

Настройка TCP/IP:

1. Натиснути кнопку Пуск, вибрати пункт меню Настройка, а потім - Панель управління.

2. Двічі натиснути піктограму Мережа і віддалений доступ до мережі.

3. Правою кнопкою миші натиснути пункт Підключення по локальній мережі, а потім вибрати команду Властивості.

4. Вибрати пункт Протокол Інтернету (TCP/IP) і натиснути кнопку Властивості.

5. Вказати статичну IP-адресу сервера, маску підмережі та адресу шлюзу.

6. Натиснути кнопку Додатково.

7. Відкрити вкладку DNS.

8. Вибрати параметр "Дописувати основний DNS-суфікс и суфікс підключення"

9. Встановити прапорець "Дописувати рідні суфікси основного DNS-суфікса"

10. Установити прапорець "Зареєструвати адреси цього підключення в DNS"

11. Натиснути кнопку ОК, щоб закрити діалогове вікно "Додаткові параметри TCP/IP".

12. Натиснути кнопку ОК, щоб підтвердити зміни конфігурації TCP/IP.

13. Натиснути кнопку ОК, щоб закрити діалогове вікно "Властивості підключення по локальній мережі".

Далі налаштовується Microsoft DNS Server:

1. Натиснути кнопку Пуск, вибрати пункт меню Настройка, а потім - Панель управління.

2. Двічі натиснути Установка і видалення програм.

3. Натиснути кнопку Додання і видалення компонентів Windows.

4. Після запуску майстра компонентів Windows натиснути кнопку Далі.

5. Вибрати компонент Мережеві служби, а потім натиснути Вміст.

6. Установити прапорець DNS, а потім натиснути кнопку ОК.

7. Натиснути кнопку ОК, щоб запустити інсталяцію сервера. На комп'ютер буде скопійовано DNS-сервер і службові програми.

Налаштування DNS-сервера за допомогою диспетчера DNS:

1. Натиснути кнопку Пуск і послідовно вибрати команду Програми, Адміністрування та Диспетчер DNS. Під іменем комп'ютера буде відображено імена двох зон: Зона прямого перегляду і Зона оберненого перегляду.

2. Після запуску майстра налаштування DNS-сервера натиснути кнопку Далі.

3. Натиснути пункт Зона прямого перегляду, а потім вибрати команду Властивості.

4. Додати зону прямого перегляду. Натиснути кнопку Далі.

5. Для підтримки динамічних оновлень потрібно, щоб нова зона прямого перегляду була основною зоною. Вибрати пункт Основна, а потім натиснути кнопку Далі.

6. Нова зона містить записи покажчика для цього домену Active Directory. Ім'я зони має бути таким самим, як і ім'я домену Active Directory, або бути логічним DNS-контейнером для цього імені.

7. Прийняти ім'я зони, яке пропонується за замовчуванням, для файлу нової зони. Натиснути кнопку Далі.

8. Не додавати зону оберненого перегляду. Натиснути кнопку Далі.

9. Натиснути кнопку Готово, щоб завершити роботу майстра.

Увімкнення підтримки динамічних оновлень у зоні прямого перегляду:

1. У вікні диспетчера DNS розгорнути об'єкт DNS Server. Розгорнути папку Зони прямого перегляду.

2. Клацнути правою кнопкою миші на створену зону, а потім вибрати команду Властивості.

3. Перейти на вкладку Загальні, встановити прапорець Дозволити динамічне обновлення, а потім натиснути кнопку ОК, щоб підтвердити зміни.

Увімкнення інтегрованого сховища Active Directory для DNS:

1. У вікні диспетчера DNS розгорнути об'єкт DNS Server.

2. Розгорнути папку Зони прямого перегляду.

3. Клацнути правою кнопкою миші на створену зону, а потім вибрати команду Властивості.

4. Перейти на вкладку Загальні, переконатися, що для параметра Тип зони встановлено значення Основний. Натиснути кнопку Змінити, щоб змінити тип зони.

5. У діалоговому вікні Зміни типу зони вибрати тип Інтегрована в Active Directory основна, а потім натиснути кнопку ОК. DNS-сервер запише базу даних зони до Active Directory.

6. Клацнути правою кнопкою миші зону ".", а потім вибрати команду Властивості.

7. Перейти на вкладку Загальні, переконатися, що для параметра Тип зони встановлено значення Основний. Натисніть кнопку Змінити, щоб змінити тип зони.

8. У діалоговому вікні Зміна типу зони вибрати тип Інтегрована в Active Directory основна, а потім натисніть кнопку ОК.

Також для запуску мережі потрібно налаштувати комутаційне обладнання.

Будь який комутатор (концентратор, комутатор чи маршрутизатор) має інтерфейс для забезпечення діалогу з користувачем для забезпечення можливостей налаштовування систем. Для цього використовують в більшості систем протоколи Telnet, SNMP або найчастіше Web - інтерфейс. Для управління в таких системах використовують спеціалізоване програмне забезпечення, яке записано в енергонезалежну пам’ять. Дане програмне забезпечення можна обновляти .

Консольне управління виконується через термінал. Для підключення використовують стандартний послідовний порт RS-232C в асинхронному режимі. В якості терміналу найчастіше застосовують Hyper Terminal при цьому слід відповідно налаштувати порт, за допомогою якого виконується підключення (як правило COM1).

Підключення з допомогою Telnet дозволяє віддалено задавати налаштування пристроями по мережі передачі даних з використанням IP. До використання Telnet наш пристрій повинен бути налаштований відповідним чином через консоль, йому повинна бути призначена IP адреса, маска підмережі для відповідного порту, через який буде виконуватися підключення.

В нижній частині діалогового вікна міститься список Type Access, що розкривається (Тип доступу). В переліку типів доступу містяться такі відомі опції, як List (Відображати список), Read (Читати), Add (Додавати) і Change (Змінювати). Крім того, в списку містяться елементи Special Directory Access (Доступ до спеціальних тек) і Special File Access (Доступ до спеціальних файлів). При їх виборі для доступу до тек і файлів можна призначити спеціальні дозволи.

NTFS надає два способи призначення дозволів на доступ до ресурсів. Можна використовувати окремі дозволи, що містяться в групі спеціальних дозволів (special permissions), або призначити більш вузьку групу стандартних дозволів (standard permissions), що містить комбінацію спеціальних дозволів. Щоб розібратися з принципами використовування цих груп, краще всього проглянути список спеціальних дозволів, а потім познайомитися з тим, як з них формуються стандартні дозволи, які застосовуються більшістю користувачів.

В переліку спеціальних дозволів визначені дії, які можуть бути виконані над ресурсом, а також рівень управління ними:

1. R — читання;
2. W — запис;
3. X — виконання;
4. D — видалення;
5. P — зміна;
6. O — зміна власника.

Щоб спростити призначення дозволів для файлів, можна скористатися стандартними дозволами. Вони є наступними комбінаціями:

1. Read (Читання) — RX;
2. Change (Зміна) — RWXD;
3. Full Control (Повний доступ) — RWXDPO;
4. No Access (Немає доступу).

Використовування стандартних дозволів знижує ступінь деталізації процесу управління доступом. При цьому для дозволу або заборони доступу до ресурсу в більшості випадків цього цілком достатньо.

Після першого входу в ОС запуститься майстер «Налаштування Windows Server Essentials», який допоможе зробити первинну настройку.

На першому кроці необхідно задати налаштування дати і часу.

На другому кроці необхідно заповнити англійською мовою назву компанії. Ім'я домента та ім'я сервера будуть в такому випадку згенеровано автоматично, хоча їх можна поміняти.

На наступному кроці необхідно заповнити ім'я адміністратора і задати пароль.

На останньому кроці необхідно вказати спосіб оновлення операційної системи і натиснути налаштувати.

Після цього запуститься процес, який зробить всі необхідні початкові налаштування. Це займе близько 30 хвилин і зажадає кілька перезавантажень. За цей час ОС встигне зокрема встановити необхідні параметри і налаштувати сервер в якості домен контролера для нового домену.

Налаштування

Вся настройка відбувається в панелі моніторингу, доступ до неї є з робочого столу, панелі швидкого запуску і стартового екрану.

Створення користувачів

При першому запуску даної панелі відкриється вкладка установка, на якій можна виконати ряд завдань по налаштуванню сервера.

Додавання користувачів. Клацаємо посилання для додавання облікових записів.

Заповнюємо поля форми облікового запису (див. рис. 4.1) і натискаємо далі.

Вибираємо рівень доступу до загальних папок, які були створені. На початковому етапі існує лише одна - Організація. Надалі можна змінювати дозволи на доступ, як з властивостей користувача, так і з властивостей папки.

Далі встановлюємо, що буде доступно для користувача віддалено.

Обліковий запис створено. Тиснемо закрити.

Додавання папок сервера

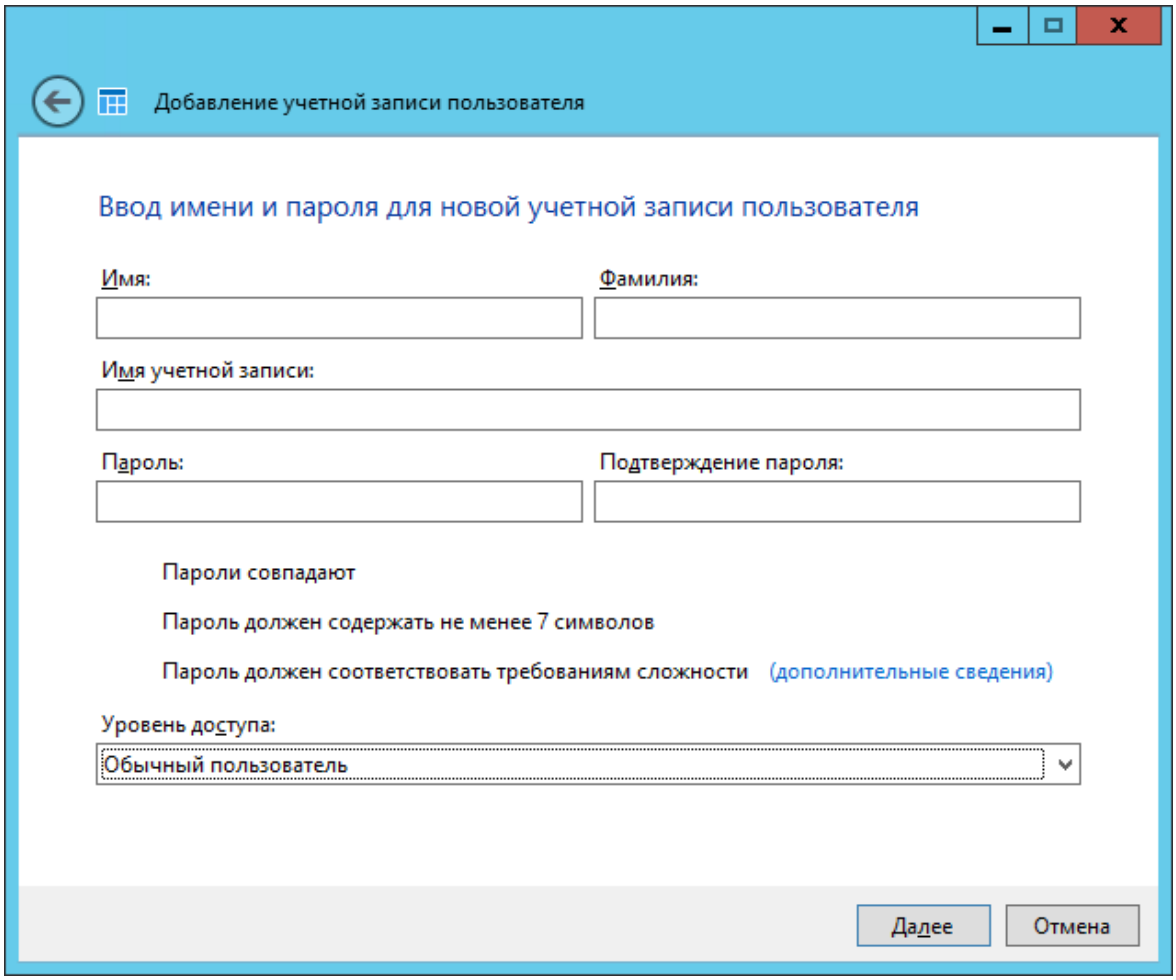

Рисунок 4.1 – вікно створення облікового запису

Для додавання папок існує інший майстер, який допоможе і створити папку на диску, і загальний доступ для неї налаштувати, і дозволу видати. Для його запуску необхідно клацнути відповідне посилання в панелі моніторингу.

У вікні майстра вводимо назву. Можна змінити розташування і додати опис. Натискаємо далі.

На наступній сторінці вказуємо необхідні дозволи. При необхідності робимо її недоступною при віддаленому доступі.

З останнього кроку даного майстра можна запустити майстер настройки архівації. Натискаємо закрити.

Підключення робочих станцій

Якщо ми і на цей раз відкриємо панель моніторингу та перейдемо на сторінку підключення комп'ютерів, то побачимо там лише інструкцію до дії. Слідуючи

інструкції на клієнті в браузері відкриваємо сторінку http: // <Ім'я сервера> / connect. Натискаємо посилання для скачування. Скачуємо програму натискаємо відкрити. Приймаємо ліцензію.

– вводимо ім'я користувача та пароль користувача даного комп'ютера або адміністратора;

– перезавантажуємо сервер;

– вибираємо, хто буде користуватися комп'ютером. Настройка для себе або для себе та інших користувачів;

– вводимо описання комп'ютер;

– налаштовуємо параметри архівації;

– готово.

Заходимо на комп'ютер під обліковим записом користувача. На робочому столі вже буде ярлик з загально доступними папками.

Налаштування FTP – сервера.

Операційна система windows server 2016 має вбудовану функціональність FTP. Перш за все, необхідно активувати серверну роль FTP. У Windows Server 2012 зробити це можна в меню установки веб-сервера IIS. Для цього потрібно зайти в диспетчер серверів і вибрати на пункт «Додати ролі та функції».

Далі потрібно вибрати пункт «Установка ролей або компонентів».

Вибрати сервер на якому будемо налаштовувати FTP.

Потім в списку ролей сервера потрібно знайти блок, що відноситься до веб-сервера IIS, і розгорнути його. Далі потрібно поставити галочку в клітинку навпроти напису «FTP-сервер» і натиснути далі.

На наступному кроці здійснює установка ролі FTP-сервера.

Далі потрібно відкрити Диспетчер служб IIS і вибрати в ньому локальний сервер.

Потім потрібно натиснути правою кнопкою миші на меню Сайти і вибрати пункт «Додати FTP-сайт».

На наступному етапі потрібно придумати назву FTP-сайту і вказати папку, в якій будуть зберігатися файли.

Потім необхідно ввести IP-адресу сервера (він повинен збігатися з адресом, зазначеною в налаштуваннях мережевого адаптера), встановити галочку навпроти «Запускати сайт FTP автоматично» і вибрати пункт «Без SSL».

На наступному кроці потрібно вибрати звичайну автентифікацію і дозволити доступ усім користувачам (з дозволами на читання і запис).

Потім на сервері потрібно відкрити браузер і в адресному рядку ввести ftp: // ip-адреса (наприклад, ftp://188.227.16.74). Після введення логіна і пароля відкриється наступна сторінка.

Тут потрібно натиснути клавішу Alt, потім зайти в меню Вид і вибрати пункт «Відкрити FTP-сайт в провіднику».

Після чого відкриється вміст папки FTP-сервера.

Далі потрібно зробити настройки брандмауера. Для цього потрібно відкрити PowerShell і вбити туди наступну команду:

netsh advfirewall firewall add rule name=”FTP” action =allow protocol=TCP dir=in localport=21.

Після цього підключення до сервера з клієнтського комп’ютера можна проводити наприклад через браузер.

Захист мережі

В операційну систему Windows Server 2016 інтегровано засоби захисту клієнтських робочих станцій від несанкціонованого доступу до них з Інтернет.

Налаштування сервера зберігання інформації

В якості мережевого сховища використовується сервер qnap TS-832XU-RP, на даному сервері встановлено власна операційна система, QTS створена спеціально для пристроїв зберігання даних. Встановлювати операційну систему непотрібно так як сервер продається готовий до роботи, нам залишається лише налаштувати його.

Для того щоб підключитися до сервера для налаштування підключаєм його до нашої мережі після цього з допомогою програми Qnap qfinder pro (див. рис. 3.2) скануємо мережу і знаходимо наш сервер і дивимось під якою ip адресою він знаходиться.

Рисунок 4.2 Вікно програми Qnap qfinder pro

Для того щоб підключитися до веб інтерфейсу налаштування сервера використовуючи будь-який браузер вводимо в адресну строку його ip, після цього відкриється вікно входу (див. рис 4.3) в веб інтерфейс, де потрібно ввести пароль і логін тому, що вхід перший то пароль буде стандартний «admin».

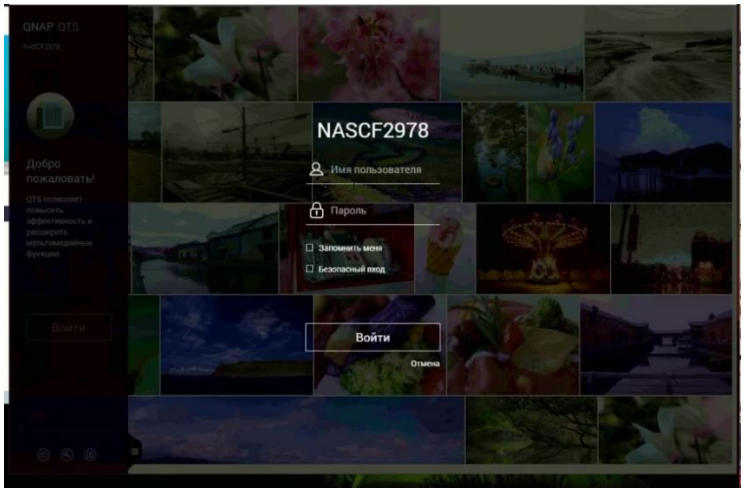

Рисунок 4.3 вікно входу в веб інтерфейс

Наступним кроком буде додавання сервера в домен, для цього потрібно зайти в панель керування і вибрати пункт меню «привілеї» підпункт «безпека домена»,

далі вибираємо з списку додати сервер в домен і в наступному вікні настройки нам запропонують ввести назву домена (див. рис. 4.4), вводимо назву і адресу DNS сервера, тиснем далі.

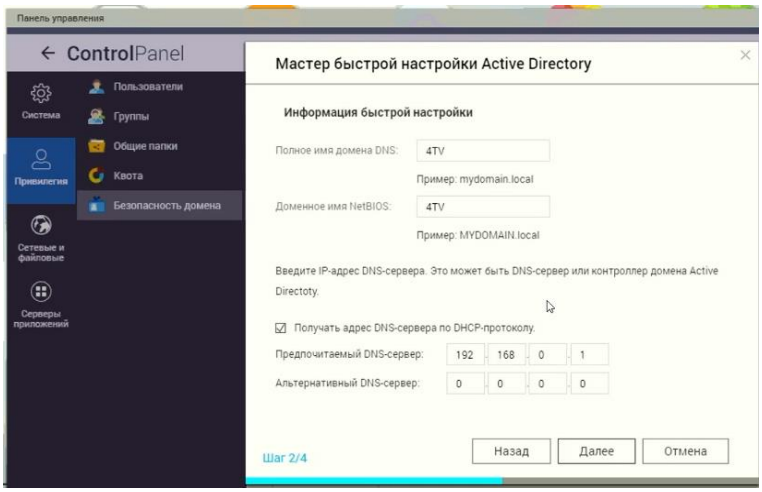

Рисунок 4.4 вікно внесення сервера в домен

Вікно авторизації (див. рис. 4.5) в якому потрібно обрати домен і ввести логін і пароль адміністратора для підтвердження входу в домен, після цього відкриється наступне вікно з підтвердженням про внесення сервера в домен. На цьому кроці внесення в домен сервера завершено.

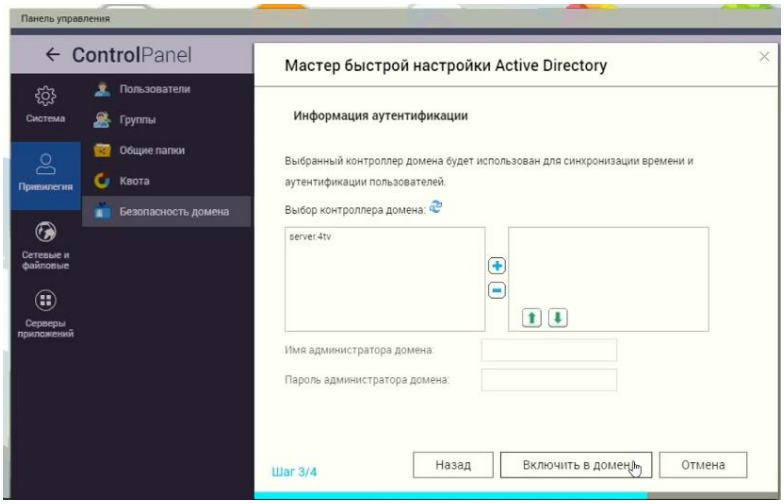

Рисунок 4.5 вікно авторизації

Наступний крок створення RAID масиву. Для створення RAID масиву потрібно зайти в панель керування пункт меню «менеджер зберігання» після цього обираєм вкладку управління томами (див. рис 4.6) і тиснем кнопку «створити».

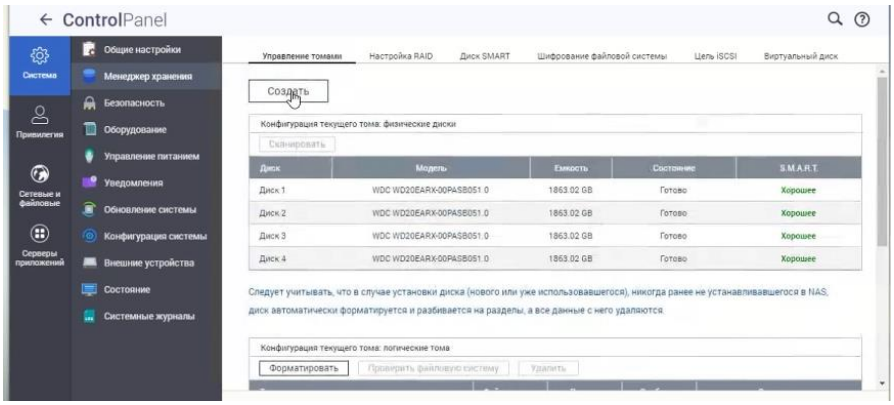

Рисунок 4.7 вікно програми управління томами

Після натискання кнопки створити в нас відкриється вікно вибору рівня RAID (див. рис. 4.8), нам потрібен 5 рівень при якому при виході із ладу одного з дисків ми не втратимо інформацію а зможем відновити за рахунок інших носіїв інформації.

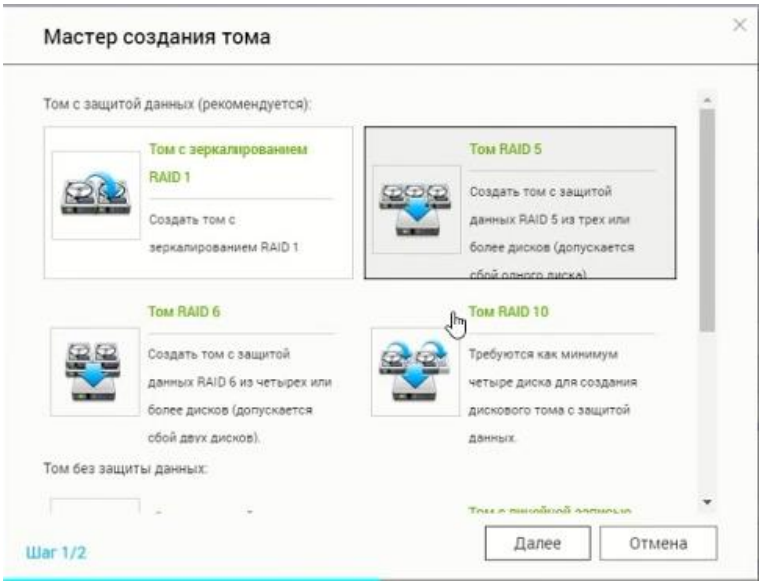

Рисунок 4.8 вікно вибору рівня RAID

Далі потрібно обрати, які диски будуть використовуватися для створення RAID масиву (див. рис 4.9) , для цього потрібно відмітити потрібні нам диски і

натиснути кнопку «створити». Після створення масиву потрібно провести форматування дисків, надалі всі диски будуть відображатися як один том.

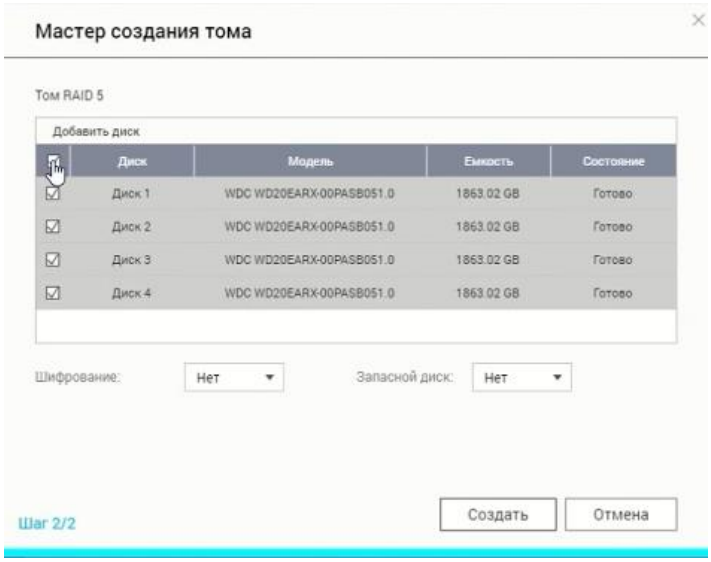

Рисунок 4.9 вікно вибору дисків для створення масиву

Після форматування тому можна створювати папки на сервері і налаштовувати доступ, для цього заходим в панель керування далі привілеї тоді загальні папки (див. рис 4.10) , вкладка спільні папки, для створення папки натискаєм створити в меню вибираєм «спільна папка».

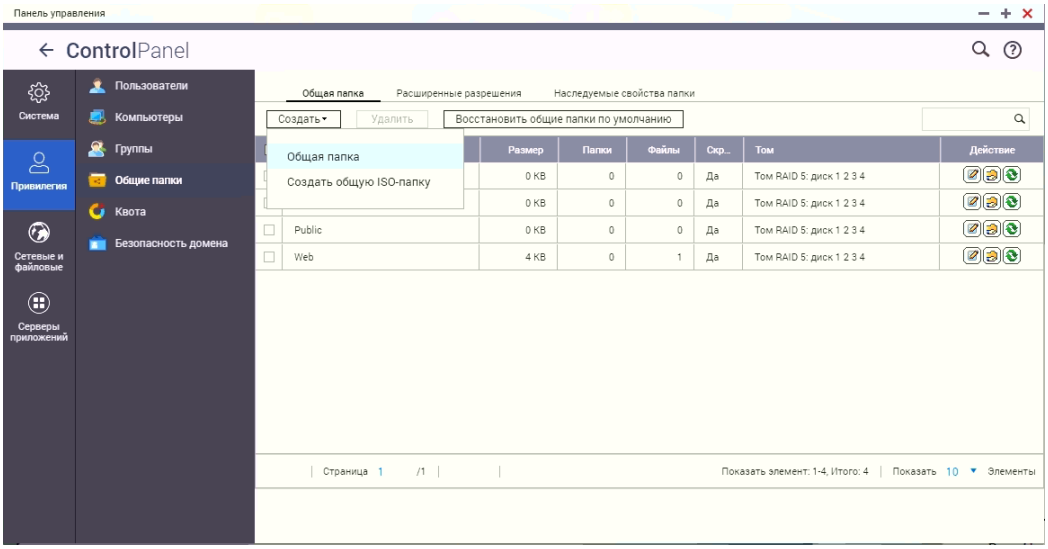

Рисунок 4.10 вікно створення папок

В наступному вікні дається можливість дати назву папки і настройки доступу користувачів(див. рис. 4.11)

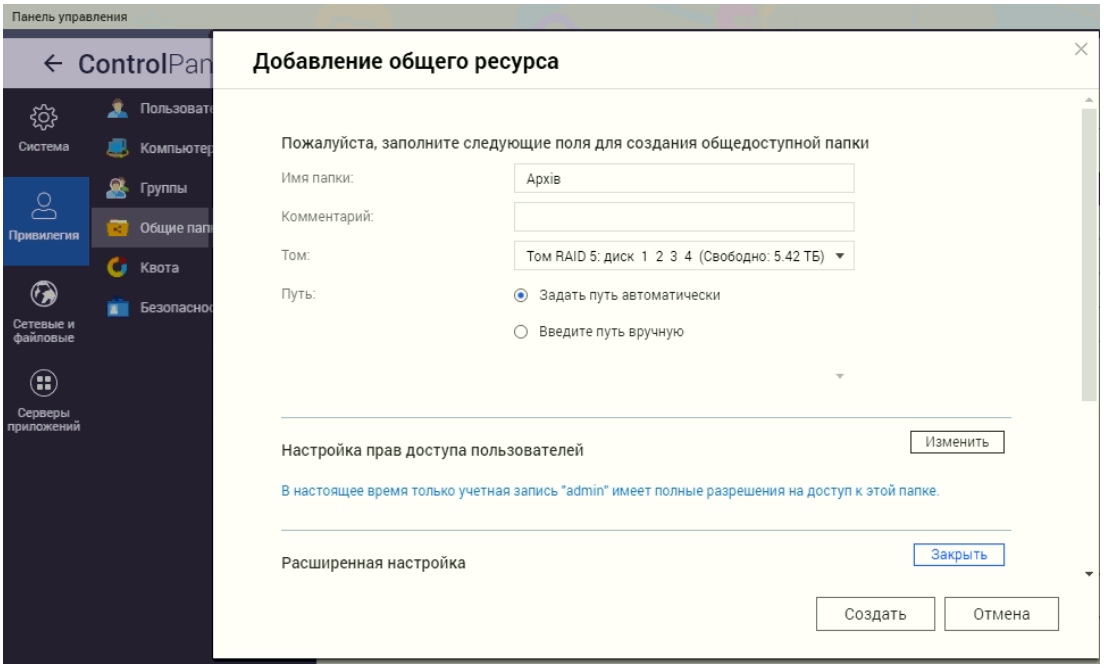

Рисунок 4.11 додаткові настройки папок

В разі, якщо необхідно змінити налаштування доступу до папок, потрібно вибрати потрібну папку і натиснути кнопку настройка прав доступу до спільних папок, після чого відкриється вікно налаштування доступу в якому можна змінити права вже доданих користувачів заборонити доступ дати дозвіл на читання чи на читання і запис. Якщо потрібно додати користувача натискаєм кнопку «добавити», після чого відкриється вікно вибору користувачів, груп і комп'ютерів, в списку якого будуть відображатися користувачі, комп'ютери і групи домену.

4.2 Інструкції з налаштування активного комутаційного обладнання

Для підключення до маршрутизатора потрібно взяти консольний кабель, підключити в порт консолі маршрутизатора і до COM порту комп'ютера. Запускаємо програму HyperTerminal на комп'ютері. Вибираємо COM порт до якого підключений маршрутизатор вибираємо швидкість передачі даних 9600 і включаємо маршрутизатор.

При першому запуску маршрутизатора, так як в ньому немає ніякої записаної конфігурації він запускає програму setup, яка за допомогою різних питань сама намагається все налаштувати.

Якщо вибрати «n», перервавши тим самим setup, то необхідно буде вручну налаштувати комутатор з нуля.

Після цього отримаємо доступ до консолі:

R1>

Це командний режим управління маршрутизатором Cisco. Далі переходимо до налаштування, для переходу в привілейований режим вводимо команду:

R1>enable

Далі якщо на маршрутизаторі встановлено пароль з’являється напис «Password» після якого потрібно ввести пароль по стандарту пароль «Cisco» якщо ж паролю немає після натискання клавіші «Ввід» ми потрапляємо в привілейований режим:

R1#

Тепер запрошення на введені змінилося і стало таким «Router#» це означає що ми знаходимося в привілейованому режимі.

Перше що нам потрібно це задати пароль на вхід в привілейований режим:

R1# conf t

R1(config)#enable secrer «Пароль»

R1(config)#exit

R1#

Налаштування параметрів входу:

R1#conf t

R1(config)#line VTY 0 4

R1(config-line)#login

R1(config-line)#password «пароль на вхід»

R1(config-line)#exit

R1(config)#exit

R1#

Для того щоб зберегти конфігурації потрібно ввести команду:

R1#write

Після цього буде виведено напис «Building configuration OK»

Далі будемо налаштовувати IP адреси підмереж, для цього потрібно ввести наступні команди:

R1>enable // вхід в привілейований режим

R1#conf t // вхід в режим конфігурації термінала

Так як ми використовуємо VLAN для розподілу мережі на сегменти потрібно налаштувати на маршрутизаторі підінтерфейс для кожної VLAN, для цього вводимо такі команди:

r_1(config)#interface gigabitEthernet 9/0.2 підключення віртуального порту.

R_1(config-subif)#encapsulation dot1Q 21 підключення інкапсуляції для VILAN 21.

R_1(config-subif)#ip address 192.168.1.200 255.255.255.0 d в подальшому ця адреса буде використовуватися як шлюз для комп’ютерів які віднесені до VILAN 21.

R_1(config-subif)#no shutdown

R_1(config-subif)#exit

Після налаштування інтерфейсів налаштовуємо поділ локальної мережі на підмережі засобами маршрутизаторів. Для маршрутизаторів використовується протокол динамічної маршрутизації RIP версії 2.

Більше про налаштування маршрутизатора і комутатора в додатку А.

4.3 Інструкції з використання тестових наборів та тестових програм

Для перевірки і тестування мережі використовуються тестові програми і утиліти, такі як ping, traceroute.

Ping — це службова комп'ютерна програма, призначена для перевірки з'єднань в мережах на основі TCP/IP.

Для передачі пакетів з віддаленою системою ping використовує протокол ICMP який має наступний вигляд:

ping [ключі] адреса (ім’я) вузла ключі:

t - безперервно відправляє пакети даних, доки команда не буде зупинена командою Ctrl-C;

a – дозволяє використовувати імена замість IP-адрес;

n - дає можливість задати конкретну кількість запитів ;

l довжина – вказує довжину exo – запитів;

f – визначає чи пристрій змінював розмір пакету, забороняє фрагментування пакету,;

i час – встановлює час життя пакету;

v тип – встановлює тип обслуговування (TOS);

r число – відображає шляхи для заданого числа повторних прийомів;

s число – відмічає час для вказаного числа повторних прийомів;

w час – встановлює час в мілісекундах після закінчення якого пакети рахуються втраченим.

Traceroute – команда перевірки, практично така ж як і команда ping. Використовує протокол ICMP щоб визначити всі проміжні вузли, через які проходить пакет по дорозі до вузла призначення. Використовується такий синтаксис :

tracert [ключі] ім’я вузла

ключі :

d – використовувати імена вузлів замість IP адрес;

h максимальне число повторних прийомів – максимально допустиме число повторних прийомів для досягнення мети;

j список вузлів - маршрутизація пакетів через вказані вузли. Послідовні вузли можуть бути розділені шлюзами. Вільний вибір шляху серед систем у вказаному списку;

w час – встановлення часу очікування в мілісекундах.

За допомогою цих команд можна виконати повну діагностику мережі, що дозволяє знайти і виправити більшість поломок в мережі.

4.4 Інструкції по налаштуванню засобів захисту мережі

Маршрутизатор cisco має свій мережевий екран який називається Cisco ASA.

Cisco ASA є апаратним фаєрволом з інспекцією сесій зі збереженням стану (stateful inspection). ASA вміє працювати в двох режимах: routed (режим маршрутизатора, за замовчуванням) і transparent (прозорий міжмережевий екран)

Приклад налаштування:

```
int g0/0
 ip address {адрес} {маска}
 security-level {number}
 nameif {ім’я}
 no shutdown
```

Параметр «рівень безпеки» (security level) - це число від 0 до 100, яке дозволяє порівнювати кілька інтерфейсів і визначити, хто з них більш «безпечний». Параметр використовується якісно, а не кількісно, тобто важливо тільки співставлення «більше-менше». За замовчуванням трафік, що йде «назовні», тобто з інтерфейсу з великим рівнем безпеки на інтерфейс з меншим рівнем безпеки, пропускається, сесія запам'ятовується і назад пропускаються тільки відповіді по цих сесіях.

4.5 Інструкції з експлуатації та моніторингу в мережі

Після закінчення розробки і впровадження в дію мережі залишається лише спостерігати з її роботою. Для правильної оцінки стану мережі адміністратор повинен мати план мережі, тобто її фізичну і логічну топологію, а також знати її характеристики. Моніторинг мережі може проводитись як з робочого місця адміністратора, так і за допомогою функції віддаленого доступу.

Для оцінки стану мережі використовують як апаратні, так і програмні засоби. До апаратних засобів відносять модулі, які підключають до мережі. Наприклад, за допомогою модуля тестування мереж доступу Acterna 2357 можна перевірити синхронізацію в мережах ATM, IP маршрутизацію, проводити тестування термінального устаткування користувача і доступності додатків, перевірити правильність роботи мультиплексорів абонентського доступу (DSLAM), оцінити канали абонентського доступу на фізичному рівні.

До програмних – утиліти і програми, такі як Total Network Monitor 2 MyLanViewer, HyperTerminal Networx Free. Ці програми призначені для тестування і налаштування мереженого обладнання.

MyLanViewer - програма для сканування і моніторингу комп'ютерів в мережі з можливістю пошуку загальнодоступних файлів. Вона показує комп'ютери в зручному для перегляду вигляді, який містить ім'я комп'ютера, IP адреса, MAC адреса, загальні ресурси та інші деталі для кожного комп'ютера. За допомогою якої ви можете стежити за комп'ютерами в мережі і отримувати сповіщення, коли стан одного з них зміниться. Також ви можете управляти своїми загальними ресурсами, забороняти їх і закривати до них сесії.

Можливості MyLan Viewer:

– Багато-потокове сканування, що забезпечують високу швидкість сканування;

– Автоматичне сканування і пошук за розкладом;

– Пошук комп'ютерів в мережі за допомогою: ICMP, ARP, NetBIOS, DNS;

– Сканування NetBIOS, FTP і HTTP ресурсів;

– Пошук файлів в загальних ресурсах за заданими умовами;

– Відкриття знайдених ресурсів в різних програмах;

– Збереження списків всіх раніше знайдених комп'ютерів в мережі;

– Відображення, які комп'ютери включені, а які ні;

– Оприлюднення у разі виключення / включення обраних комп'ютерів;

– Отримання імені комп'ютера по IP-адресі і назад;
– Показує, хто зайшов на ваш комп'ютер, і які файли скачує;
– Збереження звітів в HTML, TXT файлі.

Networx — проста програма, що дозволяє керувати інтернет-трафіком і контролювати швидкість інтернет-з’єднання. Програма працює будь-якими типами з’єднань.

Networx дозволяє перевіряти як вхідний, так і вихідний трафік. Дає можливість переглянути статистику для кожного користувача комп’ютера, статистику за день, тиждень або місяць. Також програма практично не використовує системних ресурсів і споживає лише 25 МБ оперативної пам’яті.

Основні можливості Networx:

– Побудова звіту для кожного користувача в системі.
– Створення статистки за будь які періоди роботи.
– Експорт статистики у таблиці Excel.
– Збереження резервної копії файлів і даних та їх відновлення.
– Тестування і моніторинг швидкості інтернет-з’єднання.
– Контроль використання додатками мережевого трафіку.
– Встановлення обмежень і правил для різного періоду часу.
– Перевірка маршруту пройденого пакетами.

4.6 Моделювання мережі

Моделювання проводиться в програмі Cisco Packet Tracer. Завданням моделювання є конфігурування мережевого обладнання для роботи змодельованої системи та показати можливість обміну трафіком між окремими сегментами мережі.

Засобами моделювання Cisco Packet Tracer змоделюємо мережу так як показано на рисунку 4.12

Налаштовуємо мережу і проводимо перевірку. Щоб перевірити чи правильно налаштовано мережу заходим на один з комп’ютерів і використовуючи консольний порт виконавши команду ping.

В результаті ми отримаємо такий результат.

PC>ping 192.168.22.1

Pinging 192.168.22.1 with 32 bytes of data:

Reply from 192.168.22.1: bytes=32 time=42ms TTL=255

В результаті ми отримаєм повідомлення що всі 4 пакети пройшли по потрібні адресі і все працює правильно.

Ping statistics for 192.168.22.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Якщо ж підключення неправильне тоді в результаті ми отримаємо повідомлення про те, що пакети не пройшли.

В випадку коли ми пінгуєм комп’ютер який налаштовано правильно але він не відноситься до нашої VILAN тоді ми отримуємо повідомлення, що даний комп’ютер недоступний, це буде виглядати так :

Packet Tracer PC Command Line 1.0

PC>ping 192.168.200.1

Pinging 192.168.200.1 with 32 bytes of data:

Reply from 192.168.1.222: Destination host unreachable.

Reply from 192.168.1.222: Destination host unreachable.

Request timed out.

Reply from 192.168.1.222: Destination host unreachable.

Ping statistics for 192.168.200.1:

В результаті всі 4 пакети втрачено і ми отримуємо таке повідомлення:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

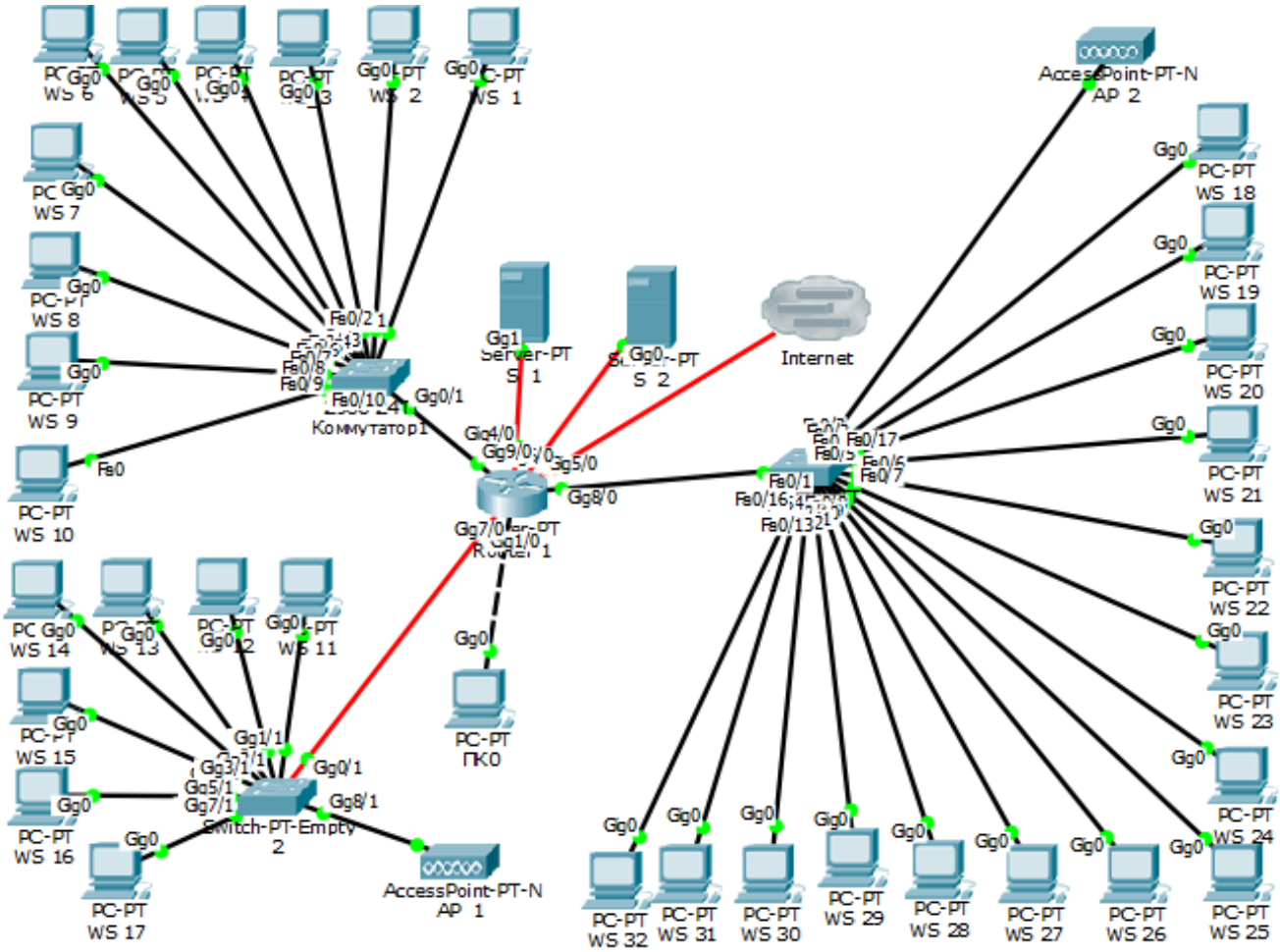

Рисунок 4.12 – Логічна топологія комп’ютерної мережі

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

5.1 Показники частоти та тяжкості травматизму на виробництві.

Метою дослідження виробничого травматизму є розробка заходів по запобіганню нещасних випадків на підприємстві. Для цього необхідно систематично аналізувати і узагальнювати їх причини. Аналіз причин травматизму дозволяє поділяти їх на організаційні, технічні, психофізіологічні та санітарно-гігієнічні.

Організаційні: порушення законодавчих актів з охорони праці, вимог інструкцій, правил і норм, відсутність або неякісне проведення інструктажу і навчання, невиконання заходів щодо охорони праці, невідповідність норм санітарно-гігієнічних факторів, несвоєчасний ремонт або заміна несправного і застарілого обладнання.

Технічні: невідповідність вимогам безпеки або несправність виробничого обладнання, інструменту і засобів захисту, конструктивні недоліки обладнання.

Психофізіологічні: помилкові дії працівника внаслідок втоми, надмірної важкості і напруженості роботи, монотонності праці, хворобливого стану, необережності.

Санітарно-гігієнічні: надмірні рівні шуму, вібрації, несприятливі метеорологічні умови; підвищений вміст у повітрі робочих зон шкідливих речовин; наявність різних випромінювань вище допустимих значень; недостатнє або нераціональне освітлення; порушення правил особистої гігієни та інше.

Найбільш поширеними взаємодоповнюючими методами дослідження виробничого травматизму є статистичний і монографічний. Але сьогодні все більше уваги приділяють економічному, ергономічному та психофізіологічному методам.

Статистичний метод базується на аналізі статистичного матеріалу по травматизму, який накопичений на підприємстві або в галузі за декілька років. Статистичний метод дозволяє всі нещасні випадки і причини травматизму

групувати по статі, віку, професії, стажу роботи потерпілих, часу, місцю, типу нещасних випадків, характеру отриманих травм, виду обладнання. Цей метод дозволяє встановити найбільш поширені види травм по окремим підприємствам, визначити причини, які спричиняють найбільшу кількість нещасних випадків, виявити небезпечні місця, розробити і провести необхідні організаційно-технічні заходи.

При проведенні статистичного аналізу для характеристики рівня виробничого травматизму на підприємстві і в галузі використовують кількісні і якісні відносні показники, засновані на вивченні первинних документів про травматизм. Коефіцієнт частоти травматизму Кч розраховується на 1000 працюючих: Кч = (А х 1000) / Б, де А – загальна кількість нещасних випадків на підприємстві за обліковий період, Б – загальна чисельність працюючих на підприємстві за той самий обліковий період.

Тобто, коефіцієнт частоти травматизму Кч - це кількість нещасних випадків або профзахворювань, які сталися у відповідний період часу (півріччя, рік), на 1000 працюючих.

Якісний показник травматизму Кт, або коефіцієнт тяжкості травматизму (нещасних випадків), характеризує середню втрату працездатності в днях, що припадають на одного потерпілого за звітний період: кт-д/н, де Д - сумарне число днів непрацездатності всіх потерпілих, які втратили працездатність на добу і більше під час звітного періоду.

До цього показника не включаються випадки стійкої втрати працездатності, що не закінчилася за звітний період, і тому він повністю не характеризує тяжкості травматизму. Тобто, коефіцієнт тяжкості нещасних випадків - це середня довготривалість непрацездатності одного потерпілого, яка виражена в робочих днях за відповідний звітний період (півріччя, рік). Крім цих показників, застосовується показник, за яким визначається кількість втрачених через травми робочих днів, що припадають на 1000 працюючих. Його називають коефіцієнтом мінімальних матеріальних збитків або коефіцієнтом трудових втрат. Він підраховується як добуток двох вищенаведених показників: Ктв = Кч-Кт = 1000

Д/С. Різновидами статистичного методу є груповий і топографічний методи. При груповому методі травми групуються за окремими однорідними ознаками: часу травмування, кваліфікації; спеціальності і віку потерпілого; видам робіт; причинам нещасних випадків та інші. Це дозволяє визначити найбільш несприятливі ділянки в організації робіт та фактичний стан умов праці в цеху, на підприємстві.

При топографічному методі всі нещасні випадки систематично наносять умовними знаками на плані розташування обладнання у цеху або на ділянці. Накопичення таких знаків на позначці робочого місця або обладнання характеризує його підвищену небезпечність і потребує відповідних профілактичних заходів.

Монографічний метод являє собою аналіз небезпечних і шкідливих виробничих факторів, які властиві технологічному процесу, обладнанню, ділянці виробництва. За цим методом поглиблено аналізуються всі обставини нещасних випадків і, за необхідності, виконуються відповідні дослідження та випробування. Цей метод дозволяє не тільки проаналізувати нещасні випадки, що сталися, а й виявити потенційні небезпечні фактори, які існують на ділянці технологічного процесу або обладнання, що вивчається, а також використати отримані результати при проектуванні виробництва та для розробки заходів з охорони праці.

Економічний метод полягає в визначенні економічної шкоди від заподіяного травматизму, визначенні економічної ефективності від затрат на розробку та впровадження заходів з охорони праці. Цей метод не дозволяє виявити причини травматизму і тому застосовується як доповнення до інших методів.

Ергономічний метод ґрунтується на комплексному вивченні системи "людина - машина - виробниче середовище". Відомо, що кожному виду трудової діяльності відповідають визначені фізіологічні, психофізіологічні і психологічні якості людини, а також її антропометричні дані. Тому при комплексній відповідності вказаних властивостей людини до конкретної трудової діяльності можлива ефективна і безпечна робота. Порушення відповідності може призвести до нещасного випадку.

При такому аналізі травматизму слід враховувати, що здоров'я і працездатність людини залежать від біологічних ритмів функціонування організму

під впливом геліогеофізичних явищ. Дія таких явищ, як іонізація атмосфери, магнітне і гравітаційне поле Землі, активність Сонця, гравітація Місяця та інші, викликає відповідні зміни в організмі людини, що змінюють її поведінку. Це може призвести до зниження сприйняття змін у навколишньому середовищі і до нещасних випадків.

5.2 Забезпечення електробезпеки користувачів ПК

Приміщення із робочими місцями користувачів комп'ютерів для забезпечення електробезпеки обладнання, а також для захисту від ураження електричним струмом самих користувачів ПК повинні мати достатні технічні засоби захисту відповідно до ГОСТ 12.1.009-76, НПАОП 40.1-1.07-01 "Правила експлуатації електрозахисних засобів", НПАОП 40.1-1.21-98 "Правила безпечної експлуатації електроустановок споживачів", НПАОП 40.1-1.32-01 "Правила будови електроустановок. Електрообладнання спеціальних установок"

З метою запобігання ушкодженням, що можуть статися через ураження електричним струмом, загоряння, коротке замикання тощо, розроблено загальний стандарт безпеки IEC 950. Загальним стандартом електробезпечності для країн Європейської співдружності є Cemark.

Під час проектування систем електропостачання, монтажу силового електрообладнання та електричного освітлення будівель та приміщень для ПЕОМ необхідно дотримуватись вимог вищеназваних нормативно-правових актів, а також СН 357-77 "Инструкция по проектированию силового осветительного оборудования промышленных предприятий", затверджених Держбудом СРСР, ГОСТу 12.1.006, ГОСТу 12.1.030 "ССБТ. Электробезопасность. Защитное заземление, зануление", ГОСТу 12.1.019 "ССБТ. Электробезопасность. Общие требования и номенклатура видов защиты", ГОСТу 12.1.045, ВСН 59-88 Держкомархітектури СРСР "Электрооборудование жилых и общественных зданий. Нормы проектирования", Правил пожежної безпеки в Україні, ДСанПіН 3.3.2.007-

98, розділів СНиП, що стосуються штучного освітлення і електротехнічних пристроїв, та вимог нормативно-технічної і експлуатаційної документації заводу-виробника ПЕОМ.

ЕОМ, периферійні пристрої ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ, інше устаткування (апарати управління, контрольно-вимірювальні прилади, світильники тощо), електропроводи та кабелі за виконанням та ступенем захисту мають відповідати класу зони за ПУЕ, мати апаратуру захисту від струму короткого замикання та інших аварійних режимів.

Під час монтажу та експлуатації ліній електромережі необхідно повністю унеможливити виникнення електричного джерела загоряння внаслідок короткого замикання та перевантаження проводів, обмежувати застосування проводів з легкозаймистою ізоляцією і, за можливості, перейти на негорючу ізоляцію.

Лінія електромережі для живлення ЕОМ, периферійних пристроїв ЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ виконується як окрема групова трипровідна мережа, шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів.

Використання нульового робочого провідника як нульового захисного провідника забороняється. Нульовий захисний провід прокладається від стійки групового розподільчого щита, розподільчого пункту до розеток живлення. Не допускається підключення на щиті до одного контактного затискача нульового робочого та нульового захисного провідників. Площа перерізу нульового робочого та нульового захисного провідника в груповій трипровідній мережі повинна бути не менше площі перерізу фазового провідника.

Усі провідники повинні відповідати номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу провідників, температурному режиму та типам апаратури захисту, вимогам ПУЕ.

У приміщенні, де одночасно експлуатується або обслуговується більше п'яти персональних ЕОМ, на помітному та доступному місці встановлюється аварійний

резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення.

ПЕОМ, периферійні пристрої ПЕОМ та устаткування для обслуговування, ремонту та налагодження ЕОМ повинні підключатися до електромережі тільки з допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення. Штепсельні з'єднання та електророзетки крім контактів фазового та нульового робочого провідників повинні мати спеціальні контакти для підключення нульового захисного провідника. Конструкція їх має бути такою, щоб приєднання нульового захисного провідника відбувалося раніше ніж приєднання фазового та нульового робочого провідників. Порядок роз'єднання при відключенні має бути зворотним. Необхідно унеможливити з'єднання контактів фазових провідників з контактами нульового захисного провідника.

Неприпустимим є підключення ПЕОМ та периферійних пристроїв ПЕОМ до звичайної двопровідної електромережі, в тому числі – з використанням перехідних пристроїв.

Електромережі штепсельних з'єднань та електророзеток для живлення ПЕОМ, периферійних пристроїв слід виконувати за магістральною схемою, по 3…6 з’єднань або електророзеток в одному колі. Штепсельні з'єднання та електророзетки для напруги 12 В та 36 В за своєю конструкцією повинні відрізнятися від штепсельних з'єднань для напруги 127 В та 220 В і мають бути пофарбовані в колір, який візуально значно відрізняється від кольору штепсельних з'єднань, розрахованих на напругу 127 В та 220 В.

Індивідуальні та групові штепсельні з'єднання та електророзетки необхідно монтувати на негорючих або важкогорючих пластинах з урахуванням вимог ПУЕ та Правил пожежної безпеки в Україні.

Електромережу штепсельних розеток для живлення ПЕОМ, периферійних пристроїв ПЕОМ при розташуванні їх уздовж стін приміщення прокладають по підлозі поряд зі стінами приміщення, як правило, в металевих трубах і гнучких металевих рукавах з відводами відповідно до затвердженого плану розміщення обладнання та технічних характеристик обладнання.

При розташуванні в приміщенні за його периметром до 5 ПЕОМ, використанні трипровідникового захищеного проводу або кабелю в оболонці з негорючого або важкогорючого матеріалу дозволяється прокладання їх без металевих труб та гнучких металевих рукавів.

Електромережу штепсельних розеток для живлення ПЕОМ при розташуванні їх у центрі приміщення, прокладають у каналах або під знімною підлогою в металевих трубах або гнучких металевих рукавах. При цьому не дозволяється застосовувати провід і кабель в ізоляції з вулканізованої гуми та інші матеріали, що містять сірку. Відкрита прокладка кабелів під підлогою забороняється. Металеві труби та гнучкі металеві рукави повинні бути заземлені. Заземлення повинно відповідати вимогам НПАОП 40.1-1.21-98.

Для підключення переносної електроапаратури застосовують гнучкі проводи в надійній ізоляції.

Тимчасова електропроводка від переносних приладів до джерел живлення виконується найкоротшим шляхом без заплутування проводів у конструкціях машин, приладів та меблях. Доточувати проводи можна тільки шляхом паяння з наступним старанним ізолюванням місць з'єднання.

Є неприпустимими:

– експлуатація кабелів та проводів з пошкодженою або такою, що втратила захисні властивості за час експлуатації, ізоляцією; залишення під напругою кабелів та проводів з неізольованими провідниками;

– застосування саморобних подовжувачів, які не відповідають вимогам ПВЕ до переносних електропроводок;

– застосування для опалення приміщення нестандартного (саморобного) електронагрівального обладнання або ламп розжарювання;

– пошкодженими розетками, розгалужувальними та з'єднувальними коробками, вимикачами та іншими електровиробами, а також лампами, скло яких має сліди затемнення або випинання;

– підвішування світильників безпосередньо на струмопровідних проводах, обгортання електроламп і світильників папером, тканиною та іншими горючими матеріалами, експлуатація їх зі знятими ковпаками (розсіювачами);

– використання електроапаратури та приладів в умовах, що не відповідають вказівкам (рекомендаціям) підприємств-виготовлювачів.

ВИСНОВКИ

Проект містить детальний аналіз використаних технологій та опис побудови проекту і всіх його складових. Результатом виконання є повний пакет документації та листів, які дозволяють легко впровадити проект.

У кожному з розділів описано певний вид робіт, або певне обладнання, яке необхідне для монтажу мережі і її подальшого обслуговування.

В першому розділі дипломного проекту розглянуто сутність призначення, класифікація, основні види комп'ютерних мереж та способи передачі даних.

В другому розділі охарактеризовано відділи організації, вибрано топологію мережі. Було прийнято рішення будувати мережу на базі розширеної зірки. Тут підібрано пасивне та активне обладнання. В якості середовища передачі даних вибрано кабель виту пару категорії 6. роль центрального вузла мережі призначена гігабітному маршрутизатору Cisco ASR1001-X. Комутатори рівня доступу – гігабітні керовані комутатори Cisco Catalyst WS-C2960S. В цьому ж розділі розглянуто особливості монтажу та тестування кабельної частини мережі

За результатами виконання другого розділу розроблено логічну та фізичну топології мережі, які подані на окремих плакатах в графічній частині.

В третьому розділі приведено інструкцію з налаштування активного комутаційного обладнання, описані способи використання тестових утиліт, розроблено інструкцію з експлуатації та моніторингу мережі.

В четвертому розділі проведено математичне моделювання середнього часу функціонування системи без збоїв на основі журналу спостережень даної мережі.

В п'ятому розділі описані питання охорони праці та техніки безпеки при роботі з обчислювальним обладнанням.

Таким чином даний дипломний проект являє собою цілісний комплекс документації по проектуванню та введенню в експлуатацію інформаційно забезпечення комп'ютерної мережі ТОВ «TV-4».

ПЕРЕЛІК ПОСИЛАНЬ

1. Антонов В. М. Сучасні комп'ютерні мережі. _ К.: "МК-Прес", 2005. _480 с., іл. і

2. Буров Є. Комп'ютерні мережі, 2-е видання. - БаК, 2004. - 584 с.: іл.

3. Ватаманюк А. И. Создание, обслуживание и администрирование сетейна 100%. _ СПб. : Питер , 2010. _ 288 с.

4. Додонов О. Г., Ланде Д. В., Путятін В. Г. Інформаційні потоки в глобальних комп”ютерних мережах. _ К.: Наук, думка, 2009. - 295 с

5. Жидецький В. Ц. Джигерей В. С. Сторожук В. М Практикум із охорони праці Львів: Афіша, 2000. – 349 с.

6. Жуков І.А., Дрововозов В.І., Махновський Б.Г. Експлуатація комп'ютерних систем та мереж. - К.: НАУ, 2007. - 361 с.

7. Іртегов Д.В. Введення в мережні технології, К., 2014.

8. Кузин А.В. Компьютерные сети. М.: Форум: Инфра-М, 201 1. - 192с.

9. Микитишин А.Г., Митник М.М., Стухляк П.Д., В.В. Пасічник Компіютерні мережі [навчальний посібник] - Львів, «Магнолія 2006», 2013. - 256 с.

10. Николайчук Я.М., Возна Н.Я., Пітух І.Р. Проектування спеціалізованих

11. Комп’ютерних систем. Навчальний посібник. - Тернопіль: ТзОВ “Терно-граф”, 2010. - 3940.

12. Новожилов Е.О., Новожилов О.П. Компьютерные сети. 4-е изд. _ Москва: Академия, 2014. - 224 с.

13. Олексюк В., Балик Н., Балик А. Організація компютерної локальної

14. мережі. - Видавництво: -Тернопілы «Підручники та посібники», 2006. - 80 с.

ДОДАТОК А

Налаштування маршрутизатора і комутаторів

Для налаштування динамічної маршрутизації потрібно ввести такі команди:

R1(config)#router rip // налаштування rip

R1(config-router)#version 2 // вибираємо версію rip.

R1(config-router)#network 192.168.1.0 // записуємо адреси під мереж підключених безпосередньо до маршрутизатора

R1(config-router)#exit

R1(config)#exit // виходимо

R1#write // зберігаємо конфігурації.

В результаті ми буде мати такі налаштування маршрутизатора:

interface GigabitEthernet0/0

no ip address

interface GigabitEthernet1/0

no ip address

interface GigabitEthernet1/0.210

encapsulation dot1Q 210

interface GigabitEthernet1/0.211

encapsulation dot1Q 211

ip address 192.168.211.200 255.255.255.0

interface GigabitEthernet1/0.214

encapsulation dot1Q 214

ip address 192.168.214.200 255.255.255.0

interface GigabitEthernet1/0.315

encapsulation dot1Q 315

no ip address

interface GigabitEthernet1/0.317

encapsulation dot1Q 317

```
no ip address
interface GigabitEthernet1/0.320
encapsulation dot1Q 320
no ip address
interface GigabitEthernet2/0
no ip address
interface GigabitEthernet3/0
no ip address
shutdown
interface GigabitEthernet4/0
ip address 192.168.4.1 255.255.255.0
interface GigabitEthernet5/0
ip address 192.168.5.1 255.255.255.0
interface GigabitEthernet6/0
ip address 192.168.6.1 255.255.255.0
interface GigabitEthernet7/0
ip address 192.168.22.1 255.255.255.0
duplex auto
speed auto
interface GigabitEthernet8/0
ip address 192.168.3.1 255.255.255.0
duplex auto
speed auto
interface GigabitEthernet8/0.115
encapsulation dot1Q 315
ip address 192.168.115.200 255.255.255.0
interface GigabitEthernet8/0.117
encapsulation dot1Q 117
ip address 192.168.117.200 255.255.255.0
interface GigabitEthernet8/0.120
```

encapsulation dot1Q 320

ip address 192.168.120.200 255.255.255.0

interface GigabitEthernet8/0.320

no ip address

interface GigabitEthernet8/0.324

encapsulation dot1Q 324

ip address 192.168.124.200 255.255.255.0

interface GigabitEthernet9/0

no ip address

duplex auto

speed auto

interface GigabitEthernet9/0.2

encapsulation dot1Q 21

ip address 192.168.1.222 255.255.255.0

interface GigabitEthernet9/0.22

encapsulation dot1Q 22

ip address 192.168.122.200 255.255.255.0

interface GigabitEthernet9/0.27

encapsulation dot1Q 27

ip address 192.168.27.200 255.255.255.0

router rip

version 2

network 192.168.0.0

network 192.168.4.0

network 192.168.22.0

Налаштування комутатора виконується так само як і маршрутизатор з допомогою консольного кабелю і програми huperterminal.

Для початку налаштовуємо пароль на вхід:

Sw1#conf t

Sw1(config)#line VTY 0 4

Sw1(config-line)#login

Sw1(config-line)#pssword

Sw1(config-line)#exit

Sw1(config)#exit

Для створення vlan вводимо такі команди:

Sw1 (config)#interface GigabitEthernet0/1 вибір порту який буде налаштовуватися

Sw1 (config-if)#switchport access vlan 21 установка номеру VLAN вибраного порту

Sw1 (config-if)#exit

Sw1 (config)#interface GigabitEthernet0/2

Sw1 (config-if)#switchport access vlan 22

Sw1 (config-if)#exit

Налаштування портів для зв’язку між комутаторами і маршрутизаторами.

Для зв’язку між різними підмережами на комутаторах порти які безпосередньо підключенні до маршрутизатора порт налаштовується в режимі trunk це дозволить всім підмережам даного маршрутизатора здійснювати передачу даних через даний порт.

Наприклад:

Sw1 (config)#interface GigabitEthernet0/2

Sw1 (config-if)#switchport trunk

В результаті отримуємо такі налаштування:

Налаштування комутатора SW_1

spanning-tree mode pvst

interface FastEthernet0/1

switchport access vlan 21

switchport mode access

interface FastEthernet0/2

switchport access vlan 22

interface FastEthernet0/3

switchport access vlan 22

interface FastEthernet0/4

switchport access vlan 22

interface FastEthernet0/5

switchport access vlan 22

interface FastEthernet0/6

switchport access vlan 22

interface FastEthernet0/7

switchport access vlan 22

interface FastEthernet0/8

switchport access vlan 27

interface FastEthernet0/9

switchport access vlan 27

interface FastEthernet0/10

switchport access vlan 27

interface FastEthernet0/11

switchport access vlan 210

interface FastEthernet0/12

switchport access vlan 210

interface FastEthernet0/13

switchport access vlan 210

interface GigabitEthernet0/1

switchport mode trunk

interface GigabitEthernet0/2

switchport mode trunk

interface Vlan1

Налаштування комутатора SW_2

spanning-tree mode pvst

interface GigabitEthernet0/1

switchport mode trunk

interface GigabitEthernet1/1

switchport access vlan 21

interface GigabitEthernet2/1

switchport access vlan 210

interface GigabitEthernet3/1

switchport access vlan 210

interface GigabitEthernet4/1

switchport access vlan 211

interface GigabitEthernet5/1

switchport access vlan 211

interface GigabitEthernet6/1

switchport access vlan 211

switchport access vlan 214

interface Vlan1

no ip address

shutdown

line con 0

line vty 0 4

Налаштування комутатора SW_3

spanning-tree mode pvst

interface FastEthernet0/1

switchport mode trunk

interface FastEthernet0/2

witchport access vlan 315

interface FastEthernet0/3

switchport access vlan 315

interface FastEthernet0/4

switchport access vlan 317

interface FastEthernet0/5

switchport access vlan 317

interface FastEthernet0/6
switchport access vlan 317
interface FastEthernet0/7
switchport access vlan 317
interface FastEthernet0/8
switchport access vlan 317
interface FastEthernet0/9
switchport access vlan 317
interface FastEthernet0/10
interface FastEthernet0/11
interface FastEthernet0/12
switchport access vlan 324
interface FastEthernet0/13
switchport access vlan 324
interface FastEthernet0/14
witchport access vlan 320
interface FastEthernet0/15
switchport access vlan 320
interface FastEthernet0/16
switchport access vlan 320