

Форма № 24

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет радіоелектроніки та телекомунікацій
(повне найменування інституту, факультету)

Мікро – та наноелектроніки
(повне найменування кафедри)

Пояснювальна записка

до магістерської роботи

магістр

(ступінь вищої освіти)

на тему «Розробка локально-обчислювальної мережі підприємства роздрібної торгівлі з використанням багаторівневого комутатора Dell N4032F»

Виконав: студент VI курсу, групи РТз-319м
Спеціальності 153 – «Мікро- та наносистемна техніка»

(код і найменування спеціальності)

Освітня програма (спеціалізація) «Мікро- та наноелектронні прилади і пристрої»

Борщ Ю. С.

(прізвище та ініціали)

Керівник Сніжної Г.В.

(прізвище та ініціали)

Рецензент _____

(прізвище та ініціали)

2020р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»
(повне найменування закладу вищої освіти)

Інститут, факультет Радіoeлектроніки та телекомунікації
Кафедра Мікро та нанoeлектроніки
Ступінь вищої освіти магістр
Спеціальність 153 «Мікро- та наносистемна техніка»
(код і найменування)
Освітня програма (спеціалізація) «Мікро- та нанoeлектронні прилади і пристрої»
(назва освітньої програми (спеціалізації))

ЗАТВЕРДЖУЮ

Завідувач кафедри
мікро- та нанoeлектроніки
В. В. Погосов
« » 2020 року

ЗАВДАННЯ
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТА

Борща Юрія Сергійовича

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Розробка локально-обчислювальної мережі підприємства роздрібної торгівлі з використанням багаторівневого комутатора Dell N4032F

керівник проекту (роботи) Сніжної Геннадій Валентинович,
доктор технічних наук, професор

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом закладу вищої освіти №«334» від 13.11. 2020 року

2. Строк подання студентом проекту (роботи) 28 грудня 2020 року

3. Вихідні дані до проекту (роботи) багаторівневий комутатор Dell N4032F, технологія Fast Ethernet, метод доступу CSMA/CD, топологія «зірка»

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Розглянути переваги та недоліки хмарних технологій та локально серверних рішень. Вибрати найбільш відповідне обладнання, та програмне забезпечення для збільшення працездатності підприємства та пропускної здатності активного обладнання.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
14 аркушів А4 презентації

Г.В. Сніжной

АНОТАЦІЯ

ПЗ: 109 с., 25 рисунків, 8 табл., 10 додатків, 23 джерела.

Мета роботи: Розробка локально-обчислювальної мережі підприємства роздрібною торгівлі з використанням багаторівневого комутатора Dell N4032F.

Об'єкт: багаторівневий комутатор Dell N4032F.

Предмет: оптимізація роботи локальної мережі.

Методи дослідження: розрахунково-аналітичний.

Результати: результатом дослідження є модернізація існуючої локальної мережі на підприємстві.

Рекомендації щодо впровадження: результати роботи можуть бути використані при виборі апаратного та програмного забезпечення серверних систем, локальних мереж та поліпшенню роботи Ethernet.

Результати: Розроблено приклад модернізації локально обчислювальної мережі на підприємстві.

Практична цінність: проведено аналітичне дослідження придатності та вигідності обладнання для модернізацій локальної мережі.

ЛОМ, МЕРЕЖІ, СЕРВЕР, МАРШРУТИЗАТОР, СВІТЧ, ЗАСТАВА,
ETHERNET, СКС, DELL N4032F

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	8
ВСТУП	9
1 ОГЛЯД ХМАРНОЇ ТЕХНОЛОГІЇ ТА ЛОКАЛЬНИХ СЕРВЕРІВ	11
1.1 Хмарні технології.....	11
1.1.1 Послуги, що надаються хмарними системами.....	12
1.1.2 Можливості хмарних обчислень	15
1.1.3 Хмарні технології - погляд з боку користувача	18
1.1.4 Хмарні технології та зберігання даних	19
1.2 Мережа на основі сервера	21
1.2.1 Локальний сервер - швидкість і доступність	24
1.3 Поняття структурованої кабельної системи.....	26
1.3.1 Горизонтальна підсистема СКС	27
1.3.2 Вертикальна (або магістральна) підсистема СКС	28
1.3.3 Підсистема робочого місця	30
2 ВИБІР АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ	32
2.1 Вибір активного обладнання.....	32
2.1.1 Вибір мережевого адаптера для робочих станцій.....	32
2.1.2 Вибір мережевого адаптера для сервера.....	33
2.1.3 Вибір мережевого сервера.....	34
2.1.4 Вибір джерела безперебійного живлення.....	36
2.1.5 Вибір комутаторів	36
2.1.6 Вибір маршрутизатора.....	39
2.1.7 Вибір модему	40

2.1.8 Вибір оптичного конвертора.....	40
2.1.9 Вибір міні АТС	41
2.1.10 Вибір VoIP – шлюзу.....	42
2.2 Вибір пасивного обладнання	44
2.2.1 Вибір телекомунікаційних шаф.....	44
2.2.2 Вибір полиць.....	46
2.2.3 Вибір оптичного кросу	47
3 РОЗРОБКА МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ТА КОНФІГУРУВАННЯ ПРОГРАМНИХ ЗАСОБІВ	48
3.1 Проектування локальної мережі на базі технології Fast Ethernet	48
3.1.1 Методика проектування локальної мережі	48
3.1.2 Вибір мережевої технології.....	49
3.1.3 Вибір мережевої топології	50
3.1.4 Розробка горизонтальної кабельної підсистеми	53
3.2 Конфігурування програмних засобів	55
3.2.1 Операційна система для серверів	55
3.2.2 Операційна система для робочих станцій	56
3.2.3 Мережеві служби	57
4 ТЕХНІКО-ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ	64
4.1 Розрахунок капітальних витрат	64
4.2 Розрахунок основних виробничих фондів.....	66
4.3 Розрахунок експлуатаційних витрат	66
5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА У НАДЗВИЧАЙНИХ СИТУАЦІЯХ	70
5.1 Аналіз потенційних небезпек.....	70
5.2 Заходи по забезпеченню техніки безпеки.....	71

5.3 Заходи з виробничої санітарії та гігієни праці.....	75
5.4 Заходи безпеки у надзвичайних ситуаціях.....	84
5.4.1 Заходи з пожежної безпеки.....	84
5.4.2 Заходи з цивільного захисту.....	86
ВИСНОВКИ.....	87
ПЕРЕЛІК ПОСИЛАНЬ.....	88
Додаток А.....	90
Додаток Б.....	91
Додаток В.....	94
Додаток Г.....	97
Додаток Ґ.....	100
Додаток Д.....	103
Додаток Е.....	104
Додаток Є.....	107
Додаток Ж.....	108
Додаток З.....	109

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

FTP – file transfer protocol – протокол передачі файлів

БД – база даних

ДБЖ – джерело безперебійного живлення

ЛМ – локальна мережа

ЛОМ – локальна обчислювальна мережа

ЛПБ – локальна політика безпеки

ОС – операційна система

ПЗ – програмне забезпечення

ПК – персональний комп'ютер

СКС – структурована кабельна система

СУБД – система управління базою даних

ВСТУП

В кінці 20 і початку 21-го століть почалося бурхливе зростання комп'ютерних мереж. Ця тенденція ілюструється швидким зростанням мережі Інтернет, яка захопила всі країни світу. Локальні мережі - це основа автоматизації будь-якого підприємства або фірми. Розподілені мережі проникли в усі сфери діяльності людини, економіку, освіту, культуру і т.д. Сучасні мережі надають користувачам широкий набір послуг, включаючи передачу факсимільних і голосових повідомлень, електронну пошту, службу новин та інші послуги. На основі цих мереж реалізується: дистанційне навчання, телеконференції, телемедицина і т.д. В даний час успіх будь-якого підприємства пов'язаний з інформаційними системами, які базуються на локальних обчислювальних мережах. Системи документообігу, управління базами даних, підтримки прийняття рішень - все це технології, що збільшують ефективність роботи будь-якого підприємства, проте вони не приносять користі, якщо не об'єднані в єдину локальну мережу. Локальна мережа повинна бути надійно захищена і при цьому не повинна створювати незручності для користувачів і адміністраторів мережі. Метою даного проекту є створення обчислювальної мережі на базі технології FastEthernet. Необхідно об'єднати в локальну мережу 71 комп'ютер, всі вони знаходяться в 1 будинку, з можливістю комутації та розвитку. Реалізація проекту забезпечить проходження потоків внутрішньої інформації, дозволить скоротити паперовий документообіг, скоротить час на обробку інформації, прискорить доступ до баз даних, підвищить продуктивність праці і дасть доступ до роботи із загальними пристроями: принтерами, факсами та іншої периферією. Проектована мережа повинна відповідати наступним загальним вимогам:

- побудова деякого ядра мережі з подальшим збільшенням вузлів і нарощуванням сервісів;
- запас продуктивності і можливість переходу до нових технологій без модернізації кабельної підсистеми;

- мережа повинна мати високий ступінь захищеності і безпеки, тобто всі мережеві ресурси повинні бути захищені від несанкціонованого доступу;

- мережа повинна цілодобово працювати незалежно від неполадок електромережі;

- кабельна мережа повинна будуватися з урахуванням зростання трафіку з терміном експлуатації 5-10 років. Кабельна система повинна забезпечувати можливість переходу на інші більш швидкі протоколи;

- в якості програмних засобів повинні використовуватися максимально стандартизовані рішення;

- локальна обчислювальна мережа повинна ґрунтуватися на єдності інтерфейсів користувачів, прозорості доступу до інформації, можливості організувати ефективний пошук доменів, простоті експлуатації системи;

- в кінцевому варіанті ми можемо отримати локальну мережу, з двома стековими 10G комутаторами N4032F, в якому буде 24 фіксовані порти 10GbE SFP+ з автоматичним розпізнаванням параметрів підключень(10 або 1 Гбіт/с) на кожному.

1 ОГЛЯД ХМАРНОЇ ТЕХНОЛОГІЇ ТА ЛОКАЛЬНИХ СЕРВЕРІВ

1.1 Хмарні технології

За останні роки, ця тема, стала однією з найбільш популярних в ІТ-сфері, про неї написано чимало статей, проведено ще більшу кількість конференцій, а скільки рішень вже існує на ринку (і на всю використовується нами в повсякденному житті, часом навіть несвідомо), так і взагалі не злічити.

Однак, як завжди, є одне "але", а саме, велика частина користувачів, як і раніше і знати не знають, що це за «ноу-хау» хмарні технології і для чого воно, взагалі здалося. Що ж, будемо виправляти становище і почнемо ми, як і годиться, з теорії.

Хмарні обчислення (cloud computing) - це розподілена обчислювальна технологія, яка надає користувачеві обчислювальні ресурси та функціонує як послуга Інтернету. Іншими словами - це, в певному сенсі, робоче місце в Інтернеті або на віддаленому сервері.

Розглянемо приклад, що практично кожен з нас, так чи інакше, вже стикався з цим рішенням.

Електронна пошта (e-mail). Якщо ви працюєте з електронною поштою на веб-службі (наприклад, Gmail), яка дозволяє вам використовувати ці електронні листи, це просто хмарний сервіс, який є частиною хмарних технологій. Або обробка зображень, наприклад.

Якщо ви зменшите розмір, перевернете зображення у Photoshop або будь-яку іншу конкретну програму, ви не маєте нічого спільного з хмарною технологією - все відбувається і обробляється локально на вашому комп'ютері. І ось, якщо ви завантажили зображення через службу Picasa, наприклад, і обробляєте цю партію у браузері, це «хмара».



Рисунок 1.1 – Структура хмарного сервісу

1.1.1 Послуги, що надаються хмарними системами

Все, що стосується з cloud computing (далі CC), зазвичай прийнято називати словомaaS . Розшифровується це простий про - " as a Service ", тобто "як сервіс", або "у вигляді сервісу".

В даний час хмарні технології і, власне, їх концепція, передбачає надання наступних типів послуг своїм користувачам:

- Storage-as-a-Service ("зберігання як сервіс"). Це, мабуть, самий простий з CC-сервісів , що представляє собою дисковий простір на вимогу. Кожен з нас коли-небудь стикався з ситуацією, коли на моніторі з'являлось зловісне попередження: "Логічний диск заповнений, щоб звільнити місце, видаліть непотрібні програми або дані".

- Послуга Storage - as -a- Service - дає можливість зберігати дані у "хмарі" у зовнішній пам'яті. Для вас це схоже на додатковий логічний диск або папку. Послуга є фундаментальною для інших, оскільки є частиною кожного з них. Одним із прикладів є Google Drive та інші подібні сервіси.

- Database - as -a- Service ("база даних як сервіс"). Це більше призначено для адміністраторів, оскільки дозволяє працювати з базою даних так, ніби база даних була встановлена на локальних ресурсах. Крім того, у цьому випадку дуже легко «ділитися» проектами між різними суб'єктами, не кажучи вже про кількість комп'ютерного обладнання та ліцензій, необхідних для правильного використання СУБД у великій або навіть середній організації. Гроші можна заощадити.

- Information - as -a- Service ("інформація як сервіс"). Дозволяє віддалено використовувати всі типи інформації, які можуть змінюватися щохвилини або навіть кожної секунди, в залежності від налаштувань.

- Process - as -a- Service ("управління процесом як сервіс"). Віддалений ресурс, який може поєднувати декілька ресурсів (наприклад, послуги чи дані в одній «хмарі» або інших доступних «хмарах») для створення єдиного бізнес-процесу.

- Application - as -a- Service ("додаток як сервіс"). Також, як його ще називають, Software - as -a- Service ("програмне забезпечення як сервіс"). Він позиціонується як «програмне забезпечення на вимогу», яке розгортається на віддалених серверах і доступне всім користувачам через Інтернет. Усі оновлення та ліцензії цього програмного забезпечення охоплюються цією послугою. Регулюється постачальником. У цьому випадку оплата здійснюється за фактичне використання останнього. Прикладом є Документи Google, Календар Google тощо. Інтернет-програма.

- Platform - as -a- Service ("платформа як сервіс"). Користувачеві надається комп'ютерна платформа з встановленою операційною системою та програмним забезпеченням.

- Integration - as -a- Service ("інтеграція як сервіс"). Це можливість отримувати повний пакет інтеграції від "Хмари", який включає програмний інтерфейс між програмами та управління їх алгоритмами. Сюди входять провідні послуги та функції пакету інтеграції для централізованих послуг,

оптимізації та корпоративних програм (EAI), але вони надаються як "хмарна" послуга.

- Security - as -a- Service ("безпека як сервіс"). За допомогою цього типу послуг користувачі можуть миттєво розробляти продукти, що забезпечують безпечне використання веб-технологій, електронної пошти та локальних мереж, щоб користувачі послуги могли розгорнути власні системи безпеки.

- Management / Governace - as -a- Service ("адміністрування та управління як сервіс"). Дає можливість управління та налаштування параметрів однієї або декількох "хмарних" служб. В основному це такі параметри, як топологія, використання ресурсів, віртуалізація.

- Infrastructure - as -a- Service ("інфраструктура як сервіс"). Користувачеві надається комп'ютерна інфраструктура, як правило, підключена до мережі віртуальна платформа (комп'ютер), яку він налаштовує для своїх цілей.

- Testing - as -a- Service ("тестування як сервіс"). Надає можливість тестувати локальні або «хмарні» системи за допомогою тестового програмного забезпечення з «хмари» (обладнання та програмне забезпечення в компанії не потрібні).

Для наочності, узагальнимо всі ці сервіси архітектури «хмара», в одну схему за якою і криються хмарні технології.

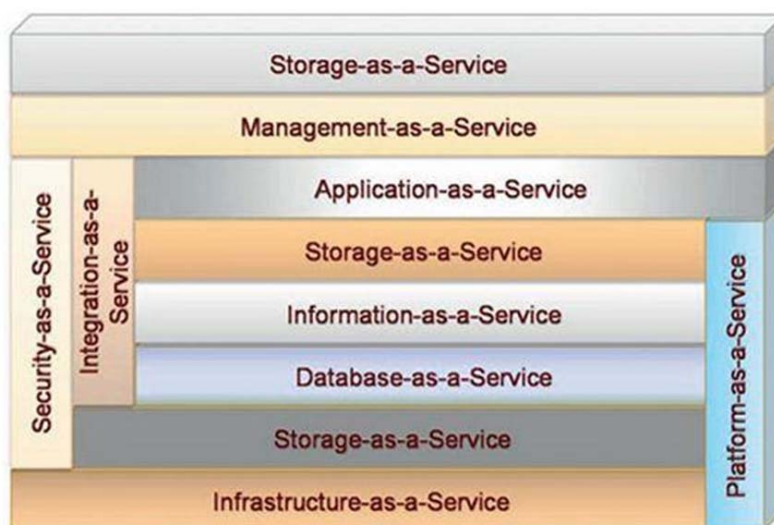


Рисунок 1.2 – Класифікація сервісів, за типом послуг

Тепер розглянемо, які бувають хмарні технології, так би мовити, за формою власності. Тут, виділяють три їх категорії:

- Публічна хмара - це IT-інфраструктура, яка одночасно використовується багатьма компаніями та службами. Користувачі не можуть керувати та підтримувати цю "хмару", і вся відповідальність за ці питання покладається на власника ресурсу. Кожна компанія та кожен користувач може стати користувачем пропонованих послуг. Прикладами онлайн-сервісів є: Amazon EC2, Google Apps / Documents, Microsoft Office Web.

- Приватна хмара - це захищена IT-інфраструктура, яка контролюється та функціонує в інтересах єдиної організації. Організація може керувати власною приватною "хмарию" або передавати цю роботу на роботу. Інфраструктура може бути або з замовником, або із зовнішнім оператором (або частково з користувачем, а частково з оператором).

- Гібридна хмара - це IT-інфраструктура, яка використовує найкращі можливості державної та приватної хмари для вирішення проблеми. Цей тип часто використовується, коли організація має сезонні заходи. Іншими словами, оскільки внутрішня IT-інфраструктура не конкурує з існуючими завданнями, і існує потенціал "затуманити" громадськість (наприклад, цифри). Великі обсяги даних) та доступ до корпоративних ресурсів через загальнодоступну "хмару", щоб забезпечити доступ для споживачів.

1.1.2 Можливості хмарних обчислень

Розглянемо можливості хмарних обчислень:

- Доступ до особистої інформації з будь-якого комп'ютера, підключеного до Інтернету.

- Ви можете працювати з інформацією з різних пристроїв (ПК, планшета, телефону тощо).

- Незалежно від того, в якій операційній системі ви хочете працювати - веб-служби виконуються в кожному браузері операційної системи.

- Одна і та ж інформація, як ви, так і інші, можете одночасно переглядати та редагувати на різних пристроях.

- Багато платних програм стали безкоштовними (або дешевими) веб-додатками.

- Якщо щось трапиться з вашим пристроєм (ПК, планшет, телефон), ви не втратите жодної важливої інформації, оскільки пристрій більше не зберігається в пам'яті.

- Завжди в курсі і в актуальному стані.

- Ви завжди використовуєте останню версію програми, і вам не потрібно стежити за оновленнями, що виходять

- Ви можете ділитися своєю інформацією з іншими користувачами.

- Ви можете легко ділитися інформацією з коханими або людьми з будь-якої точки світу.

- Можливостей, вельми достатньо, проте, є і свої недоліки (куди ж без них), про яких також слід згадати.

Слабкості:

- необхідність постійного з'єднання. Для отримання доступу до послуг «хмари» необхідно постійне з'єднання з Інтернет;

- програмне забезпечення та його "оптимізація". Існують обмеження щодо програмного забезпечення, яке можна розгорнути у «хмарі» та зробити доступним для користувача. Програмне забезпечення, яке використовує користувач, має обмеження і іноді не може бути адаптоване для власних цілей;

- конфіденційність. Конфіденційність даних, що зберігаються у загальнодоступних "хмарах", в даний час є предметом суперечок. Однак у більшості випадків експерти сходяться на думці, що цій компанії не рекомендується зберігати кошовні документи в загальнодоступних "хмарах", оскільки в даний час немає технологій. Що гарантує 100 захист даних.

- безпека. Сама «хмара» є досить надійною системою, але якщо на неї втручається зломисник, вона отримує доступ до великого сховища даних. Іншим недоліком є використання систем віртуалізації, які використовують стандартні ядра операційної системи (наприклад, Windows) як надмірно чутливі та дозволяють використовувати віруси та системні вразливості.

- дорожнеча обладнання. Для побудови власного хмари необхідно виділити значні матеріальні ресурси, що не вигідно щойно створеним і малим компаніям;

- подальша монетизація ресурсу.

- хмари повинні виділяти значні фізичні ресурси, що не вигідно для стартапів та малого бізнесу.

- Щоб заробити більше грошей.

Достоїнства хмарних технологій:

- вся інформація доступна з будь-якого пристрою, будь то ПК, планшет, смартфон і т.д. підключеного до інтернету. Тут і плюс в тому, що користувач не прив'язаний до певного робочого місця;

- з припиненням витрат на придбання дорогих потужних комп'ютерів, серверів, немає потреби оплачувати роботу ІТ-фахівця для обслуговування локального дата-центру;

- необхідні інструменти для роботи надаються автоматично веб-сервісом.

- високий рівень технологічності обчислювальних потужностей, який надається користувачу, дозволяє зберігати, аналізувати і обробляти дані;

- оплачуються сервіси тільки в міру необхідності їх використання, при цьому оплата відбувається тільки за необхідний пакет послуг;

- сучасні хмарні обчислення можуть забезпечувати найвищу надійність, до того ж, лише невелика кількість організацій можуть дозволити собі утримувати повноцінний дата-центр.

1.1.3 Хмарні технології - погляд з боку користувача

Тут будуть розглянуті рішення, сервіси, програми, які вже існують на ринку і на що варто звернути свою увагу. Почнемо з сервісів:

- iCloud. Хмарний сервіс iCloud від Apple (що прийшов на зміну MobileMe), повністю автоматичний і безкоштовний (хоча і зі скромними робочими обмеженнями). Він зберігає Ваш вміст (електронну пошту, календар, контакти, документи, музику, відео, фотографії тощо) на серверах, а потім передає його бездротовим способом на всі пристрої (iPhone, iPad, iPod touch, Mac і PC) за технології Push .

- Google Play. Корпорація Google розробила новий хмарний сервіс під назвою Google Play, який дозволяє користувачам фільмів, музики, програм та книг зберігати цифрову інформацію виключно на сервері. Доступ до сервісу здійснюється безпосередньо через браузер, незалежно від операційної системи, і тому його можна зробити з Android, а також із залежних ПК та мобільних пристроїв. Кожен користувач має можливість вільно володіти та зберігати до 20 000 музичних композицій та купувати цифрові продукти - фільми, електронні книги, програми, музику - у магазинах (Android Market, Google Music та Google eBook Stores). Їде як придбаний, так і орендований.

- OnLive. Надає можливість грати в сучасні ігри навіть на найпростішому і слабенькому комп'ютері. Технічно це виглядає так: Сама гра знаходиться на віддаленому сервері, і є обробляюча графіка, яка доступна користувачеві у "готовому" вигляді, який вже є на комп'ютері. Простіше кажучи, розрахунки, які виконують графічна карта, процесор тощо в типовій комп'ютерній грі, вже виконуються на сервері, а ваш комп'ютер використовується лише як монітор, який отримує остаточне зображення. Це означає, що всі проблеми з продуктивністю комп'ютера та вільним дисковим простором будуть виправлені автоматично, оскільки вам навіть не потрібно встановлювати. Крім того, вам не доведеться переплачувати за товар (гру тощо) відразу, який Вам не обов'язково припаде до душі. До того, що, не секрет , що більшість ігор не хочеться

проходити повторно, тому виходить, що вартість декількох годин (або нехай навіть декількох днів) задоволення - невиправдано висока. Куди зручніше був би варіант, при якому Ви платили б тільки за той час, який граєте. Або ж - Ви б платили якусь невелику фіксовану суму щомісяця, що дозволяло б грати без обмежень в будь-які з доступних ігор. Саме це і пропонує OnLive .

- Xbox Live. Ще одна відома ігрова послуга, яка також пропонує повну функціональність Інтернету та стосується хмарних технологій. Короткий зміст послуги полягає в тому, що власники Xbox 360 та КПК на базі Windows Phone 7 можуть грати в комп'ютерні ігри та спілкуватися між собою та купувати доповнення та різноманітний мультимедійний вміст в Інтернет-магазині. Це свідчить про те, що служба створює своєрідний віртуальний всесвіт для геймерів, компоненти яких перебувають у хмарі, а не на консолях кінцевих користувачів.

Таким чином, два останніх сервіси пропонують гри як послугу. А тепер уявімо, що мова йде не про ігри, а про ПЗ. Тобто, Ви платите не за продукт як такої (за коробку з диском), а за конкретні функції / можливості, які він Вам надає.

1.1.4 Хмарні технології та зберігання даних

Не менш популярні і хмарні сховища файлів. Найвідомішими сховищами вважаються:

- Dropbox. У Вас може бути кілька комп'ютерів, але за допомогою цього хмарного сховища можна зробити загальну папку з файлами для всіх Ваших ПК і навіть смартфонів. Найцікавіше, що тут не доведеться робити ніяких особливих дій, бо операційна система сама буде сприймати загальну папку, як і всі інші папки на вінчестері, а дропбокс просто займеться синхронізацією. Ця послуга дозволяє безкоштовно зберігати до 2 ГБ даних. Основна увага приділяється синхронізації та обміну інформацією. Dropbox має історію завантажень для отримання даних після видалення файлів із сервера та дату модифікації файлу, яка доступна протягом 30 днів.

- Windows Live SkyDrive. Послуга SkyDrive дозволяє замовити до 7 ГБ (і файли до 100 МБ спільного використання) у послідовному форматі за допомогою стандартних папок. Зображення мають режим попереднього перегляду та можливість перегляду їх як слайдів. На додаток до послуг, інтегрованих у Microsoft Office, він також підтримує операційну систему Windows 8 (особливо клієнт SkyDrive, інтегрований у додатки Metro) та завантажує документи та фотографії в хмару одним клацанням миші. Дозволяє відкривати файли з віддаленого сховища.

- Google Диск.

До слова, не тільки всякі офіси і Файлосховище використовують хмарні технології. Наприклад, в стані боротьби з цифровою "нечистю" також зробили ставку на хмарні обчислення. І ось результат - безкоштовний антивірус Panda Cloud Antivirus. Загальні принципи синтезу систем автоматичного керування

Він базується на передовій технології "Колективний інтелект" (яка автоматично виявляє нові загрози в найкоротші терміни) і використовує обчислювальні можливості хмарних технологій для більшості завдань, впливу захисту на ресурси комп'ютерної системи. Скорочено: аналіз, блокування та видалення шкідливих програм.

Антивірусні сервери використовують інформацію від мільйонів користувачів продуктів Panda Antivirus по всьому світу для автоматичного виявлення та класифікації нових типів шкідливих програм щодня.

Передові інформаційні технології сьогодні відіграють часто основну роль в успіху підприємства - швидкість, з якою реагує бізнес на зміни на ринку, повинна бути найвищою і перевершувати конкурентів. Від цього безпосередньо залежить його рентабельність і успішність. Тому проблеми хмарних технологій сьогодні широко обговорюються і вирішуються. Експерти стверджують, що існує ряд інструментів і можливостей, які дозволено використовувати на повну потужність cloud technologies, незважаючи на їхні недоліки. Це велика робота, і стосується вона не тільки розробників. Концепція хмарних технологій дійсно важлива, так як може стати переломним моментом у веденні бізнесу і вивести

його на абсолютно новий рівень, а значить, приносити дохід не тільки керівництву, а й державі.

1.2 Мережа на основі сервера

Мережа на основі сервера (рисунок 1.3), або, як її ще часто називають, мережа типу "клієнт - сервер", - найбільш затребуваний тип мережі, основними показниками якої є високі швидкість передачі даних і рівень безпеки. Під словом "сервер" слід розуміти виділений комп'ютер, на якому встановлена система управління користувачем і ресурсами мережі. Комп'ютер в ідеалі повинен відповідати тільки за обслуговування мережі, і ніякі інші завдання виконувати на ньому не слід. Цей сервер називається контролер домену. Він є найбільш важливим об'єктом мережі, оскільки від нього залежить працездатність всієї мережі. Саме тому даний сервер обов'язково підключають до системи безперебійного живлення. Крім того, в мережі, як правило, присутня дублюючої сервер, який називається вторинний контролер домену.

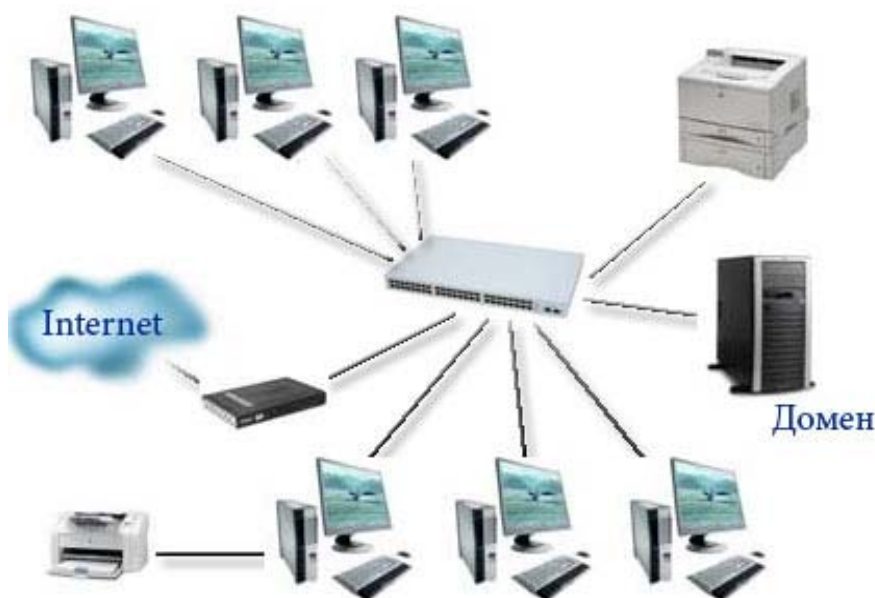


Рисунок 1.3 – Приклад мережі з керуючим сервером

Крім контролера домену в мережі можуть використовуватися і інші сервери різного призначення, до числа яких відносяться наступні.

Файл-сервер. Даний сервер являє собою сховище файлів різного типу. Навіть, як правило, зберігаються файли користувачів, загальні файлові ресурси, аудіо та відео-файли і багато іншого. Головна вимога до файлового серверу - надійна дискова підсистема, яка може забезпечувати безпечне зберігання файлів і доступ до них у будь-який час доби. Часто на даному сервері встановлюється архівуються система, наприклад стрімер, за допомогою якого здійснюється планове створення архівних даних. Це забезпечує гарантоване відновлення даних користувачів в разі непередбачених збоїв обладнання.

Сервер БД. Сервери подібного типу найбільш затребувані, оскільки дозволяють забезпечити доступ до єдиної бази даних. В якості такої можуть виступати бази даних бухгалтерського та іншого типу обліку, юридично-правові бази даних і т.д. В якості сервера бази даних використовуються потужні комп'ютери з великим обсягом оперативної пам'яті і RAID-масивом з швидких жорстких дисків. Дуже важливим є факт організації архівування даних, оскільки від цілісності бази даних і доступу до неї залежить робота всього підприємства.

Сервер додатків. Сервер додатків використовується як проміжна ланка між сервером бази даних і клієнтським комп'ютером. Це дозволяє організувати так звану триланкову (або трирівневу) архітектуру, за допомогою якої виконання програм, що вимагають обмін з базою даних, відбувається максимально швидко і ефективно. Крім того, за рахунок такої організації підвищується безпека доступу до даних і збільшується керованість процесом, оскільки легше контролювати роботу одного комп'ютера, ніж сотні.

Принт-сервер. Спеціальний сервер, що дозволяє зробити процес друку більш контрольованим і швидким. Використовується в мережах, яким необхідний доступ до спільного принтера. Сервер подібного роду забезпечує управління чергою друку і доступ до принтера для клієнтів будь-якого типу: при дротовому або бездротовому з'єднанні, для портативного пристрою або мобільного телефону.

Інтернет-шлюз. Даний сервер дозволяє надати користувачам локальної мережі доступ в Інтернет, а також організувати доступ до ресурсів по протоколах FTP і HTTP. Оскільки цей сервер є "вікном" в зовнішню мережу, до нього пред'являються певні вимоги, серед яких основними є вимоги до безпеки локальних даних і захист від доступу до них ззовні. Саме тому на такому сервері встановлюють різні фільтри і брандмауери, що дозволяють ефективно фільтрувати вхідний і вихідний трафік, що робить використання Інтернету більш безпечним.

Поштовий сервер. Практично кожне серйозне підприємство, що застосовує для організації обміну даними мережу на основі сервера, для спілкування із зовнішнім світом користується корпоративними електронними ящиками. Цей підхід цілком виправданий, оскільки дозволяє контролювати вхідний і вихідний трафік, тим самим блокуючи можливість витоку інформації. Подібну систему обміну інформацією дозволяє реалізувати поштовий сервер відповідним програмним забезпеченням. На цей сервер додатково встановлюються різноманітні антиспамовий фільтри, що дозволяють боротися (наскільки це можливо) з усе зростаючим обсягом рекламних листів, які і називаються спамом.

Крім згаданих вище, можуть використовуватись і інші типи серверів, що залежить тільки від потреб мережі. Підключення нових серверів не викликає ніяких труднощів, оскільки гнучкість і можливості мережі на основі сервера дозволяють зробити це в будь-який момент.

З точки зору системного адміністратора, мережа на основі сервера хоча і найбільш складна в створенні і обслуговуванні, але в той же час найбільш керована і контрольована. Завдяки наявності головного комп'ютера управління обліковими записами користувачів відбувається дуже легко і, найголовніше, - ефективно. Завдяки політикам безпеки також спрощується контроль над самими комп'ютерами, що робить мережу більш керованою, а дані в ній більш захищеними.

На сервер встановлюється серверна операційна система, яка, на відміну від звичайної операційної системи, володіє деякими перевагами, наприклад підтримкою декількох процесорів, більшого обсягу оперативної пам'яті, інструментами адміністрування мережі і т.д. До таких операційних систем відносяться Windows Server 2003 Windows Server 2008 і т. д.

1.2.1 Локальний сервер - швидкість і доступність

Основна перевага розташування центру управління корпоративною мережею на локальному сервері - висока швидкість обробки / передачі даних і постійна доступність. Сервер знаходиться в одній локальній мережі з користувачами і не залежить від наявності доступу в Інтернет, так само як і не обмежений пропускною спроможністю Інтернет каналу.

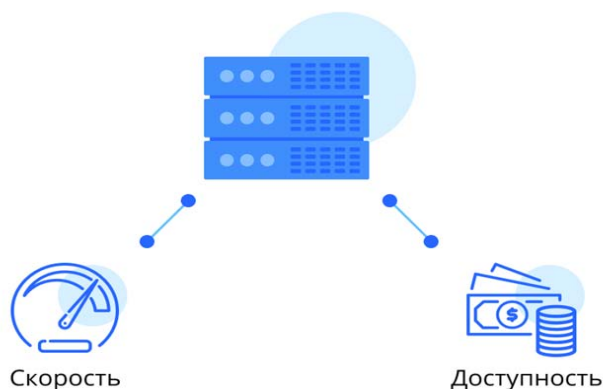


Рисунок 1.4 – Схематичне представлення простої системи керування

Таким чином, застосування локального сервера рекомендовано для підприємств і організацій які повинні обробляти великі масиви даних швидко або територіально віддалені від потужних каналів доступу в Інтернет:

- агропромислові комплекси;
- туристичні бази та будинки відпочинку;
- гірничорудні або шахтні комплекси і т.д.

Для таких підприємств можливе використання хмарного сервера, але це зажадає додаткової установки дорогого супутникового устаткування для забезпечення надійного і досить потужного каналу зв'язку з Інтернетом.

На жаль, локальний сервер має і ряд суттєвих недоліків:

- дороге обладнання завантажено в повному обсязі навіть у робочі години і часто простоює вночі;
- потрібно покупка резервних серверів для забезпечення відмовостійкості мережі;
- складно підтримувати ідеальний температурний режим, рівень вологості і електростатичного захисту;
- ризик втрати даних при рейдерському захопленні.

Незважаючи на ці обмеження, локальний сервер може стати єдиним виходом при ріс ті запитів бізнесу, що розвивається. Альтернативою такому підходу служить хмарний сервер, або термінальний сервер.

Таблиця 1.1 – Особливості мереж на основі виділеного сервера

Переваги мережі	Недоліки мережі
- Висока швидкість і продуктивність мережі - Використання виділених серверів, що полегшує роботу з ресурсами і спрощує контроль за їх використанням - Наявність дублюючих систем дозволяють захистити дані і зробити доступ до них безперебійним - Повний контроль над користувачами мережі - Високий рівень безпеки даних - Просунуті засоби моніторингу працездатності мережі - Легка розширюваність мережі	- Дорога в створенні і обслуговуванні - Постійна необхідність в системному адміністраторові - Залежність мережі від працездатності домена

Від вибору типу мережі залежить її майбутнє: розширюваність, можливість використання того чи іншого програмного забезпечення і

устаткування, надійність мережі і багато іншого. В цьому плані мережу на основі сервера є найкращою і вигідною.

1.3 Поняття структурованої кабельної системи

При створенні мережі використовується структурована кабельна система (СКС) (Structured Cabling System, SCS). СКС - це набір комутаційного обладнання, такого як кабелі, роз'єми, конектори, кросові панелі і шафи, а також методи їх спільного використання, які дозволяють створювати регулярні, легко розгортаються структури зв'язків в ЛВС.

SCS - це свого роду "конструктор", за допомогою якого мережевий дизайнер створює необхідну конфігурацію зі стандартних кабелів у поєднанні зі стандартними штекерами та замінює стандартні крос-панелі. За необхідності можна змінити конфігурацію мережі та з'єднання між комп'ютером та входом.

При створенні СКС мається на увазі, що на кожному робочому місці повинні бути розетки для підключення телефону і комп'ютера, навіть якщо в

Нині цього не потрібно. В майбутньому це може допомогти значно заощадити кошти. СКС планується і будується ієрархічно, з головною магістраллю і численними відгалуженнями від неї (рисунок 1.5).



Рисунок 1.5 – Структура кабельних підсистем

Загальна класифікаційна структура СКС складається з таких компонентів, як:

- горизонтальна підсистема (усередині землі);
- вертикальна підсистема (всередині будівлі);
- кампусна підсистема (в районі з декількома будівлями).

1.3.1 Горизонтальна підсистема СКС

Горизонтальна кабельна система бере початок від телекомунікаційної розетки на робочому місці і закінчується горизонтальним кросом в телекомунікаційному шафі (рисунок 1.6).

Для реалізації горизонтальної кабельної системи повинна використовуватися топологія "зірка", де кожна розетка на робочому місці з'єднується з горизонтальним кросом в телекомунікаційному шафі. Максимальна довжина будь-якого сегменту в горизонтальній системі не повинна перевищувати 90 м незалежно від типу використовуваної передавальної середовища, а також повинен бути запас на вигини кабелю, який становить 10% від довжини кабелю.

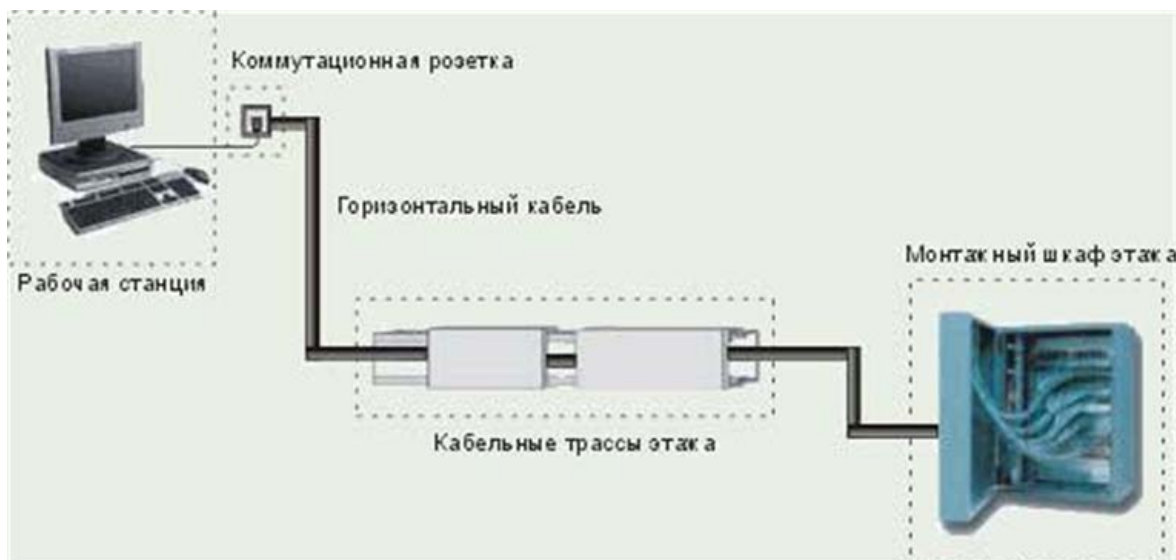


Рисунок 1.6 – Горизонтальна кабельна система

Горизонтальні кабельні системи ставлять високі вимоги до простої обробки та прокладання гілок, оскільки підсистема має велику кількість гілок.

Особливості горизонтальної кабельної підсистеми:

- компоненти, які виконують функцію конкретних додатків (наприклад, розгалужувачі), не повинні входити в частину горизонтального кабельної системи, при необхідності їх можна розмістити поза телекомунікаційної розетки або горизонтального кросу;

- визнані типи горизонтальних кабелів:

- 1) 4 парний кабель UTP 100 Ом;

- 2) 2 волоконний (дуплекс) багатомодовий волоконно-оптичний кабель 62.5 / 125 мкм;

- 3) 2 парний кабель STP-A 150 Ом.

- допускається наявність однієї перехідної точки між різними формами кабелю одного типу;

- коаксіальні кабелі 50 Ом визнаються стандартом 568-A, але не рекомендуються для установки в нових кабельних системах;

- можуть бути встановлені додаткові розетки. Такі розетки є додатковими елементами і не можуть замінювати собою мінімальні вимоги стандарту;

- використання шунтованих виводів і муфт не допускається в горизонтальних кабельних системах на основі мідних середовищ (дозволяється використання муфт для оптичного волокна).

1.3.2 Вертикальна (або магістральна) підсистема СКС

Маршрут кабелю всередині будівлі, що з'єднує шафа з шафою або шафа з апаратної, називається вертикальною (магістральною) підсистемою будівлі, що з'єднує головний крос в апаратної з проміжними кросами і з горизонтальними кросами в телекомунікаційних шафах. Підключення до нього складається з носія, який несе інформацію про автостраду між цими місцями, а також пов'язаних комутаційних пристроїв, що усувають подібні джерела.

Всі телекомунікаційні кабельні системи та обладнання повинні бути заземлені.

Основні положення, визначені для магістральної кабельної підсистеми:

- з'єднання обладнання з магістральної кабельної системою повинні виконуватися за допомогою кабелів довжиною до 30 м;

- вертикальна (магістральна) кабельна система повинна бути сконфігурована по топології "зірка". Кожен горизонтальний крос з'єднується безпосередньо з головним кросом, або спочатку з проміжним, а потім з головним;

- магістраль має мати не більше двох ієрархічних рівнів кросів (головний і проміжний). Між головним і горизонтальним кросом має бути не більше одного кросу, а між двома горизонтальному ними кросами - не більше трьох;

- сумарна максимальна довжина магістралі в 90м визначена для забезпечення високої пропускної спроможності мідного кабелю. Ця довжина передбачена для безперервних ділянок магістралі (проміжний крос відсутня);

- кабель вертикальної (основної) підсистеми, який підключений до підлоги будівлі, повинен передавати дані на великі відстані та швидше, ніж горизонтальний системний кабель.

Для вертикальних підсистем вибір кабелю наразі обмежений трьома варіантами:

- оптоволокно - відмінні можливості для пропускної здатності, Чудові, відстані та захисту даних. Стійкість до електричних перешкод; Може передавати голос, відео та дані. Але відносно дорогі, важкі в експлуатації філії;

- товстий коаксіал - хороші характеристики пропускної здібності, відстані і захисту даних; може передавати дані. Але з ним складно працювати, хоча фахівців, що мають подібний досвід роботи, достатньо багато;

- широкосмуговий кабель, який використовується в кабельному телебаченні має хороші показники пропускної здатності і відстані; може передавати голос, відео і дані. Однак дуже важко експлуатувати і має високу вартість під час експлуатації.

1.3.3 Підсистема робочого місця

Ця підсистема (рисунок 1.7) створює з'єднання між інформаційною розеткою (телекомунікаційний роз'єм) і абонентським пристроєм (комп'ютер / телефон). У підсистемі визначені вимоги до апаратним шнурах і телекомунікаційним розеток на робочому місці користувача.

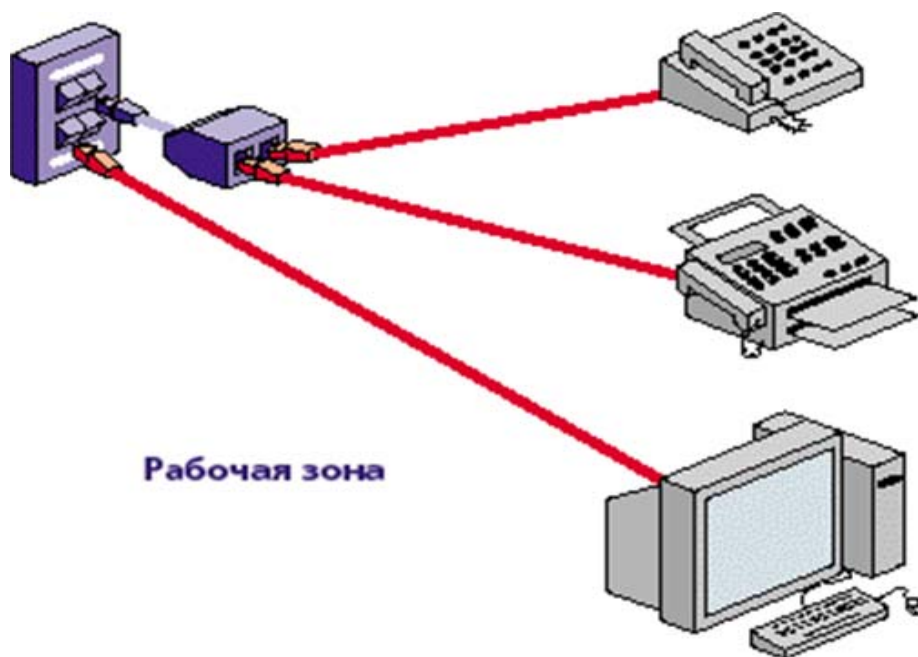


Рисунок 1.7—Робоча зона

Телекомунікаційні роз'єми розташовуються в будь-якій області робочого місця. При проектуванні кабельної системи телекомунікаційні роз'єми повинні розміщуватися в легкодоступних місцях. Висока щільність розміщення роз'ємів збільшує масштабованість системи. У багатьох країнах роз'єми встановлюються з розрахунку: два роз'єми на мінімум 6 кв. м. і максимум 10 кв. м. робочої площі. Роз'єми можуть встановлюватися як окремо, так і в групі, але кожне робоче місце повинно бути забезпечено мінімум двома роз'ємами.

Кожен телекомунікаційний роз'єм повинен бути промаркований постійної, добре помітною для користувача етикеткою. слід звернути увагу на маркування кожної дуплексної пари: всі зміни маркування повинні фіксуватися в документації.

При проектуванні СКС, на етапі вибору типу кабельної системи, слід визначитися з тим, який тип кабелю і роз'єму використовуватиметься в кожній підсистемі. Згодом це вплине на вибір мережевого обладнання.

Основні положення, які стосуються кабельної системи робочого місця:

- передбачається, що апаратні шнури мають такі ж характеристики, як патч - корд того ж типу і категорії;
- при використанні адаптерів передбачається, що їх характеристики сумісні з характеристиками передачі обладнання, до якого вони підключаються;
- у специфікаціях довжин кабелів в горизонтальній системі прийнято, що для апаратних шнурів на робочому місці максимальна довжина кабелю визначена в 3 м;
- адаптери і пристрої, що служать для підтримки конкретних додатків, повинні розміщуватися поза телекомунікаційної розетки.

2 ВИБІР АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

2.1 Вибір активного обладнання

Відповідно до технічного завдання, необхідно вибрати наступне активне обладнання:

- мережеві адаптери для робочих станцій;
- конвертер оптичний;
- мережеві адаптери для серверів;
- мережеві сервери;
- джерела безперебійного живлення;
- маршрутизатори;
- xDSL-модем;
- комутатори;
- міні АТС;
- VoIP-шлюзи.

В даний час є велика кількість фірм, що роблять мережеве обладнання. Найбільш поширеними є Cisco, Allied Telesis, D-Link, Intel, 3COM, ATI, і інші.

2.1.1 Вибір мережевого адаптера для робочих станцій

Плати мережевого адаптера виконують функцію фізичного інтерфейсу між робочою станцією і мережевим кабелем. Плати вставляються в слоти розширення всіх мережевих робочих станцій і серверів. Щоб створити фізичне з'єднання між робочою станцією і мережею, до відповідного роз'єму плати підключається мережевий кабель.

Основними елементами мережевих адаптерів є:

- пам'ять мікропрограм;
- приймач (трансивер);

- мережевий контролер;
- оперативна пам'ять.

Оскільки плата мережевого адаптера значно впливає на швидкість передачі даних, то вона впливає і на працездатність всієї мережі.

Для комп'ютерів беремо адаптер Intel EtherExpress PRO/100 +, який має такі технічні характеристики:

- вставляється в стандартний PCI-слот;
- має один порт 10 / 100TX, що підтримує віддалене включення і активізацію комп'ютера після засипання (Remote Power On (RPO), Remote Wake Up (RWU));
- має один роз'єм для Flash-пам'яті, яка забезпечує перевірку на віруси;
- режим Full-Duplex;
- чіпсет: Intel 82558B.

Кількість мережевих карт повинна дорівнювати кількості комп'ютерів в мережі плюс плати для сервера.

2.1.2 Вибір мережевого адаптера для сервера

В даний час все частіше і частіше піднімається питання підвищення пропускної здатності каналів між робочою станцією і серверами. Це відбувається з різних причин:

- підвищення продуктивності робочих станцій;
- збільшення масштабу мережі;
- поява програм, які працюють з мультимедійною інформацією, яка зберігається в файлах великих розмірів.

В проєктованій мережі передбачається встановити чотири файлових сервера, в основному всі комп'ютери будуть працювати з ресурсами серверів. Отже, може з'явиться потенційний вузьке місце в мережі, а конкретно - порт комутатора для підключення сервера. Залежно від створюваного ними трафіку,

час затримки серверів може змінюватися в значних межах. Вирішити цю проблему можна двома способами:

- 1) використовувати комутатор з одним високошвидкісним гігабітним портом для підключення сервера і декількома портами на 100 Мбіт / сек для підключення комп'ютерів;
- 2) для підключення сервера скористатися спеціальною двоканальною повнодуплексною мережевою картою. Друге рішення видається більш економічним.

На підставі вищесказаного вибираємо для серверів мережеві адаптери Intel на чіпсеті Intel 82571GB, з інтерфейсом PCI Express x4:

- тип мережі: - Ethernet, - Fast Ethernet, - Gigabit Ethernet;
- макс. швидкість передачі (WAN) 1000 Мбіт / сек;
- віддалене завантаження Wake-on-LAN;
- протоколи віддаленого управління DMI 2.0, SNMP;
- системні вимоги Linux 2.4, MS Windows 2000, MS Windows Server 2003, Novell NetWare 5.x, SunSoft Solaris 8.

2.1.3 Вибір мережевого сервера

Під сервером розуміється комп'ютер, що надає свої ресурси іншим комп'ютерам. Сервер обробляє і зберігання основну інформацію в ЛОМ. У зв'язку з величезною варіацією використовуваної інформації і способів її обробки існують різні типи серверів: файловий сервер, сервер друку, сервер бази даних, Web-сервер, поштовий сервер та ін.

По складу обладнання сервери мало чим відрізняються від звичайних комп'ютерів, однак до них пред'являють більш високі вимоги. Це пов'язано з тим, що сервер повинен достатньо швидко обробляти велику кількість запитів від всіх абонентів. З ростом числа абонентів і ускладненням вирішуваних завдань значно збільшуються вимоги до сервера по продуктивності, об'єму пам'яті, надійності.

Мережеві сервери повинні мати масштабність. У зв'язку з цим сервери проектується з урахуванням можливості встановлення більш потужних або додаткових процесорів, оперативної пам'яті і жорстких дисків.

Як сервер буде використано обладнання фірми Kraftway (рисунок 2.1), так як дане обладнання має оптимальне співвідношення ціна/продуктивність.



Рисунок 2.1—Зовнішній вигляд сервера Kraftway Express ISP ES12

Сервер досить компактний, зручний в обслуговуванні, дозволяє досягти високої продуктивності в мінімальному обсязі простору, надійний і відмовостійкий. У сервері використовується пам'ять з можливістю резервування і віддзеркалення. У ньому встановлені передові засоби автоматичної діагностики і усунення несправностей, а також функція віддаленого управління. Сервер виготовляється в корпусі Rackmount висотою 1U, що дозволяє створити масив з 42 серверів в стандартній 42U стійці.

Характеристики Сервер Kraftway Express ISP ES12:

- побудований на основі серверної архітектури Intel з використанням чіпсета Intel 5000P з частотою системної шини до 1333MHz;
- підтримує роботу двох процесорів Multi-Core Intel Xeon;
- використовує пам'ять ECC FBDIMM (Fully Buffered DIMM) DDR2-533 або DDR2-667 (до 32GB) шина PCI-Express x8, x4 і / або PCI-X 64bit / 66MHz (в залежності від комплектації);
- сервер орієнтований на використання дискової підсистеми на базі SATA або SAS HDD з підтримкою гарячої заміни.

2.1.4 Вибір джерела безперебійного живлення

Щоб забезпечити безперебійне живлення (ДБЖ) сервера, потрібно вибрати джерело безперебійного живлення, щоб забезпечити безперебійну роботу мережі та захист від раптових відключень електроенергії. Сервер ДБЖ використовує акумулятор, достатньо довгий для зберігання даних та нормального вимкнення для стабільної роботи.

При виборі ДБЖ важливо враховувати використовувану потужність обладнання, для якого необхідна установка ДБЖ.

Як джерело безперебійного живлення буде використано обладнання APC Smart-UPS SUA3000I (рисунок 2.2).



Рисунок 2.2 – ДБЖ APC Smart-UPS SUA3000I

Технічні характеристики APC Smart-UPS SUA3000I приведені в додатку А.

2.1.5 Вибір комутаторів

Комутатор (англ. Switch) виступає в якості ведучого елемента ЛОМ. Він забезпечує зв'язок з базовою магістраллю або групою серверів по високошвидкісних каналах, також з'єднує сегменти мережі, служить для ізоляції трафіку в мережі, що підвищує швидкість передачі інформації.

Комутатори вирішують такі проблеми:

- дають можливість для масштабування мережі;
- усувають вузькі місця, які з'являються в результаті підключення надлишкового числа абонентів і зростання трафіку.

Комутатор зберігає в пам'яті таблицю, в якій вказується відповідність MAC-адреси вузла порту комутатора. При першому включенні комутатора ця таблиця не заповнена, і він працює в режимі навчання. У цьому стані дані, що надходять до порту, передаються на всі інші порти комутатора. При цьому комутатор аналізує кадри і, визначивши MAC-адресу хоста-відправника, заносить його в таблиці. Згодом, якщо на один з портів комутатора надійде кадр, призначений для хоста, MAC-адресу якого вже є в таблиці, то цей кадр буде переданий тільки через порт, зазначений у таблиці. Якщо MAC-адресу хоста-одержувача ще не відомий, то кадр буде продубльований на всі інтерфейси. Через якийсь час комутатор будує повну таблицю для всіх своїх портів, і в результаті трафік локалізується.

Комутатори розрізняються за розміром таблиці MAC-адресів:

- магістральні комутатори. Мають таблицю більш 32.000 MAC-адрес, з якої не менше 8.000 MAC-адрес може виділятися на будь-який порт. Використовуються для об'єднання великих мереж і підключення їх до магістрального кабелю;

- базові комутатори. Мають таблицю більш 8.000 MAC-адрес, з якої не менше 512 MAC-адрес може виділятися на будь-який порт. Використовуються для об'єднання концентраторів і комутаторів усередині мережі;

- комутатори для робочих груп. Зазвичай мають таблицю від 256 до 8.000 MAC-адрес, однак з більшістю портів пов'язуючи тільки один MAC-адрес (всі інші адреси зв'язуються з Uplink-портом). Використовуються замість класичних концентратор для підключення до мережі великого числа робочих станцій і серверів.

Для побудови мережі будемо використовувати комутатори фірми Allied Telesis, так як вони мають оптимальним співвідношенням ціни і якості (детальні характеристики наведено в додатку Б).

На другому поверсі в місці об'єднання будівель використовуємо комутатор Allied Telesis AT-8000S / 48, 48 X 10/100, 2 - 1000 МБ / С або 2 SFP, WEBVIEW, SNMP, STACK (рисунок 2.3).



Рисунок 2.3 – Комутатор Allied Telesis AT-8000S / 48

На всіх інших поверхах використовуємо комутатори Allied Telesis AT-8000S / 24, 24 X 10/100, 2 - 1000 МБ / С або 2 SFP, WEBVIEW, SNMP, STACK (рисунок 2.4).



Рисунок 2.4 – Комутатор Allied Telesis AT-8000S / 24

Allied Telesis AT-8000S / 24 являє собою недорогий стекуємий, керований комутатор Gigabit Ethernet, що є ідеальним рішенням для збільшення кількості портів на кордоні мережі. Цей ефективний за вартістю комутатор має форм-фактор 1RU, 2 комбінованих порту Gigabit Ethernet SFP і спеціальні інтерфейси для стекування.

Додатковий набір можливостей включає в себе агрегацію з'єднання, підтримку VLAN і віддзеркалення портів в стеку. Усі інші характеристики наведено в додатку В.

Для об'єднання всіх комутаторів використовуємо комутатор другого рівня Dell 4032F/24POE. 24 – 10МБ/10ГБ /С, 2 SFP COMBO. WEBVIEW. SNMP 24 POE 180Вт (рисунок 2.5).

Dell 4032F/24POE є недорогим стекуємий керований комутатор з підтримкою Power over Ethernet (PoE) для IP-телефонів і точок доступу з підтримкою PoE. Цей ефективний по вартості комутатор має форм-фактор 1RU, 2 комбінованих порту Gigabit Ethernet SFP і спеціальні інтерфейси для стекування. Додатково набір можливостей включає в себе агрегацію з'єднання, підтримку VLAN і віддзеркалення портів в стеку (див. додаток Г).



Рисунок 2.5 – Комутатор Dell 4032F/24POE

2.1.6 Вибір маршрутизатора

Маршрутизатор (англ. Router) - це мережевий пристрій, який здійснює вибір маршруту між декількома мережами передачі даних або сегментами однієї мережі, що мають різну архітектуру або протоколи.

Поділивши маршрутизатор на конфліктуючі домени та домени трансляції, навантаження мережі можна зменшити за допомогою фільтрації пакетів. Маршрутизатори широко використовуються для забезпечення доступу до глобальної мережі Інтернет через локальну мережу, яка виконує функції перекладу адрес та функції брандмауера.

Для побудови даної мережі візьмемо маршрутизатор добре зарекомендував себе компанії Cisco 2 821-SEC / K9 SECURITY BUNDLE, ADV SECURITY, 64F / 256D (рисунок 2.6).

Маршрутизатор Cisco серії 2800 серії мають можливість одночасового забезпечення великої кількості сервісів з великою швидкістю на кількох з'єднаннях T1 / E1 / xDSL (див. додаток Г).



Рисунок 2.6 – Маршрутизатор CISCO +2821-SEC / K9

2.1.7 Вибір модему

Головною функцією модему є узгодження спектра сигналу джерела повідомлень з частотними характеристиками каналу. Крім того, в сучасних модеми створюють захист від колізій, стискають дані, шифрують інформацію. При роботі модем входить у з'єднання з іншим модемом за схемою «точка - точка».

Для передачі даних по комутованій телефонній лінії використовуватимемо SHDSL модем SG-17BT. SHDSL модем SG-17BT - швидкість в лінії до 15 296 кбіт / с по одній парі (рисунок 2.7).



Рисунок 2.7 – SHDSL модем SG-17BT

SHDSL модем SG-17BT призначений для об'єднання розподілених локальних мереж, підключення віддалених комп'ютерів і пристроїв, оснащених інтерфейсом Ethernet.

Параметри лінійного інтерфейсу G.SHDSL наведені в додатку Д.

2.1.8 Вибір оптичного конвертора

Конвертер служить для перетворення мідної середовища в оптичну і навпаки. Для цього використовуємо медіа-конвертор Allied Telesis AT-FS202, 10 / 100TX, 100FX MULTIMODE, 1310 нм, до 2 км, SC (рисунок 2.8).



Рисунок 2.8 – Медіа-конвертор Allied Telesis AT-FS202

Медіа-конвертери Allied Telesis AT-FS200 серії мають 2 порти, є некерованими і автономними. Медіа-конвертери дають такі можливості:

- масштабованість мережі шляхом додавання оптики тільки там, де вона дійсно потрібна;
- додавати нові пристрої без необхідності заміни дорогих сполучних кабелів;
- інтегрувати пристрою з широкою смугою пропускання в мережі.

Технічні характеристики Allied Telesis AT-FS202 наведено в додатку Е.

2.1.9 Вибір міні АТС

В даний час існує безліч фірм-виробників міні-АТС, здатних вкластися в задані параметри мережі, зупинимо вибір на фірмі Samsung.

Цифрова офісна АТС Samsung iDCS-500 (Internet-ready Digital Communications System) - це сучасна цифрова система засновницької зв'язку ємністю до 488 портів (рисунок 2.9), з можливостями передачі голосу по каналах даних, комп'ютерної телефонії, а також широким спектром додатків телефонного сервісу комп'ютерної телефонії CTI (Voice Mail, Auto Attendant та ін).

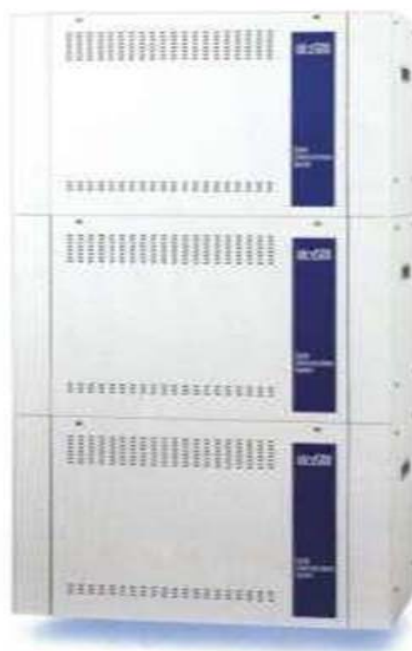


Рисунок 2.9 – Зовнішній вигляд цифрової АТС Samsung iDCS 500

Комплектуючі АТС Samsung iDCS-500 розміщуються в максимум трьох компактних стативах. Все Стативи iDCS-500 містять по 2 слота для блоків живлення, по 1 слоту керуючої карти і по 9 універсальних слотів. Універсальні слоти поділяються на 32-х каналні (3шт / статив) і 16-каналні (6 шт / статив).

Також в кожному стативі є спеціальний слот для сервісної карти, що містить модем, Ethernet-порт, послідовні RS-232 порти. Основний статив АТС Samsung iDCS-500 завжди оснащується процесорним модулем, а додаткові Стативи - модулями розширення, які об'єднують загальну шину модулів системи.

2.1.10 Вибір VoIP – шлюзу

VoIP-шлюз (Voice over IP-шлюз) - це пристрій, призначений для підключення телефонних апаратів або офісних АТС до IP-мережі для передачі голосового трафіку. Коли актуальність і затребуваність IP-технологій в корпоративному секторі стала очевидна, виробники офісних АТС почали випускати плати розширення для офісних АТС. Ці плати дозволяли здійснювати передачу трафіку безпосередньо в IP-мережі. Однак вартість плат розширення виявилася надто висока, що і призвело до появи VoIP-шлюзів на ринку.

Основні відмінності VoIP-шлюзів від плат розширення АТС:

- ціна на VoIP-шлюзи в кілька разів нижче (в розрахунку на один канал);
- витрати на установку, настройку і обслуговування VoIP-шлюзів значно нижче (за рахунок того, що ці роботи можуть виконуватися силами власної ІТ служби);
- розширення числа каналів VoIP-шлюзів теж в рази дешевше (докуповуються модулі розширення);
- VoIP-шлюзи краще сумісні з VoIP-устаткуванням інших виробників (помітно менше ймовірність проблем при стикуванні з обладнанням оператора IP-телефонії).

Як VoIP-Шлюзу буде використано обладнання Addpack AP2620-2E1 - цифровий VoIP шлюз (рисунок 2.10).



Рисунок 2.10 – Цифровий VoIP шлюз Addpack AP2620-2E1

Основні характеристики AP2620-2E1:

- високопродуктивний шлюз для сервісу VoIP;
- модульна архітектура - до 60 каналів;
- VoIP протоколи - H.323, SIP, MGCP;
- розширені функції QoS;
- підтримка основних протоколів маршрутизації даних;
- функції мережевий масштабованості;
- функції забезпечення безпеки.

Специфікація апаратної частини AddPac AP2620-2E1:

- 2 встановлених модуля 1 * E1 ISDN PRI / R2;
- 2x10 / 100 Mbps Ethernet інтерфейсу для WAN, LAN (RJ-45);
- 1 порт консолі RS-232C (RJ-45);
- внутрішнє джерело живлення;
- габарити (висота x ширина x довжина): 44мм x 444мм x 220мм;
- маса: 3,5 кг.

2.2 Вибір пасивного обладнання

Відповідно до технічного завдання проектованої мережі, необхідно вибрати наступне пасивне обладнання:

- телекомунікаційні шафи;
- полки, органайзери, фальш-панелі;
- оптичний крос;
- патч-панелі;
- блок силових розеток.

2.2.1 Вибір телекомунікаційних шаф

Телекомунікаційні шафи використовують для зручного розміщення кросового обладнання, активного обладнання, такого як комутатори, маршрутизатори, сервери, джерела безперебійного харчування і так далі. При виборі шафи, необхідно знати, яке обладнання буде встановлено в ньому, його кількість і де буде встановлений шафа.

Висота шафи вимірюється в «юнітах», що позначають кількість монтажних місць для обладнання, один «юніт» дорівнює 44,45 мм. Також монтажні стійки виконуються в двох варіантах: підлогового і настінного виконання.

В даному проекті для приміщення серверної, на 2-му поверсі, найдоцільніше використовувати телекомунікаційний шафа підлогового виконання, висотою 42U.

Підлогова шафа серії ШТК-М (рисунок 2.11) призначений для розміщення активного і пасивного телекомунікаційного обладнання, в офісних і закритих промислових приміщеннях.

Шафа має розбірну каркасну конструкцію. Складається з підстави, даху і двох зварних рам, з'єднаних комплектом швелерів (сталь 2 мм.). Легкий у збірці. За рахунок елементів кріплення каркас шафи має підвищену жорсткість, залежно від модифікації можливе розподілене вертикальне навантаження до

650 кг. ШТК-М комплектується посиленими бічними стінками. Стінки надійно фіксуються пластиковими засувками і точковими замками.



Рисунок 2.11 – Підлогова шафа 19" серії ШТК-М

Технічні характеристики підлогової шафи 19" серії ШТК-М:

- висота - 42U або 2030 мм;
- ширина - 600мм;
- глибина - 1020мм;
- корисна глибина - 880мм;
- Вага виробу - 133кг;
- розподілене навантаження - 550кг;
- матеріал передніх дверцят - скло.

Для захисту обладнання в приміщеннях на решті поверхів будівель використовуємо настінні шафи висотою 12U.

Настінна шафа 19 "серії ШРН призначений для розміщення активного і пасивного телекомунікаційного обладнання (рисунок 2.12).



Рисунок 2.12 - Настінна шафа 19" серії ШРН

Технічні характеристики настінного шафи 19" серії ШРН:

- висота, 12U або 632 мм;
- ширина - 600мм;
- глибина - 300мм;
- корисна глибина - 250мм;
- вага виробу - 18кг.

2.2.2 Вибір полиць

Полка металева стаціонарна призначена для установки і підтримки важкого устаткування вагою до 50 кг (рисунок 2.13). Мають чотири точки фіксації до вертикальних напрямних шаф і відкритих стійок. Для вільного проходження холодного повітря полки мають розвинену перфорацію.



Рисунок 2.13 – Полка перфорована в шафу

Технічні характеристики:

- висота - 25мм;
- ширина - 496мм;
- глибина - 750мм;
- вага виробу - 3,6 кг.

2.2.3 Вибір оптичного кросу

Кроси оптичні стійку 19 дюймові встановлюються в місцях переходу з магістральних оптичних кабелів на локальні інформаційні мережі. Оптичні кроси монтуються в 19 дюймові стійки або шафи всередині приміщень. Кроси забезпечують механічно захищене зі'єднання вхідного оптичного кабелю і обладнання. Як оптичного кросу вибираємо полку оптичну 19 "шафа 2 U 48 порту FC / SC.



Рисунок 2.14 – Полка оптична 19 "

3 РОЗРОБКА МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ ТА КОНФІГУРУВАННЯ ПРОГРАМНИХ ЗАСОБІВ

3.1 Проектування локальної мережі на базі технології Fast Ethernet

Мета проектування – розрахувати технічні характеристики корпоративної мережі, визначення апаратного та програмного забезпечення для всього набору корпоративних локальних мереж, розташування вузлів мережі та мережевих каналів зв'язку та розрахунок корпоративних мережевих витрат.

- Початковими даними для побудови мережі є:
- кількість і розміщення комп'ютерів і серверів;
- перелік необхідних завдань і служб, що виконуються в мережі;
- план приміщень, в яких необхідно побудувати локальну мережа;
- додаткові технічні, економічні та експлуатаційні вимоги.

3.1.1 Методика проектування локальної мережі

Під час проектування вирішуються наступні завдання:

- вибір мережевої технології, на якій буде базуватися сітьова інфраструктура;
- розрахунок і планування середнього коефіцієнта використання трафіку та мережі;
- вибір топології підключення до мережі;
- генерування списку потрібних сітьових пристроїв, визначення виду кабелів;
- розробка схеми розподілу кабелів та розташування ПК та серверів;
- підбір мережевого програмного забезпечення та протоколів, що будуть використовуватися;

- розрахувати вартість впровадження ЛМ та економічний вплив від її функціонування.

При створенні нової мережі слід враховувати такі моменти:

- необхідний об'єм мережі (в даний час, найближчим часом і на майбутнє).

- структура, класифікація та важливі частини мережі (через осередки компанії, а також кімнати, поверхи та будівлі компанії);

- пріоритетні напрямки та щільність трафіку даних у мережі (зараз, найближчим часом та у довгостроковій перспективі);

- тип потоку даних, що передається по мережі, що безпосередньо впливає на бажану швидкість передачі ($< x \cdot 10^2$ Мбіт/с для телевізійних зображень з високою роздільною здатністю);

- характеристики обладнання (ПК, адаптери, кабелі, ретранслятори і т.д.) та його вартість.

- можливість прокладання кабельної системи між приміщеннями та в них, а також заходи щодо попередження пошкоджень кабелів.

- контроль та адміністрування мережі та її надійності та безпеки;

- вимоги до ПЗ з точки зору дозволеного розміру мережі, швидкості, гнучкості, обмеження прав доступу, витрат, можливості моніторингу обміну даними тощо.

- з'ясувати, чи потрібно підключатися до інтернету або інших локальних мереж.

3.1.2 Вибір мережевої технології

Проаналізувавши мережеві технології, що наведені в таблиці 3.1, і врахувавши, що мережа повинна гарантувати надійність, простоту і масштабованість, явними перевагами володіє технологія Fast Ethernet.

Головними перевагами технології Fast Ethernet є:

- пропускна здатність сегментів мережі зростає до 100 Мб/с;
- збереження методу випадкового доступу;
- збереження формату кадру, прийнятого в стандарті IEEE 802.3;
- підтримка основних способів передачі даних - кручений пари і оптоволоконного кабелю.

Різновиди Ethernet і їх фізичні характеристики наведені в таблиці Є.1 додатка Є.

3.1.3 Вибір мережевої топології

В даному проекті поставлено завдання зв'язати адміністративний корпус установи високошвидкісною мережею зі швидкістю передачі даних - 100 Мбіт/сек.

При виборі виду мережі Ethernet, що складається з ділянок різних типів, виникає безліч питань, пов'язаних з максимально можливим розміром (діаметром) мережі та максимально допустимим числом різних елементів мережі. Мережа буде правильно функціонувати тільки, в разі, якщо затримка поширення сигналу в ній не перевищить граничну величину. Це визначається обраним методом управління обміном CSMA / CD, який заснований на виявленні та вирішенні колізій.

По-перше, для отримання складних конфігурацій Ethernet з окремих ділянок мережі використовуються проміжне обладнання двох основних типів:

- репітерні концентратори (хаби) - являють собою набір репітерів і ніяк логічно не поділяють ділянки мережі, півинятком до них;
- комутатори - передають інформацію між ділянками мережі, але не передають конфлікти з сегмента на сегмент.

При встановленні більш складних комутаторів колізії в окремих ділянках мережі вирішуються на місці, не поширюючись по мережі, як у випадку застосування більш простих репітерних концентраторів. Це має принципово важливе значення для вибору топології мережі Ethernet, так як в ній

використовується метод доступу CSMA / CD, що передбачає наявність колізій і їх дозвіл, при цьому загальна довжина мережі якраз і визначається розміром зони конфлікту, області колізії (collision domain).

Для визначення працездатності мережі Fast Ethernet стандарт IEEE 802.3 пропонується два методи. Перший заснований на декількох нескладних правилах. Він виходить з того, що всі абоненти мережі (зокрема, кабелі) мають найгірші з можливих тимчасові характеристики, тому завжди дає результат зі значним запасом. Другий метод використовує систему точних розрахунків з реальними часовими характеристиками кабелів.

При виборі першого методу необхідно керуватися такими принципами:

- ділянки, виконані на електричних кабелях (кручених парах), не перевищують 100 метрів. Це відноситься до кабелів усіх категорій - 3, 4 і 5, до сегментів 100BASE-T4 і 100BASE-TX;

- ділянки на оптоволоконних кабелях не перевищують 412 метрів;

- якщо використовуються адаптери з зовнішніми (виносними) трансиверами, то трансиверного кабелі (МІІ) не повинні бути довше 50 сантиметрів.

Другий метод для мережі Fast Ethernet заснований на обчисленні сумарного подвійного часу проходження сигналу по мережі. Для розрахунків відповідно до другого методом спочатку необхідно визначити шлях максимальної довжини мережі. Якщо таких шляхів кілька, то розрахунок повинен проводитися для кожного з них.

Слід зазначити, що другим методом доцільно користуватися в основному при наявності в мережі оптоволоконних сегментів, тому що на електричному кабелі важко створювати мережу значного розміру.

Залежно від виду роботи кожна організація має свої вимоги до характеристик мережі. Для організації з горизонтальною структурою, в якій усі працівники повинні обмінюватись даними один з одним, найкращим рішенням є звичайна однорангова мережа. Організація, яка базується на принципі вертикальної структури і точно знає, на яких співробітниках та до якої

інформації слід отримати доступ, слід зусередитись на більш дорогій версії мережі - із виділеним сервером. Правами доступу можна керувати лише в такій мережі.

Структура установи - вертикальна. Усе підкоряються міністру, і кожен співробітник має доступ до певної частини інформації. Виходячи з цього, для даної ЛОМ вибираємо технологію «клієнт-сервер». У цьому випадку застосування діляться на дві частини: клієнтську і серверну. Кілька найбільш потужних комп'ютерів мережі налаштовуються як сервери додатків: на них виконуються серверні частини додатків. Клієнтські частини виконуються на робочих станціях; саме на них створюються запити до серверів додатків і відображаються отримані результати. Для взаємодії визначається деякий протокол (зазвичай TCP / IP). Часто кожна сторона в моделі клієнт/сервер може виконувати функції як сервера, і клієнта.

На рисунку 3.1 зображена структурна схема проектованої локальної мережі.

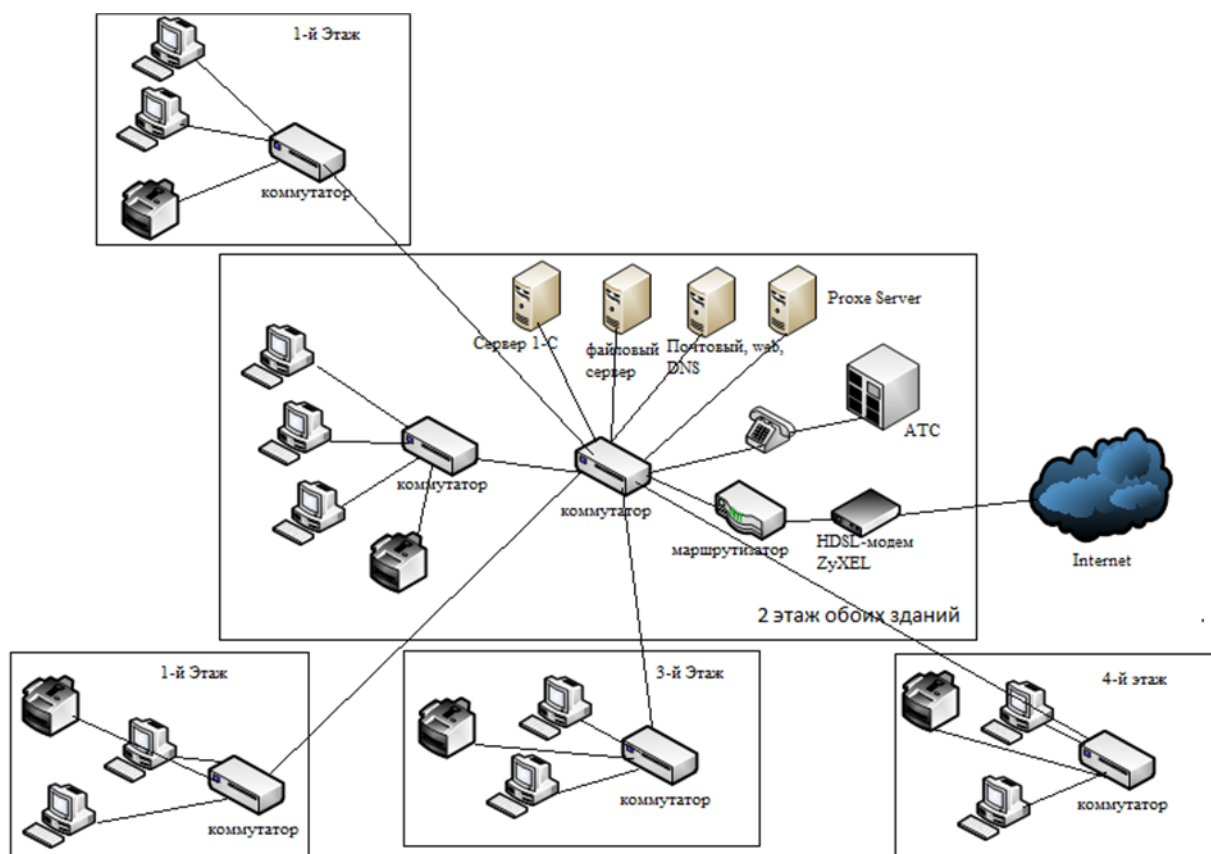


Рисунок 3.1 – Структурна схема проектованої мережі

В даному проекті поставлено завдання модернізувати ЛОМ високошвидкісної мережі зі швидкістю передачі даних - 100 Мбіт/сек. Для взаємодії визначається протокол TCP/IP. Топологія мережі - зірка.

Для доступу в глобальну мережу Інтернет використовуємо SHDSL-модем зі швидкістю 15 Мбіт/с. Канал буде орендований у магістрального Інтернет-провайдера «ТОВ» СПІКОМ. Доступ в Інтернет здійснюється через сервер з встановленим програмним забезпеченням проксі-сервера (сервер 1). Захист від хакерів реалізується за участю брандмауера, що входить до складу проксі-сервера. Додатково захист мережі організовується за допомогою брандмауера провайдера. На всіх серверах і робочих станціях буде встановлено відповідне антивірусне ПЗ.

Сервер 2 виконує функції файлового сервера.

Сервер 3 є сервером баз даних підприємства.

Сервер 4 виконує функції поштової служби - на даний сервер приходить зовнішня (Інтернет) і внутрішня електронна пошта. До нього підключені принтери загального користування, тобто додатково він є сервером друку.

Мережеві служби, побудовані на основі комп'ютерних мереж, створюються за допомогою спеціалізованого клієнт-серверного мережевого програмного забезпечення, яке входить до складу мережевих ОС.

Для організації телефонного зв'язку передбачається використовувати VoIP-шлюзи, підключені до локальної мережі з одного боку і до офісної міні-АТС з іншого. Вихід на міжміські і міжнародні лінії буде забезпечений за допомогою VoIP-шлюзів і Softswitch, що виконують маршрутизацію дзвінка по каналах Інтернет до VoIP-провайдера, який надає послуги міжміського/міжнародного зв'язку.

3.1.4 Розробка горизонтальної кабельної підсистеми

Створювана СКС повинна забезпечити функціонування обладнання локальної обчислювальної мережі, а також вихід в Internet.

При виборі СКС в якості кабельної підсистеми використовується топологія "зірка" і технологія Fast Ethernet.

Вибір кабелю і аксесуарів

Як кабелю горизонтальної підсистеми буде використовуватися кабель UTP cat. 5e фірми Molex (рисунок 3.2), в якому знаходиться вісім провідників, перевитих попарно (тобто 4 пари). Даний вид кабелю є найдешевшим з'єднанням, дозволяє передавати дані зі швидкістю до 100 Мбіт/с, легко нарощується, не викликає особливих складнощів при монтажі, довжина сегмента не перевищує 100 метрів, що задовольняє умовам проекту.

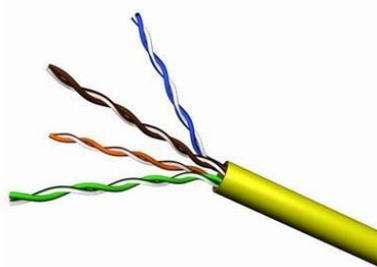


Рисунок 3.2 – Кабель Molex категорії 5e

Цей кабель продається в бухтах по 305 м. Для прокладки 3025 м кабелю буде потрібно 10 бухт.

Як кабелю магістральної підсистеми вибираємо одномодовий кабель ІКС-М - оптичний кабель для прокладки в каналізацію на основі модульної конструкції. Оптичні кабелі марки ІКС призначені для прокладки в ґрунті 1-3 категорії, в тому числі, зараженому гризунами, а також в кабельної каналізації, трубах, на мостах і естакадах. Допускається прокладати кабель в тунелях, колекторах, будівлях.

У кабінетах для розведення кабелю використовується система декоративних коробів і фальшстеля, а в коридорі - фальшстеля, де в якості кріплення кабелю до стелі використовуються стельові гаки. введення кабелів з коридору в кабінети виконується під фальшстелею, далі одним вертикальним спуском від фальшстелі до ІР по декоративному короба, довжина якого становить 3м.

Короба для прокладки в приміщеннях були обрані фірми Legrand (рисунок 3.3).



Рисунок 3.3 – Кабель-канал 40 × 16мм, заглушки, кутки Legrand

3.2 Конфігурування програмних засобів

3.2.1 Операційна система для серверів

- В якості операційної системи для серверів виберемо ОС
- Windows Server 2016 Standard, вибір обумовлений високою надійністю ОС і відмінними функціональними можливостями.

- Windows Server 2016 - операційна система, яка є частиною сімейства Windows NT, призначена для роботи на серверах. Вона була випущена 29 вересня 2016 року. Windows Server 2016 доступна в шести основних виданнях, кожне з яких орієнтоване на певний сектор ринку.

- Windows Server 2016 Datacenter - редакція для середовищ з високим використанням віртуалізації;

- Windows Server 2016 Standard - редакція для середовищ без потреби або з малим ступенем використання віртуалізації;

- Windows Server 2016 Essentials - редакція для малого бізнесу, обмежена 25 користувачами і 50 пристроями;

- Windows Server 2016 Multipoint Premium Server - редакція, спеціально призначена для великої кількості користувачів;

- Windows Storage Server 2016 - спеціальна редакція для організації дискових сховищ;

- Microsoft Hyper-V Server 2016 - безкоштовна версія гіпервізора.

Таблиця 3.1 – Системні вимоги Windows Server 2016

Комплектуючі	Мінімальні вимоги	Рекомендовані вимоги
ОЗУ	512 (2 ГБ для варіанту установки «Сервер з робочим столом»)	4 ГБ оперативної пам'яті і вище Максимально: 24 Тб ОЗУ
Відеокарта і монітор	1024 * 768	1024 * 768 і вище
Вільне місце на жорсткому диску	32 ГБ	40 ГБ і вище
Інші приводи	DVD-ROM	DVD-ROM
Інші пристрої	Клавіатура і миша	Клавіатура і миша

3.2.2 Операційна система для робочих станцій

В якості операційної системи для комп'ютерів виберемо ОС Windows 10, вибір обумовлений високою поширеністю ОС, відмінною функціональністю, простотою і доступністю.

Windows 10 - призначена для користувача ОС із сімейства Windows NT, вийшла на зміну Windows 8. Станом на 2020 рік Windows 10 є найпопулярнішою операційною системою в світі. перший випуск був 20 липня 2015 року.

Windows 10 випускається в багатьох редакціях:

- Початкова (Starter) - урізана версія, яку ви можете придбати лише при покупці комп'ютера або ноутбука; несе тільки ознайомчу особливість.

- Домашня базова (Home Basic) - це редакція початкового рівня, яка призначена клієнтам з недорогими робочими станціями. Вона має всі переваги Windows 7 (Безпека, надійність, швидкість роботи, активні ескізи, розширена підтримка роботи в мережі та ін.)

- Домашня розширена (Home Premium) - це найкраща редакція для домашніх користувачів. У ній можна легко підключатися до інших комп'ютерів і пристроїв в інтерфейсі з безліччю візуальних ефектів. У цій редакції ОС підтримується створення домашньої групи, яка дозволяє спільно з іншими

підключеними до мережі комп'ютерами Windows 10 звертатися до різного вмісту: улюбленим фотографіям, відеозаписів або музичних файлів.

- Професійна (Professional) - поєднує всі необхідні бізнес-функції з розважальними можливостями в редакції Windows 7 Домашня розширена. Ви зможете запускати безліч робочих програм для Windows XP безпосередньо в Windows 10 або за допомогою режиму Windows XP, а також без праці відновлювати дані завдяки можливостям автоматичного резервного копіювання в домашній або робочій мережі. Підключення до мереж компанії стало простіше і безпечніше.

- Корпоративна (Enterprise) - Ця версія призначена, перш за все, для ІТ-фахівців, щоб надати їм можливість ознайомитися з ОС в рамках організації. Дана редакція поширюється виключно для програми ліцензування та має 90-денний термін безкоштовного використання для ознайомлення.

- Максимальна (Ultimate) - це найбільш повнофункціональна і потужна редакція, призначена для потреб корпоративних клієнтів, яким необхідний повний набір можливостей Windows 10. Ця редакція дає можливість ефективно працювати де завгодно, підвищує безпеку і контроль і оптимізують управління ПК. Вона також забезпечує гнучкий інтерфейс з підтримкою різних мов.

Таблиця 3.2 – Мінімальні апаратні вимоги до апаратного забезпечення ЕОМ Windows 10

Процесор:	1 ГГц і швидше з підтримкою PAE, NX і SSE2
RAM:	1 Гбайт (32 біт) або 2 Гбайт (64 біт)
HDD:	16 Гбайт (32 біт) або 20 Гбайт (64 біт)
Відеокарта:	підтримка Microsoft DirectX 9 з драйвером WDDM .

3.2.3 Мережеві служби

Мережева служба (сервіс) - це певний вид обслуговування, надається сервером.

Файлова служба. На комп'ютері з великим об'ємом дискового простору мережева ОС налаштовується таким чином, щоб інші комп'ютери (клієнти)

мали змогу використовувати даний простір для запису файлів за рахунок комп'ютерної мережі. Такий сервер називається файловим або файл-сервером.

Для створення файлової служби використовуємо FTP-Server, що дозволяє використовувати це програмне забезпечення для підключення до FTP-сервера, перегляду вмісту каталогів та завантаження файлів із сервера. Також є можливість передавати файли між серверами.

Служба друку. На комп'ютері, до якого підключений принтер, мережева операційна система налаштовується таким чином, щоб інші комп'ютери (клієнти) також могли роздруковувати свої документи. Ефективність використання дорогих пристроїв (принтерів) при цьому збільшується.

Для організації служби друку використовуємо Microsoft Office – пакет додатків, створених корпорацією Microsoft для операційних систем Microsoft Windows та Apple Mac OS X. До складу цього пакету входить програмне забезпечення для роботи з різними типами документів: текстами, електронними таблицями, базами даних тощо.

Управління базами даних. Як в локальних, так і в глобальних мережах важливим завданням є зберігання і обробка великих обсягів табличних даних. До систем, які керують базами даних, висуваються вимоги надійного централізованого зберігання інформації, швидкого пошуку, вибірки за запитом з будь-якої робочої станції мережі. Ці послуги виконує сервер баз даних.

Для управління базами даних будемо використовувати MySQL - вільна система управління базами даних (СУБД).

MySQL - це рішення для малих та середніх додатків. MySQL, як правило, використовується як сервер, до якого мають доступ місцеві або віддалені клієнти. Однак дистрибутив включає внутрішню бібліотеку сервера, яку можна використовувати для додавання MySQL до автономної програми.

Web-служба

Веб-служба є найпопулярнішою службою Інтернет. веб-служба надає користувачам в інтерактивному режимі електронні документи - гіпертекстові документи (гіпертексту), що передаються по протоколу HTTP.

Браузер - це програма, яка дозволяє отримувати інформацію з глобальної мережі Інтернет. Найпопулярнішими браузерами є Opera, Mozilla, Firefox, Google Chrome. Основні відмінності між браузерами полягають в швидкості роботи. Для організації Web служби в нашій мережі будемо використовувати браузер Google Chrome.

Google Chrome (Гугл Хром) - інтернет веб-браузер, за допомогою якого ви зможете більш безпечно і швидко працювати в Інтернеті. Розроблено компанією Google і має відкритий вихідний код.

Розробники Хрома виділяють дві головні особливості - це ізольовані вкладки, які виключають ризик збою програми (при одній завищій вкладці всі інші продовжують працювати), а також більш надійні механізми захисту від небезпечних сайтів в інтернеті.

Поштова служба

Для доставки електронних листів в комп'ютерних мережах використовують поштові сервіси. Електронні листи зазвичай використовують для передачі текстової, графічної та рідше звукової інформації.

Для організації поштової служби використовуємо Courier Mail Server - це поштовий сервер (сервер електронної пошти) під Windows для офісних і домашніх мереж.

Переваги:

- компактність, простота установки і видалення;
- легкість настройки і адміністрування;
- мале споживання системних ресурсів;
- багатопоточність;
- зручна графічна оболонка;
- оперативна технічна підтримка.

Основні можливості:

- SMTP- і POP3-сервіси;
- Web-сервер з підтримкою PHP (HTTP-сервіс);

- проксі-сервер (SOCKS-сервіс);
- робота системною службою (сервісом);
- підтримка декількох поштових доменів;
- гнучка сортування і антиспам-фільтрація пошти;
- обмеження розмірів локальних поштових скриньок;
- псевдоніми користувачів і доменів;
- списки розсилки на основі псевдонімів;
- відправка пошти на фіксовані сервера (smart hosts);
- доставка пошти безпосередньо на сервера одержувачів (MX-delivery);
- автоматичне повторення відправлення вихідної пошти;
- повідомлення про недоставку листів, віруси та інші події;
- розмежування прав доступу по IP-адресами клієнтів;
- перегляд списку підключень з можливістю відключення;
- збирач пошти з зовнішніх поштових скриньок;
- обробка листів зовнішніми додатками (архіватор, антиспам);
- використання віддаленого доступу (RAS dial-up);
- вибір мови інтерфейсу.

Проксі-сервер

Дефіцит IP-адрес в мережі Інтернет, а також необхідність захисту локальної мережі від зовнішніх несанкціонованих проникнень привели до появи спеціальних шлюзів - проксі-серверів.

Більшість проксі-серверів використовуються для таких цілей.

- кешування (стиснення) інформації: проксі-сервер завантажує інформацію з інтернету і передає інформацію кінцевому користувачеві в стислому вигляді. Такі проксі-сервери використовуються в основному з метою

економії зовнішнього трафіку клієнта або внутрішнього - компанії, в якій встановлений проксі-сервер;

- захист ЛМ від зовнішнього доступу: Ви можете налаштувати проксі-сервер, наприклад, таким чином, щоб локальні комп'ютери мали доступ лише до зовнішніх ресурсів через цей доступ, а зовнішні комп'ютери не могли отримати до них доступ локально (Проксі-сервер видно лише їм);

- лімітування зовнішнього доступу через ЛМ. Наприклад, ви можете заборонити доступ до деяких веб-сайтів, обмежити доступ до інтернету певним місцевим користувачам, встановити квоти трафіку або пропускну здатність, фільтрувати рекламу та віруси.

Для організації захисту інформаційних ресурсів та економічно вигідного і безпечного їх використання будемо використовувати VPN-продукти «ЗАСТАВА».

Послідовний і системний підхід до побудови захищених мереж передбачає не тільки захист зовнішніх каналів зв'язку, а й ефективний захист внутрішніх мереж шляхом виділення замкнутих внутрішніх контурів VPN, які використовуються певним набором комп'ютерів з певними бізнес-додатками. При цьому нова сегментація буде відображати тільки структуру бізнес-процесів корпорації і не залежати від конкретної топології і сегментації внутрішніх локальних мереж.

Сімейство VPN продуктів ЗАСТАВА складається з власне VPN продуктів, що встановлюються в контрольних точках мережі (Клієнт-Сервер-Шлюз), а також з продуктів управління корпоративною VPN. Комплекс цих продуктів надає користувачам повне і гнучке рішення попостроенню корпоративних VPN.

VPN- клієнт ЗАСТАВА

VPN-клієнт ЗАСТАВА-Клієнт служить для аутентифікації користувачів корпоративної VPN, захисту локальних ресурсів робочих станцій мережі від

несанкціонованого доступу, а також для забезпечення захищеного взаємодії віддалених користувачів зі шлюзами і хостами корпоративної мережі незалежно від способу доступу до мережі: dial-up, з іншого ЛВС або через Інтернет-провайдера.

Застава-Клієнт поставляється в двох модифікаціях: Застава-Персональний Клієнт і Застава-Корпоративний Клієнт. При використанні продукту Застава-Персональний Клієнт політика інформаційної безпеки задається самим користувачем за допомогою набору конфігураційних правил за допомогою графічного інтерфейсу користувача. Застава-Корпоративний Клієнт не має інтерфейсу користувача. Конфігурація продукту відбувається централізовано адміністратором безпеки. На віддалені комп'ютери конфігурація завантажується за допомогою дискети, смарт-карти або е-токена.

VPN-сервер ЗАСТАВА

VPN-сервер ЗАСТАВА-Сервер забезпечує захист локальних ресурсів сервера, таких як бази даних, додатки, веб-сайт і т.д. від несанкціонованого доступу з будь-якої точки мережі. Продукт також забезпечує захищені IP з'єднання з іншими комп'ютерами і шлюзами мережі, захищеними VPN-продуктами сімейства ЗАСТАВА і / або SKIP-продуктами інших виробників. Крім того, Застава-Сервер дозволяє підтримувати захищене з'єднання із мобільними користувачами Застава-Клієнт, що не мають постійних IP-адрес.

VPN-шлюз ЗАСТАВА

VPN-шлюз ЗАСТАВА-Офіс забезпечує колективний захист локальної мережі (сегмента локальної мережі) від несанкціонованого доступу із зовнішніх (внутрішніх) мереж. Застава-Офіс також забезпечує організацію захищених IP з'єднань (асоціацій) між локальними мережами корпоративної мережі, а також з віддаленими комп'ютерами і серверами з сегментів локальних мереж, захищених VPN-продуктами сімейства ЗАСТАВА і / або SKIP-продуктами інших виробників. Застава-Офіс також може виконувати функції фільтрації

трафіку при спільному використанні з програмним продуктом - Брандмауер Застава.

Брандмауер ЗАСТАВА

Являє собою пакетний фільтр, який забезпечує захист ресурсів локальної мережі від несанкціонованого доступу з зовнішніх мереж, а також сегментацію мережі відповідно до організаційної структури та політикою безпеки компанії. Продукт сертифікований Держтехкомісії РФ по 3-му класу захищеності РД для МЕ.

Сервер сертифікатів ЗАСТАВА

Сервер сертифікатів ЗАСТАВА являє собою програмний продукт рівня підприємства, який призначений для створення БД сертифікатів корпоративних користувачів VPN (PKI Directory Server), а також для інтеграції VPN Застава із зовнішніми стандартними системами PKI. Сервер сертифікатів Застава призначений для завантаження X.509 v.1-3 сертифікатів користувачів в стандартну БД, верифікації цифрового підпису кожного сертифіката, а також їх автоматичного розподілу за запитами VPN пристроїв за допомогою Certificate Discovery Protocol (CDP). Сервер сертифікатів Застава може обмінюватися сертифікатами з іншими системами PKI за допомогою протоколу LDAP, будучи проксі-сервісом між зовнішньої LDAP-сумісної службою PKI і корпоративної VPN, побудованої на базі VPN Застава.

Центр управління ЗАСТАВА

Центр управління ЗАСТАВА служить робочим інструментом Адміністратора безпеки корпоративної VPN, який призначений для генерації, цифрового підпису та експорту на зовнішні носії (дискети, смарт-карти, е-токени) конфігурацій локальної політики безпеки (ЛПБ) для VPN продукту Застава - Корпоративний Клієнт. ЛПБ містить профіль безпеки кожного користувача корпоративної VPN і визначає права доступу користувача до корпоративних інформаційних ресурсів.

4 ТЕХНІКО-ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ

Тема дипломної роботи «Розробка локально-обчислювальної мережі підприємства роздрібної торгівлі з використанням багаторівневого комутатора Dell N4032F». В роботі здійснюється розробка проекту локальної мережі, з метою оптимального підбору пасивного та активного апаратного забезпечення, і програмних засобів.

4.1 Розрахунок капітальних витрат

Реалізація проекту локальної мережі потребують капіталовкладень. У цьому розділі наведена техніко-економічна оцінка прийнятих проектних рішень, характеризує доцільність проекту. Оцінка економічної ефективності капітальних вкладень здійснюється на основі зіставлення економічного ефекту і витрат.

Капітальні витрати включають в себе кошторисну вартість обладнання проекрованої мережі, кошторисну вартість монтажних робіт і налаштування обладнання, транспортні витрати, затрати на розробку проекту без ПДВ.

Таблиця 4.1 – Розрахунок кошторисної вартості обладнання

Тип обладнання/роботи	Ціна за одиницю з ПДВ, грн.	Кількість, од.	Загальна вартість з ПДВ, грн.
Коммутатор Allied Telesis AT-8000S/24	7100	4	28 400
Коммутатор Allied Telesis AT-8000S/48	31000	1	31 000
Коммутатор 2-го уровня Dell 4032F/24POE	42000	1	42 000
Маршрутизатор Cisco 2821-SEC/K9 SE-CURITY BUNDLE, ADV SECURITY, 64F/256D	32000	1	32 000
Медиа-конвертор ALLIED TELESIS AT-FS202	4573	4	18 292
SHDSL модем SG-17BT	14000	1	14 000
ИБП APC Smart-UPS SUA3000I	53913	5	269 565
Цифровая АТС Samsung IDCS 500	3543	1	3543

Тип обладнання/роботи	Ціна за одиницю з ПДВ, грн.	Кількість, од.	Загальна вартість з ПДВ, грн.
VoIP-Шлюз AddPac AP2620-2E1	153486	1	153 486
Рабочая станция	9800	71	695 800
Принтер Epson M105	5182	9	46 638
Серверы Kraftway Express ISP ES12	41624	4	166 496
Напольный шкаф 19"серии ШТК-М 42U	25754	1	25 754
Настенный шкаф 19" серии ШРН 12U	4417	4	17 668
Полка стационарная, 600 мм	432	8	3456
Кабельный органайзер 1 U 5 колец 60 мм	194	6	1 164
Патч-панель 19", 2U, 48 портов RJ45, категория 5е, Krone IDC	2927	6	17 562
Патч-корд UTP, кат.5е, 2м	31	92	2 852
Розетка RJ45 двойная категории 5е Keystone	50	92	4600
Кабельный канал 20×16мм (2,0м), (шт.)	22	121	2662
Кабельный канал 100×60мм (2,0м)	59	5	295
Металлический лоток ПЛМ-100.60	224	40	8 960
Блок сетевых розеток на 7 гнезд с автоматическим выключателем	518	5	2 590
Кабель UTP Molex категории 5е, бухта	4424	10	44 240
Кабель многомодовый ОКС-М8Т-50-0,7-04	10000	2,75	27 500
Итого по пункту 1			1 660 523
2. Стоимость неучтенного оборудования (15% от суммы п.1)			249 078,45
Итого по смете			1 909 601,45

Витрати на монтажні роботи складають 30% від витрат на обладнання. Витрати на проектні роботи складають 10% від витрат на обладнання. Витрати на транспортування становлять 13,1% від витрат на обладнання.

У таблиці 4.2 представлений зведений кошторис капітальних витрат на реалізацію проекрованої мережі.

Таблиця 4.2 – Зведений кошторис капітальних витрат на реалізацію проекрованої мережі

Найменування витрат	Сума, грн.	Питома вартість, %
Витрати на оборудование	1 909 601,45	65
Витратина монтажные работ	572 880,44	19,5
Витрати на проектные работы	190 960,15	6,5
Витрати на транспортные услуги	250 157,79	9
Итого:	2 923 599,83	100

Оскільки всі наведені в таблицях ціни містять ПДВ, потрібно розрахувати капітальні витрати без ПДВ.

$$K_{\text{безПДВ}} = \frac{K_{\text{зПДВ}}}{1.18} = \frac{2923599.83}{1.18} = 2477627 \text{ грн}$$

4.2 Розрахунок основних виробничих фондів

Величина капітальних вкладень, що переходять в основні виробничі фонди (ВПФ) проектного об'єкта, приймається на підставі середнього значення, отриманого на основі галузевих звітних даних, і прийнята 0,97 (або 97%) від капітальних вкладень, розрахованих без ПДВ.

$$\Phi = 0,97 \cdot K_{\text{безПДВ}}$$

$$\Phi = 0,97 \cdot 2477627 = 2403298,2 \text{ грн}$$

4.3 Розрахунок експлуатаційних витрат

Експлуатаційні витрати складаються з фонду оплати праці (ФОП), страхових внесків, витрат на електроенергію, витрат на матеріали і запасні частини, амортизаційні відрахування та інші витрати.

Річний фонд оплати праці (ФОП) працівників, які обслуговують проектовану мережу, розраховується за формулою:

$$E_{\text{ФОП}} = Ч \cdot Z_{\text{пл.ср}} \cdot K_{\text{тер.к}} \cdot 12 \text{ грн}$$

де Ч - чисельність працівників;

$Z_{\text{пл.ср}}$ - середня місячна заробітна плата, що склалася в експлуатаційних підприємствах аналогічного типу;

$K_{\text{тер.к}}$ - районний коефіцієнт.

Відповідно до норм чисельності обслуговуючого персоналу для групи інформаційних технологій, для обслуговування активного устаткування і структурованої кабельної системи необхідно 3 одиниці штату. Середньомісячна заробітна плата одного працівника становить 10000 грн. Районний коефіцієнт для міста Запоріжжя складає 30%.

$$E_{\text{ФОП}} = 3 \cdot 10000 \cdot 1,3 \cdot 12 \text{ грн} = 468000 \text{ грн}$$

Страхові внески складають 30% від фонду оплати праці, де:

- відрахування в пенсійний фонд - 22%;
- відрахування на соціальне страхування - 2,9%;
- відрахування на обов'язкове медичне страхування - 5,1% .

$$E_{\text{СТР.ВЗ.}} = E_{\text{ФОП}} \cdot 0,3 = 468000 \cdot 0,3 = 140400$$

Амортизаційні відрахування на повне відновлення визнаються виходячи із середньорічної вартості основних виробничих фондів і встановлених норм амортизації за формулою:

$$\mathcal{E}_{\text{ФОП}} = \frac{\Phi \cdot \overline{N_A}}{100\%}$$

де N_A - середня норма амортизації, %;

Φ - вартість основних виробничих фондів.

Розрахунок амортизаційних відрахувань показаний в таблиці 4.3.

Таблиця 4.3 – Амортизаційні відрахування

Вид ОПФ	Вартість ОПФ, грн.	Середня норма амортизації, %	Амортизаційні відрахування, грн
Обладнання	1 909 601,45	20	415 475
Кабель	71740	5	3587
Ітого $E_{\text{АМ}}$			419 062

Витрати на електроенергію визначають виходячи з споживаної потужності обладнання та діючих тарифів: по одноставочному тарифу (при

загальній потужності мережі менше 750 кВт), по двоставковому тарифу (при загальній потужності мережі понад 750 кВт). Потужності активного обладнання, використовуваного в даному проекті, наведені в розділі 2.

Розрахунок потужності, споживаної активним обладнанням на годину, приведено в таблиці 4.4.

Таблиця 4.4 – Розрахунок потужності, споживаної активним обладнання на годину

Перелік обладнання	Кількість, шт.	Потужність, Вт.	Загальна потужність, Вт.
Коммутатор Allied Telesis AT-8000S/24	4	26,5	106
Коммутатор Allied Telesis AT-8000S/48	1	32,6	32,6
Коммутатор 2-го уровня Dell 4032F/24POE	1	45	45
Маршрутизатор Cisco 2821-SEC/K9 SECURITY BUNDLE, ADV SECURITY,64F/256D	1	54	54
Медиа-конвертор ALLIED TELESIS AT-FS202	3	6	18
Цифровая АТС Samsung IDC5 500	1	500	500
VoIP-Шлюз AddPac AP2620-2E1	1	10	10
SHDSL модем SG-17BT	1	2	2
Серверы Kraftway Express ISP ES12	4	500	2000
Рабочая станция	71	300	21300
Принтер Epson M105	8	10	80
Итого:	-	-	24147,6

$$W = \frac{(\sum N_i \cdot W_i \cdot t_i)}{\eta}$$

де N_i – кількість одиниць обладнання певного типу, шт(88);

W_i – потужність, споживана за годину роботи одиницею обладнання, Вт;

t_i – час дії обладнання за рік в годинах (365×10 годин);

η – коефіцієнт корисної дії (0,8).

Загальна потужність, споживана активним обладнанням за рік:

$$W = \frac{24147.6 \cdot 365 \cdot 24}{0.8} = 264416.2, \text{ кВт}$$

На даний момент часу одноставковий тариф для промислових споживачів Запоріжжя складає 90 коп. за 1 кВт-год без ПДВ. Тоді витрати на електроенергію в рік становитимуть:

$$E_{\text{ЕЛ/ЕН}} = 264416,2 \cdot 0,9 = 237\,974,58 \text{ грн}$$

Інші витрати визначаються виходячи із ситуації, що структури витрат і складають 10% від загальної суми витрат. До інших витрат відносяться адміністративно-управлінські та експлуатаційно-господарські витрати:

$$E_{\text{ІНШІ}} = 10575254,2 \cdot 0,1 = 1057525,42 \text{ грн}$$

Таблиця 4.5 – Підсумок

Стаття витрат	Сума, грн.	Структура, %
Фонд заробітної плати	468000	43,2
Страхові внески	140400	13,1
Амортизаційні відрахування	419 062	2,1
Витрати на електроенергію	237974,58	40,2
Інші витрати	1057525,42	1,4
Ітого:	2 322 962	100



Рисунок 4.1 – Карта стейкхолдерів

Висновки

Використання ПК може зменшити витрати таких ресурсів, як час, персоналу та фінансів. Однак автономні комп'ютери не призводять до такого ефекту, що дає розгортання локальної обчислювальної мережі (ЛОМ). Її впровадження підвищить ефективність та результативність роботи підрозділів, знизить час, що йде на підрахунки та обмін результатами між відділами, оптимізуючи трудовитрати компанії.

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА У НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Тема дипломної роботи «Розробка локально-обчислювальної мережі підприємства роздрібної торгівлі з використанням багаторівневого комутатора Dell N4032F». В роботі здійснюється розробка проекту локальної мережі, з метою оптимального підбору пасивного та активного апаратного забезпечення, і програмних засобів.

5.1 Аналіз потенційних небезпек

Умовно їх можна розділити на організаційні, технологічні, санітарно-гігієнічні та психофізіологічні причини.

Організаційні причини включають в себе низький рівень грамотності, професійної підготовки та освіти працівника, відсутність достатнього досвіду і навичок в роботі, нехтування вимогами безпеки, недисциплінованість, безвідповідальність (порушення інструкцій, технічних вказівок, правил експлуатації і т.п.)

Технологічні причини - це низький технічний рівень обладнання та технологій, невідповідність їх характеристик світовим стандартам, несправність обладнання і порушення техпроцесів, низький рівень ефективності захисних заходів, несправність засобів захисту і пристосувань.

Санітарно-гігієнічні причини включають в себе невідповідність вимогам санітарних норм (правил, стандартів), характеристик виробничого середовища (освітлення, мікроклімат, шуми, вібрація, різні випромінювання і т.п.). Ці причини сприяють швидшому зниженню працездатності, ведуть до стомлення і як наслідок - порушення координації руху, погіршення уваги і підвищенню ймовірності травмування.

Психофізіологічні причини - це фізичні та нервово-психічні перевантаження, стан втоми і інші психічні стани, що виникають в результаті зовнішніх впливів або властивих даної особистості, що сприяють стомлення.

5.2 Заходи по забезпеченню техніки безпеки

Сучасне виробництво немислимо без широкого використання електричної енергії. Підвищуючи продуктивність праці і культуру виробництва, електричний струм в той же час представляє велику небезпеку для життя і здоров'я людей. На відміну від інших небезпек електричний струм неможливо виявити дистанційно без приладів.

Поразка людини електрострумом можлива при замиканні електричного кола через його тіло, що може мати місце при дотику людини до мережі не менше ніж в двох точках (наприклад, при двофазному включенні в мережу; однофазному включенні в мережу, стоячи на землі або торкаючись будь-яких заземлених конструкцій; при контакті з неструмопровідними частинами обладнання, випадково опинилися під напругою через порушення ізоляції проводів електроживлення обладнання або електрифікованого інструменту та ін.).

Захист і попередження уразки електрострумом або електробезпека включає в себе низку систем організаційних і технологічних заходів, технічних засобів, що створюють безпечні умови праці робітників з технологічним обладнанням і ручним інструментом, що використовують електроенергію, з метою скорочення електротравматизму до прийнятного (і нижче) рівня ризику.

Статистичні дослідження нещасних випадків з причин електропоразки показує, що загальне число травм, спричинених електричним струмом з втратою працездатності, невелика і складає приблизно 0,5-1,0% (в енергетиці 3-3,5%) від загальної чисельності нещасних випадків на підприємстві.

Однак зі смертельними наслідками такі випадки на виробництві становлять 30-40%, а в енергетиці до 60%. Згідно зі статистикою 75-80% смертельних уразок електрострумом трапляється в установках, електроживлення яких здійснюється напругою 380/220 і 220/127 В.

Вплив електроструму на людину

Коли електрострум проходить через організм, це призводить до термічного, електролітичного і біологічного впливу.

Термічний вплив проявляється в опіками уражених ділянок тіла, нагріванні кровоносних і нервових тканин.

Електролітичний вплив проявляється розкладанням крові та інших органічних рідин, порушуючи їх фізико-хімічний склад.

Біологічний вплив виражається в подразнюванні і ураженні живих тканин організму, що спроможне супроводжуватися довільними судомими м'язових тканин, у т.ч. серця та легень. У підсумку можуть з'явитись різноманітні порушення, в т. ч. поразка аж до повного припинення життєдіяльності органів, що відповідають за процеси дихання і кровообігу.

Подразнюючу дію, що струм чинить на тканини, буває прямим, в тому випадку, якщо струм проходить по цим тканинам безпосередньо; рефлекторним, в тому випадку, коли струм уражує через центральну нервову систему, і шлях протікання електроструму проходить за межами цих органів.

Ураження електрострумом поділяються на два види: електричні травми і електричні удари.

Електрична травма - це пошкодження біологічних тканин, локальні та чітко виражені, виникають в результаті дії електричного струму або електричної дуги.

Електричний удар - це обурення біотканей людини електрострумом, який проходить крізь нього, при цьому спостерігаються мимовільні судоми м'язів.

Класифікація електроударів:

I – судоми м'язів, свідомість зберігається;

II – судоми м'язів, втрачається свідомість, серце та легені працюють;

III – втрачається свідомість у супроводі з порушенням робочого режиму серця або легенів (або і те, і інше);

IV – клінічна смерть, відсутні процеси дихання та кровообігу.

Основні причини смерті від електроструму – це припинення биття серця, зупинка дихання та електрошок.

Фібриляція серця (тобто швидкісні хаотичні скорочення фібрил серцевого м'яза, внаслідок чого дія серця як насоса припиняється, в результаті чого в організмі перестають виконуватися процеси кровообігу, це може трапитись при прямому або рефлекторному впливі електроструму.

Зупинка дихання як головна причина смерті від електроструму провокується прямою або рефлекторною дією струму на м'язи грудної клітини, робота яких супроводжує процес дихання, результатом припинення їхньої активності є асфіксія (задуха через недостатню кількість кисню в організмі і надлишок CO_2).

Електричний шок – потужна реакція організму, що виникає в результаті інтенсивного електричного впливу, яка протікає вкупі з небезпечними порушеннями кровообігу, дихання, метаболізму і т.п. Цей стан може зберігатися від декількох хвилин до доби.

Прийнято такі заходи націлені на забезпечення електробезпеки

Застосування низьких напруг в межах найбільших допустимих значень для електроживлення приладів, електрифікованого ручного інструменту і установок є найбільш ефективним способом забезпечення електробезпеки. Тому в тих випадках, де це можливо, необхідно використовувати більш низькі напруги, що не перевищують Упр ПД.

З цією метою для електроживлення переносних установок і ручного інструменту (електричні дрилі, гайковерти, електричні паяльники та ін.) допускаються такі максимальні значення напруги в залежності від місця роботи (вид приміщення за безпекою уразки електрострумом, зовнішні умови і ін.):

- 220 В (50 Гц) при використанні установок в приміщеннях без властивостей високої і особливої небезпеки ураження електрострумом;

- 42 В (50 Гц) в приміщеннях з наявністю властивостей високої небезпеки ураження електрострумом і при роботах в зовнішніх умовах.

В таких умовах роботи допускається використовувати інструмент (переносні установки) до 220 В, але з невідворотнім застосуванням основних і додаткових ізолюючих засобів; 42 В (50 Гц) в приміщеннях з наявністю ознак особливої небезпеки з обов'язковим застосуванням основних і додаткових ізолюючих засобів.

Для електроживлення переносних світильників допускаються такі максимальні значення напружень:

- 42 В (50 Гц) в приміщеннях з наявністю властивостей підвищеної і особливої небезпеки;

- 12 В (50 Гц) - при роботах в особливо небезпечних і несприятливих умовах.

До ознак високої небезпеки уразки електрострумом в виробничих приміщеннях відносяться: наявність в приміщенні струмопровідних підлог (земляні, металеві, залізобетонні, цегляні і т.п.); підтримання в приміщенні тривалий час (більше 2 годин) температури повітря дорівнює або вище 25 ° С і відносній вологості рівною або більше 75%; наявність в повітрі струмопровідного пилу; наявність вірогідності одночасного дотику до корпусів і інших частин обладнання, на яких може виявитися напруга, з одного боку, і до будь-яких заземлених конструкцій будівлі, іншого обладнання, з іншого.

До ознак особливої небезпеки приміщень відносяться: наявність в приміщенні двох або більше ознак підвищеної небезпеки; наявність в повітрі приміщення хімічно агресивного середовища; підтримання в приміщенні високій відносній вологості, близької до 100%.

Як джерела малого (низького) напруги застосовуються гальванічні елементи, випрямлячі, перетворювачі частоти (для зменшення маси ручного інструменту на частоті 200 або 400 Гц), що знижують трансформатори і ін. Використання з цією метою автотрансформаторів не допускається, тому що в цьому випадку зберігається гальванічна зв'язок автотрансформатора з електричною мережею, а значить і небезпека електропоразки при замиканні («пробої») напруги електроживлення на корпусу або інші частини таких пристроїв.

Електричне поділ мереж. Полягає у використанні розділових трансформаторів за допомогою яких мережі великої протяжності або мережі, які мають велику кількість відгалужень поділяються на окремі невеликі мережі того ж напруги.

Електричне поділ мереж дозволяє забезпечити опір фазних проводів по відношенню до землі досить великим (≥ 500 кОм в мережах до 1000 В) і тим самим забезпечити їх безпеку при однофазному дотику.

Для поділу мереж можуть застосовуватися також перетворювачі частоти і випрямні установки.

Захисне заземлення являє собою цілеспрямоване електричне з'єднання металевих фрагментів устаткування (наприклад, корпусів), які можуть опинитися під напругою через порушення ізоляції провідникових частин обладнання (і з інших причин), з землею за допомогою заземлювального пристрою.

5.3 Заходи з виробничої санітарії та гігієни праці

Виробнича санітарія включає в себе очистку повітря робочої зони від речовин, що здатні зашкодити здоров'ю, організацію оптимальних і допустимих якостей мікроклімату, іонізацію повітряного середовища, організацію раціонального освітлення і вентиляції на робочих місцях, захист від різного виду випромінювань і ін .

Повітряне середовище, в якій здійснюється виробнича діяльність людини, характеризується хімічним складом, фізичними параметрами та іншими показниками, які надають значний вплив на здоров'я працюючих, їх психофізіологічний стан і працездатність.

Атмосферне повітря, найбільш сприятливий для дихання, в своєму складі містить 78,08% азоту, 20,95% кисню, 0,03% вуглекислого газу, 0,93% інертних і 0,01% інших газів.

У процесі виробництва в повітря робочої зони можуть потрапляти шкідливі речовини різного походження (гази, пари, аерозолі), які здатні викликати захворювання або відхилення в стані здоров'я працюючих.

Забруднення повітряного середовища і зміна його газового складу і фізичних параметрів може відбуватися: при механічній обробці матеріалів (свердління, шліфування, піскоструминна обробка поверхонь, дроблення, розмелювання, транспортування подрібненого матеріалу і ін.); газового та плазмового різання металів, електрозварювання, лудінні і пайку; знежирюванні поверхонь в органічних розчинниках; нанесенні захисних покриттів з використанням лаків, фарб, епоксидних смол; металізації і травленні різних елементів в розчинах кислот, лугів і солей, і багатьох інших техпроцесах і операціях.

Основний склад забруднювачів повітря на багатьох виробничих ділянках включає в себе оксиди вуглецю, сірки, азоту (CO , CO_2 , SO_2 , NOX), різні вуглеводні (CN , HM), альдегіди (фенол, формальдегід), пари мінеральних кислот, аерозолі фарб і ін.

За характером впливу на організм шкідливі речовини класифікуються на общетоксичные, дратівливі, сенсibiliзуючі, канцерогенні і мутагенні.

Найбільший ефект в захисті повітряного середовища від забруднення був досягнутий при поєднанні наступних заходів:

- вдосконалення технологічних процесів, створення їх безперервності, герметичності апаратури і комунікацій, застосування гідро- і пневмотранспорту для пилять речовин і матеріалів;

- впровадження комплексної механізації і автоматизації виробничих процесів, застосування дистанційного керування і автоматизації контролю за ходом технологічного процесу, що сприяє усуненню ручної праці і контакту з шкідливими речовинами;

- заміна шкідливих речовин у виробництві на нешкідливі або менш шкідливі;

- гігієнічна стандартизація хімічної сировини і продукції (наприклад, обмеження вмісту миш'яку в сірчаній кислоті; бензолу, ксилолу, вуглеводнів і сірки в бензині та інших видах палива);

- ефективна вентиляція виробничих приміщень та ін.

Забезпечення допустимого рівня іонізації повітряного середовища в робочій зоні

Встановлено, що значне зниження вмісту заряджених частинок (іонів) в повітрі збігається з появою у працюючих незвичайної хворобливості, скарг на втоми, депресію, нудоту, безсоння, дратівливість, респіраторні порушеннями і ін. В той же час перебування людей в умовах з помірно підвищеною іонізацією атмосфери, при переважному переважанні негативних іонів, - навпаки, спостерігається сприятливий вплив на організм.

Все це дозволило вважати аероіони біологічно активним чинником середовища.

Процес іонізації повітря полягає в перетворенні нейтральних атомів і молекул повітряного середовища в електрично заряджені частинки (іони).

Іони в повітрі (аероіони) можуть утворюватися внаслідок природної і штучної іонізації.

Природна іонізація відбувається в результаті впливу на повітряне середовище космічної і сонячної радіації і іонізуючих випромінювань (часток), що виникають при розпаді довгоживучих радіонуклідів земної кори (калій-40, уран-238, торій-232 і ін.). Природна іонізація повітряного середовища відбувається повсюдно і постійна в часі.

Штучна аероіонізація виникає під дією іонізуючих факторів, які супроводжують деякі технологічні процеси (рентгенівські і ультрафіолетові випромінювання, термoeмісія, фотоефект і ін.); а також в спеціальних пристроях - іонізатори, які використовують такі явища як коронний розряд і радіоактивний розпад деяких елементів.

Ступінь іонізації повітря залежить від співвідношення процесів іонізації і деіонізації. Остання обумовлюється рекомбінацією двох іонів різних полярностей, адсорбцією легких іонів на незаряджених ядрах, конденсації, нейтралізацією легких і важких іонів зарядами протилежного знака і ін.

Для нормалізації іонного режиму повітряного середовища широко застосовуються штучні іонізатори (високовольтні, індукційні, радіаційні та ін.) І ефективна, правильно організована припливно вентиляція приміщень, так як зовнішній чисте повітря містить в 2-5 разів більше іонів, ніж повітря закритих приміщень ($50 \dots 100$ іонів/см³).

Мікроклімат характеризуються фізичними параметрами повітря робочої області - його температурою ($t^{\circ}\text{C}$), відносною вологістю ($\phi, \%$), швидкістю руху (V , м/с), а також інтенсивністю теплового опромінення працюючих від нагрітих поверхонь обладнання, виробів і відкритих джерел (I , Вт/м²).

Зазначені параметри як окремо, так і в комплексі роблять значний вплив на перебіг життєвих процесів в організмі людини, багато в чому визначають його самопочуття і тому є важливою характеристикою комфортності умов праці.

Формування мікроклімату проходить під дією таких факторів:

- джерела тепловиділення (в т. ч. працівники);
- сонячна радіація;
- тепловиділення при роботі електрообладнання;
- кратності газоциркуляції в приміщенні;
- теплопередачі через перешкоди;
- температури поверхонь в приміщенні.

Метеорологічні умови (допустимі та оптимальні) – регламентуються в залежності від періоду року, категорії робіт за енерговитратами, надлишку явного тепла. Оптимальні показники поширюються на всю робочу зону, а допустимі - диференційовано для просторів і непостійних робочих місць. Допустимі показники встановлюються у випадках, коли за технологічними вимогами, технічних і економічних причин не забезпечуються оптимальні норми.

Нормами встановлюються теплий, холодний і перехідні періоди року. Теплий період року характеризується середньодобовою температурою зовнішнього повітря $+10^{\circ}\text{C}$ і вище; холодний і перехідний періоди - нижче $+10^{\circ}\text{C}$.

Найважливішими методами оптимізації мікроклімату в приміщеннях і в межах робочих місць є опалення, кондиціонування і вентиляція приміщень.

Для захисту працюючих від відкритих джерел використовуються засоби ІЗ, в т.ч. засоби захисту обличчя, зокрема очей. Передбачається захист працюючих і від охолодження закслених поверхонь віконних прорізів, а в теплий період року - від дії прямих сонячних променів.

Опалення приміщень може бути місцевим і центральним. Як теплоносії використовуються вода, пар або повітря. Тепле повітря, що подається в приміщення, зазвичай нагрівається в калорифери за допомогою гарячої води, пара або електричної енергії. Відповідно опалення може бути водяним, паровим, повітряним або комбінованим.

Центральні системи повітряного опалення зазвичай поєднуються з приточними вентиляційними системами. Калорифери таких систем встановлюються поза опалювальних приміщень.

Вентиляція являє собою систему технічних засобів, що забезпечує регулярний повітрообмін в приміщенні. Вона призначена для видалення з приміщення надлишкового тепла, вологи, шкідливих газів і парів та створення найбільш сприятливого (що відповідає санітарно-гігієнічним вимогам) мікроклімату і іонного складу.

Обмін повітря в приміщенні можна здійснювати природним шляхом через квартирки, фрамуги або вентиляційні канали за рахунок різниці температур і тисків повітря всередині приміщення і поза ним. Така вентиляція називається природною або аерацією.

Більш ефективна штучна механічна вентиляція, здійснювана за допомогою вентиляторів і ежекторів. Поєднання природної і штучної вентиляції утворює змішану систему вентиляції.

Природна вентиляція може бути неорганізованої, коли повітря поступає в приміщення і віддаляється з нього за рахунок інфільтрації через щілини і отвори зовнішніх огорож. Природна вентиляція є організованою, в тому випадку, коли вона має пристрої, що дозволяють налаштовувати напрямок руху повітря та об'єм повітрообміну (вентканали, квартирки і фрамуги будівель, аераційні ліхтарі, шахти та ін.).

Захист від механічних коливань

До механічних коливань відносяться: вібрація, акустичний шум, ультразвук і інфразвук.

Загальною властивістю цих фізичних процесів є те, що вони пов'язані з перенесенням енергії. При певній величині і частоті ця енергія може впливати на людину.

Вібрація - це коливальний процес, при якому окремі елементи механічних та інших систем періодично проходять через положення рівноваги.

Основними фізичними параметрами вібрації є частота коливань (f , Гц), амплітуда (A , м), віброшвидкість (V , м/с) і віброприскорення (W , м/с²). Причиною вібрації є невірноважені сили впливу.

Вібрація може реалізовуватися в шести напрямках відповідно до шістьма ступенями свободи.

Основними джерелами вібрацій є електричні приводи, робочі органи машин ударної дії, що обертаються маси, підшипникові вузли, зубчасті зачеплення і т.д. Вібрація генерується різним технологічним обладнанням: метало- та деревообробними верстатами, транспортними засобами, ручним

електрифікованим інструментом і різними машинами. Крім того, вібрація може використовуватися для інтенсифікації деяких технологічних процесів.

Вібрація (по каналу дії на організм) буває: загальною, яка передається через тверді середовища на все тіло; локальною, що розповсюджується через руки людини.

Загальні вібрації, впливаючи на нервову і серцево-судинну системи, викликають головний біль, нудоту, поява внутрішніх болів, відчуття тряски внутрішніх органів, розлад апетиту, порушення сну та ін.

Основним напрямком щодо захисту персоналу від вібрацій є автоматизація і механізація виробничих процесів. Однак в тих випадках, коли автоматизація і механізація неможливі, використовуються наступні методи і засоби боротьби з вібраціями.

Зниження вібрації на шляхах її поширення ефективно застосуванням вібропоглинання, винятком резонансних режимів, виброгашение, віброізоляцією і ін.

Розрахунок повітрообміну в серверній

Розрахунок повітрообміну проводиться для кімнати, де встановлено серверне обладнання, яке під час роботи виділяє надлишкову теплову енергію, отже необхідно забезпечити якісну вентиляцію та кондиціонування.

Розраховуючи процес циркуляції повітря в приміщенні, враховується кількість тепла, що виділяється таким чином, щоб отримана кількість, більше норми могла видалятися, цілий рік, без труднощів і перешкод.

Площа приміщення складає 12 м^2 , висота приміщення – $2,5 \text{ м}$. Об'єм приміщення – 30 м^3 . Кількість людей, що знаходяться в приміщенні обмежується одним системним адміністратором. Поверхня серверної шафи $t_{нов}$, в середньому розігрівається до 45°C . Площа поверхні S , що виділяє тепло, враховуючи габаритні характеристики шафи, складає $2,6 \text{ м}^2$.

Улаштування вентиляції (організованої або не організованої), залежить від результатів аналізу коефіцієнта кратності повітрообміну k – це відношення

потрібного об'єму чистого повітря, що необхідно поставляти щогодини в кімнату, до пустого об'єму приміщення, вільного від серверних шаф та ін.

$$k = \frac{L}{V_{н.в.}}, \quad (5.1)$$

де k – коефіцієнт кратності повітрообміну;

L – потрібний обсяг повітрообміну, $\text{м}^3/\text{год}$;

$V_{н.в.}$ – об'єм кімнати вільний від речей, м^3 ; $V_{н.в.} = 20,5 \text{ м}^3$.

Коли $k \leq 1$ допустимо улаштування неорганізованого типу вентиляції. При $1 < k \leq 10$ вентиляцію необхідно організовувати, при цьому, розмір вентканалів рахується, відштовхуючись від коефіцієнту повітрообміну. Якщо ж $k > 10$, вентиляція має бути примусовою.

Обчислення потрібного повітрообміну з урахуванням тепловиділення серверних шаф проводиться таким чином:

$$L = \frac{Q \cdot 3.6}{C \cdot \rho (t_{вуд} - t_{np})}, \text{ м}^3/\text{год} \quad (5.2)$$

де Q – надлишкове тепловиділення в серверній, Вт ;

C – масова теплоємність повітря, що поступає, $C = 1 \text{ кДж} / (\text{кг} \cdot ^\circ\text{C})$;

ρ – густина повітря, що поступає, $1.2 \text{ кг}/\text{м}^3$;

$t_{вуд}$ – температура повітря, що видаляється з серверної, $^\circ\text{C}$.

t_{np} – температура повітря, що поступає в серверну, $^\circ\text{C}$.

Температура видаляемого повітря, обчислюється за формулою:

$$t_{вуд} = t_{норм} + H_y \cdot (\Delta t - 2), ^\circ\text{C} \quad (5.3)$$

де $t_{норм}$ – оптимальна температура в серверній;

Δt – температурний градієнт, $\Delta t = 2.75 \text{ град}/\text{м}$;

H_y – відстань від підлоги до центра вентканалів, м

$$H_y = H - 1, \text{ м} \quad (5.4)$$

де H – висота стелі в серверній, м.

Відповідно до (5.4) розрахуємо H_y :

$$H_{\text{ш}} = 2.5 - 1 = 1.5 \text{ м.}$$

Обчислимо t повітря, що виходить з серверної, скористаємося формулою (5.3):

$$t_{\text{вих}} = 23 + 1.5 \cdot (2.75 - 2) = 24.125 \text{ }^{\circ}\text{C}.$$

Значення $t_{\text{норм}} = 23^{\circ}\text{C}$ прийнято згідно з ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень, в залежності від категорії робіт», іє нормальною температурою як для будь-яких пір року прилегкій роботі.

Обчислення надлишкового тепла Q виконується таким чином

$$Q = \alpha S (t_{\text{нов}} - t_{\text{норм}}), \text{ Вт} \quad (5.5)$$

де α – коефіцієнт теплопередачі між серверною шафою та повітрям,

$$\alpha = 5.6 + 4 \cdot v, \text{ Вт} / (\text{м}^2 \cdot ^{\circ}\text{C}) \quad (5.6)$$

де v – швидкість руху повітря, м/с. $v = 0.2 \text{ м/с}$.

Отже

$$\alpha = 5.6 + 4 \cdot 0.2 = 6.4 \text{ Вт} / (\text{м}^2 \cdot ^{\circ}\text{C}).$$

Тепер є всі дані для розрахунку надлишкового тепла Q :

$$Q = 6.4 \cdot 0.2 (45 - 23) = 320.3 \text{ Вт.}$$

Проведемо розрахунок необхідного повітрообміну відповідно до (5.2)

$$L = \frac{320.3 \cdot 3.6}{1 \cdot 1.2 \cdot (24.125 - 23)} = 854.13 \text{ м}^3 / \text{год}.$$

Визначимо коефіцієнт пропорційності повітрообміну

$$k = \frac{854.13}{20.5} = 41.7.$$

Отже, необхідно не тільки влаштування активної вентиляції, а й обов'язково потрібно встановити системи кондиціонування.

5.4 Заходи безпеки у надзвичайних ситуаціях

5.4.1 Заходи з пожежної безпеки

Пожежна безпека визначається як стан об'єкта, при якому максимально попереджається вірогідність пожежі, а в разі виникнення мінімізується вплив її небезпечних факторів і передбачається збереження матеріальних цінностей.

Таким чином, пожежна безпека забезпечується комплексом заходів, що запобігають виникненню пожежі і системою пожежного захисту, що забезпечує успішну боротьбу з виниклою пожежею або наслідками вибуху.

Запобігання пожежі досягається комплексом профілактичних заходів, що виключають утворення горючого середовища, джерел запалювання, підтримання температури горючої середовища нижче максимально допустимої до горючості і тиску в займистою середовищі нижче максимально допустимого до горючості і ін.

Попередження утворення горючого середовища забезпечується регламентацією допустимих концентрацій горючих газів, парів і суспензій в повітрі, а також кисню або інших окислювачів.

Запобігання утворенню в займистою середовищі джерел підпалювання досягається відповідним виконанням, застосуванням і режимом експлуатації машин і механізмів, матеріалів і виробів, що можуть бути джерелом запалювання горючого середовища, застосуванням відповідного електрообладнання та технологічного процесу, пристроєм блискавкозахисту будівель і споруд, регламентацією допустимої температури нагрівання поверхні устаткування, допустимої енергією іскрового розряду, ліквідацією умов для теплового, хімічного та мікробіологічного самозаймання звертаються речовин, матеріалів і виробів.

До профілактичних заходів також відносяться:

- використання негорючих та важкогорючих матеріалів;
- обмеження кількості горючих речовин;
- запобігання розповсюдженню пожежі за межу зони вогнища;

- використання конструкцій з регламентованими межами вогнестійкості та горючості; створення умов для евакуації людей;
- використання засобів захисту людей і системного захисту від диму;
- застосування засобів пожежної сигналізації та засобів сповіщення про пожежу;
- організація пожежної охорони та ін.

Обмеження кількості горючих речовин досягається регламентацією їх кількості (маси, об'єму), наявністю аварійного зливу, періодичної очищення приміщень, комунікацій та апаратури від горючих відходів, регламентацією робочих місць, на яких використовуються пожежонебезпечні речовини і ін.

Ізоляція горючої середовища забезпечується максимальною механізацією і автоматизацією технологічних процесів, застосуванням для пожежонебезпечних речовин герметизованого обладнання і тари.

Запобігання поширенню пожежі організовується за рахунок пристрою протипожежних завад (стін, зон, поясів, захисних смуг, завіс і т.п.), використання засобів, що не допускають та обмежують розлив і розповсюдження рідин під час пожежі та ін.

Заходи з профілактики пожежної загрози умовно поділяються на організаційні, експлуатаційні, технічні і режимні.

Організаційні міри щодо впровадження ПБ включають в себе:

- організацію навчання персоналу і громадян правилам ПБ;
- розробку нормативів ПБ, інструкцій до послідовності роботи з пожежонебезпечними елементами виробництва, поведінці людей під час пожежі та ін.

Експлуатаційні міри покликані забезпечити відповідні експлуатаційні якості обладнання, споруд і територій.

Технічні заходи полягають в дотриманні протипожежних норм при спорудженні будівель, пристрої опалення та вентиляції, виборі та монтажу обладнання, пристрої грозозахисту і захисту від статичної електрики.

Режимні заходи спрямовані на обмеження або заборона розведення вогню, виробництва електро- і газозварювальних робіт, а також куріння в невстановлених місцях та ін.

5.4.2 Заходи з цивільного захисту

Впровадження безпечних умов праці на підприємстві здійснюється за допомогою системи управління охороною праці (СУОП), що представляє собою підготовку, прийняття і реалізацію рішень, що складається з правових, соціально-економічних, організаційних, технічних, психофізіологічних, та інших заходів.

Об'єктом управління ОП на виробництві є діяльність структурних одиниць, функційних служб і окремих працівників, щодо забезпечення відповідних умов праці на робочих локаціях, виробничих майданчиках і на підприємстві в цілому.

Органами управління ОП є служби керівника підприємства (головного інженера, технічного директора і т.п.).

Організаційно-методичну роботу з керування ОП, підготовку управлінських рішень і контроль за їх здійсненням виконує служба ОП (відділ, бюро і т.п.), яка підкоряється напрямку голові підприємства (ведучому інженеру, технічному директору і т.п.).

Правовою основою СУОП є законодавство про працю, правові та технічні нормативні акти, в яких прописано вимоги з ОП.

Нормальне функціонування і вдосконалення СУОП можливо при наявності об'єктивної інформації про умови праці на конкретних робочих місцях, локаціях і підприємстві в цілому.

Відхилення від вимог ОП встановлюються за допомогою функції контролю, а усунення причин відхилень є функцією регулювання (керування).

Керування ОП на підприємстві включає в себе вирішення завдань, що дозволяють наймачеві реалізувати свої обов'язки відносно забезпечення вимог ОП згідно із законодавством.

ВИСНОВКИ

В ході роботи, було проведено дослідження по модернізації локальної мережі за стандартом Fast Ethernet для підприємства роздрібної торгівлі ТОВ “Альфа Проджект”. Були розглянуті переваги та недоліки хмарних серверів, послуги та функції хмарних сервісів. Локальні серверні рішення. Розглянуто різноманітне активне та пасивне (маршрутизатори 1-го то 2-го рівнів) мережеве обладнання, яке б відповідало потребам та цілям мережі з точки зору адміністрування. Програмне забезпечення як для серверної частини, так і для робочих станцій, в залежності від потреб користувачів та гостьових облікових засобів. Розраховано капітальні витрати на модернізацію обладнання та мережі. Обрані оптимальні рішення для експлуатації на довгий період часу. Проектуєма мережа дозволить знизити ризики втрати даних, забезпечити швидкісний доступ користувачів мережі до різних послуг та інформаційним ресурсам, одночасно використовувати різні мережеві протоколи та архітектури, підвищити ефективність роботи підприємства за рахунок виконання паралельних розрахунків, одночасного використання даних та мережевих пристроїв використання сучасних систем електронного документообігу.

ПЕРЕЛІК ПОСИЛАНЬ

1. **Булдыжов В.И.**, Основы вычислительной техники, информационных технологий и компьютерных сетей. Интерактивное учебное пособие. – Николаев.: УГМТУ, 2002г. – 154с.
2. **Новиков Ю.В.**, Основы локальных сетей. / Ю.В. Новиков, С.В. Кондратенко. – Москва 2016г – 94-115 с.
3. **Еві Немет**, Unix и Linux. Руководство системного администратора, Издательство Вильямс, 2015г – 508-512 с.
4. **Джеймс Хоган**, Системное и сетевое администрирование. Практическое руководство 1-е издание, СПб, 2009г – 522-702 с.
5. **Е. Танебаум**, Компьютерные сети, СПб.: Питер, 2012г . – 351-378 с.
6. **Крэйг Хант**, TCP/IP. Сетевое администрирование, СПб, 2006г. – 435-493 с.
7. **Стівен Дж. Бігелоу**, Сети. Поиск неисправностей, поддержка и восстановление, СПб.: БХВ-Петербург, 2005г. – 853-907 с.
8. **УільямР.Станек**, Microsoft Windows Server 2012. Справочник администратора, БХВ-Петербург, Русская Редакция 2014г. – 246-302 с.
9. **Уєнделл Одом**, Официальное руководство Cisco, 2015г. – 132-149 с.
10. **Олифер В.Г.**, Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 1-е изд. – Спб.: Питер, 2006г. – 201-257 с.
11. **Лавренко А.С.** Методичні вказівки до практичної роботи «Розрахунок повітрообміну у виробничих приміщеннях при загально обмінній вентиляції» з дисципліни «Охорона праці в галузі» для студентів всіх форм навчання / Укл. А.С. Лавренко, О.Л. Скуйбіда, А.Є. Островська – Запоріжжя: ЗНТУ, 2014. - 14с.
12. **Рахматуллин, Р. Р.** Расчет технико-экономических показателей и определение экономического эффекта [Текст] / Р.Р. Рахматуллин. – М.: Бибком, 2017. – 169 с.

13. **ГОСТ 12.0.003-74 ССБТ** «Опасные и вредные производственные факторы. Классификация»
14. **ГОСТ 12.1005-88 ССБТ** «Общие санитарно-гигиенические требования к воздуху рабочей зоны»
15. **ГОСТ 12.1.045-84 ССБТ** «Электростатические поля. Допустимые уровни на рабочих местах и требования к проведению контроля»
16. **ГОСТ 12.1.005-88 ССБТ** «Общие санитарно-гигиенические требования к воздуху рабочей зоны»
17. **ДСТУ Б В.1.1-36:2016** «Визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною безпекою»
18. **ДСН 3.3.6.042-99** «Санітарні норми мікроклімату виробничих приміщень, в залежності від категорії робіт»
19. **ДБН В.1.1-7:2016** «Пожежна безпека об'єктів будівництва. Загальні вимоги»
20. **ДСНП** «Гігієнічна класифікація праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу», [Електронний ресурс] / МІОУ 06.05.2014 р. за № 472/25249 – Режим доступу до ресурсу: <https://zakon.rada.gov.ua/laws/show/z0472-14#Text>
21. **Соколов А.В., Шаньгин В.Ф.**, Защита информации в распределительных сетях и системах – М.: Издательство ДМК, 2002.
22. **Горлов Н.И., Микиденко А.В., Минина Е.А.** Оптические линии связи и пассивные компоненты ВОСП. Учебное пособие. 2010г – 287-351 с.
23. **Семенов А.Б.** Проектирование и расчет структурированных кабельных систем и их компонентов. – М: ДМК Пресс; Компания АйТи, 2003. – 121-158 с.

ДОДАТОК А

Таблиця А.1 – Технічні характеристики APC Smart-UPS SUA3000I

Вихід	Максимальна вихідна потужність 2700 Ватт / 3000 ВА Максимальна задається значення потужності 2700 Ватт /3000 ВА Номинальна вихідна напруга: 230V Ефективність під повним навантаженням: 95.0%
Вхід	Номинальна вхідна напруга: 230V Вхідна частота: 50/60 Гц +/- 3 Гц (автоматичне впізнання) Діапазон вхідної напруги при роботі від мережі: 160 -285В
Батареї і тривалість автономної роботи	Тип батареї: Необслуговувана герметична свинцево-кислотна батарея з загущених електролітом: захист від витоків Типовий час перезарядки 3 години Змінний комплект батарей: RBC55 Кількість змінних комплектів батарей: 1
Комуніційні властивості і властивості адміністрування	Інтерфейсний порт: DB-9 для RS-232, Роз'єм SmartSlot, USB Кількість доступних інтерфейсів SmartSlot™: 1 Панель управління: Світлодіодний дисплей зі шкалами навантаження і заряду батарей, а також індикаторами On Line (роботи від мережі): On Battery (роботи від батарей): Replace attery (необхідності заміни батареї): і Overload (перегрівки) Індикатор режимів On Line (роботи від мережі): On Battery (роботи від батарей): Replace Battery (необхідності заміни батареї): і Overload (перевантаження). Звуковий сигнал: Сигнал переходу в режим роботи від акумуляторів: особливий сигнал вичерпання заряду батарей: можливість завдання затримок Аварійне відключення живлення (EPO): Так
Захист від сплесків напруги і фільтрація шумів	Рейтинг за рівнем енергії, що поглинається сплеску: 365 Дж Фільтрація Постійно діючий багатополосний шумовий фільтр: амплітуда залишкової напруги 0,3 за нормативами IEEE: обмеження сплеску напруги без часової затримки: відповідність вимогам UL 1449
Фізичні	Максимальна висота: 432.00 mm Максимальна ширина: 196.00 mm Максимальна глибина: 544.00 mm Маса нетто: 55.92 КГ Маса брутто: 65.00 КГ Висота в упаковці: 680.00 mm Ширина в упаковці: 380.00 mm Глибина в упаковці: 760.00 mm Пристроїв на піддоні: 3.00

ДОДАТОК Б

Таблиця Б.1 – Технічні характеристики Allied Telesis AT- 8000S / 48

Розміри (ширина x глибина x висота), см	44 x 25.7 x 4.3
Вага, кг:	3,15
Параметри живлення:	Вбудований блок живлення • Вхідна напруга: 100 - 240 В AC • Вихідна напруга: 12 В DC • Струм: 1.5 А • Потужність: 26.5 Вт
Комплектація:	• Комутатор AT-8000S/48 • Шнур живлення AC • Набір для установки в стійку • Гумові ніжки для установки на стіл • Кабель RS232 для управління (RJ-45) • Стекові кабель
Порти інтерфейсу:	
Мідні інтерфейси:	24 x RJ-45 10/100
Оптичні інтерфейси:	Об'єднані порти: • 2 x RJ-45 10/100/1000T • 2 x SFP 100FX, 1000SX, 1000LX
Інші інтерфейси:	1 x RS232, контакти DB9, тато
МЕРЕЖЕВІ ОСОБЛИВОСТІ:	
Підтримувані стандарти:	• Інтерфейсні стандарти: - IEEE 802.3 10T - IEEE 802.3u 100TX i 100FX - IEEE 802.3z 1000SX - IEEE 802.3ab 1000T • Загальні стандарти: - IEEE 802.1D мостові з'єднання - IEEE 802.3x зворотне тиск / управління по-струмом • Стандарти резервування: - IEEE 802.1D Spanning-Tree Protocol - IEEE 802.1W Rapid Spanning-Tree - IEEE 802.1s Multiple Spanning-Tree BPDU захист - IEEE 802.3ad LACP агрегація з'єднання (до 8 членів на групу і до 8 груп на пристрій) - Канал статичного порту • Стандарти Multicast: - RFC 1112 IGMP snooping (ver. 1) - RFC 2236 IGMP snooping (ver. 2) - RFC 3376 IGMP snooping (ver. 3) - RFC 3376 IGMP querier - Можливість пересилки/фільтрації незареєстрованих MAC-адресів

продуктивність:	• Оперативна пам'ять: 64 МБ • Флеш-пам'ять: 16 МБ • Процесор 400 МГц • VLAN ID: до 4,096 • MAC-адрес: 8,000 • Розмір буфера пакетів: 1 Мбіт • Комутація з провідний швидкістю на всіх портах Ethernet для пакетів всіх розмірів • Пропускна здатність: до 9.52 мільйонів пакетов / с • Комутаційна здатність: 12.8 Гбіт / с • Режим зберігання та пересилання • Неблокована комутація • Автоматичний MDI / MDI-X • Затримка: - 10 Мбіт - 85.71 мкс - 100 Мбіт - 17.30 мкс - 1000 Мбіт / с - 2.72 мкс
стекирование:	• До 6 юнітів • Єдина система управління • Управління через 1 IP-адреса • Майстер резервування • Кільцева топологія резервування в стеці продуктивністю 20 Гбіт / с • Агрегація з'єднання / каналів в стеку • Віддзеркалення портів в стеку • VLAN в стеці
управління:	• Управління та спостереження: - WEB, CLI, Telnet, SSH, послідовний консольний порт - RFC 1157 SNMPv1 / v2c - RFC 2570 SNMPv3 - RFC 1213 MIB-II - RFC 1573 розвиток MIB-II - RFC 1215 TRAP MIB - RFC тисячі чотиреста дев'яносто три міст MIB - RFC 2863 група інтерфейсів MIB - RFC 1 643 Ethernet like MIB - RFC тисяча сімсот п'ятьдесят сім 4 групи RMON: статистика, історія, сигнали, події - RFC 2674 IEEE 802.1Q MIB - RFC +1866 HTML - RFC 2068 HTTP - RFC 854 Telnet - RFC 783 TFTP - LLDP - IEEE 802.1ab - LLDP-MED • Призначення IP-адрес: - RFC 951 / RFC тисяча п'ятсот сорок-два BootP / DHCP ручне - DHCP snooping - RFC 2030 SNTP, Simple Network Time Protocol - Події в системній журналі - Два образи програмного забезпечення
Безпека:	• Безпечне управління: захист логіном і паро-

	лем • SSHv2 для управління через Telnet • SSLv3 для управління через веб-інтерфейс • RFC тисячу чотиреста дев'яносто два TACACS + • RFC 2618 ідентифікація RADIUS • IEEE 802.1x динамічні VLAN • IEEE 802.1x облікові записи RADIUS • IEEE 802.1x режим декількох сесій • IEEE 802.1x дію при порушенні • IEEE 802.1x порушення одного хоста • IEEE 802.1x таймаут гостьових VLAN • IEEE 802.1x ідентифікація не потрібно • Security login banner • RFC 2865 IEEE 802.1x управління мережевим доступом в залежності від портів • Управління мережевим доступом по MAC-адресами • Гостьові VLAN • ACL - списки управління доступом: - IP-адреси - MAC-адреси • Контроль ширококомовних штормів
QoS:	• QoS in Layer 2 (клас обслуговування, сумісний з IEEE 802.1p) • Пріоритизація трафіку за допомогою полів IEEE 802.1p, ToS, DSCP • Асоціація пріоритетів IEEE 802.1p і очередей CoS для пріоритизації вихідного трафіку • Суворі черговість і Weighted Round Robin
Мережеві функції:	• VLAN - IEEE 802.1Q VLAN tagging - До 256 активних VLAN - VLAN в залежності від портів - VLAN в залежності від MAC-адрес - Приватні VLAN - GARP VLAN Registration Protocol (GVRP) • IPv6 - IPv6 QoS - IPv6 ACL - Хост IPv6 - RFC 2461 виявлення найближчих IPv6 - RFC 2463 ICMPv6: Internet Control Message - RFC один тисяча дев'яносто вісімдесят одна виявлення Path MTU - Подвійний стек протоколів IPv4 / IPv6 - Тунелювання IPv6 через IPv4 - Мережеве управління IPv6 - Додатки IPv6: WEB / SSL сервер Telnet / SSH, AAA / Radius, управління ACL, SNMP, PING, TFTP / копіювання, системний журнал

ДОДАТОК В

Таблиця В.1 – Технічні характеристики Allied Telesis AT-8000S/24

Розміри (ширина x глибина x висота), см	44 x 25.7 x 4.3
Вага, кг:	3,15
Параметри живлення:	Вбудований блок живлення • Вхідна напруга: 100 - 240 В AC • Вихідна напруга: 12 В DC • Струм: 1.5 А • Потужність: 26.5 Вт
Комплектація:	• Комутатор AT-8000S / 24 • Шнур живлення AC • Набір для установки в стійку • Гумові ніжки для установки на стіл • Кабель RS232 для управління (RJ-45) • Стекові кабель
Порти інтерфейсу:	
Мідні інтерфейси:	24 x RJ-45 10/100
Оптичні інтерфейси:	Об'єднані порти: • 2 x RJ-45 10/100 / 1000T • 2 x SFP 100FX, 1000SX, 1000LX
Інші інтерфейси:	1 x RS232, контакти DB9, тато
МЕРЕЖЕВІ ОСОБЛИВОСТІ:	
Підтримувані стандарти:	• Інтерфейсні стандарти: - IEEE 802.3 10T - IEEE 802.3u 100TX і 100FX - IEEE 802.3z 1000SX - IEEE 802.3ab 1000T • Загальні стандарти: - IEEE 802.1D мостові з'єднання - IEEE 802.3x зворотне тиск / управління по-струмом • Стандарти резервування: - IEEE 802.1D Spanning-Tree Protocol - IEEE 802.1W Rapid Spanning-Tree - IEEE 802.1s Multiple Spanning-Tree BPDU захист - IEEE 802.3ad LACP агрегація з'єднання (до 8 членів на групу і до 8 груп на пристрій) - Канал статичного порту • Стандарти Multicast: - RFC 1112 IGMP snooping (ver. 1) - RFC 2236 IGMP snooping (ver. 2) - RFC 3376 IGMP snooping (ver. 3) - RFC 3376 IGMP querier - Можливість пересилки/фільтрації незареєстрованих MAC-адресів

продуктивність:	• Оперативна пам'ять: 64 МБ • Флеш-пам'ять: 16 МБ • Процесор 400 МГц • VLAN ID: до 4,096 • MAC-адрес: 8,000 • Розмір буфера пакетів: 1 Мбіт • Комутація з провідний швидкістю на всіх портах Ethernet для пакетів всіх розмірів • Пропускна здатність: до 9.52 мільйонів пакетов / с • Комутаційна здатність: 12.8 Гбіт / с • Режим зберігання та пересилання • Неблокована комутація • Автоматичний MDI / MDI-X • Затримка: - 10 Мбіт - 85.71 мкс - 100 Мбіт - 17.30 мкс - 1000 Мбіт / с - 2.72 мкс
стекирование:	• До 6 юнітів • Єдина система управління • Управління через 1 IP-адреса • Майстер резервування • Кільцева топологія резервування в стеці продуктивністю 20 Гбіт / с • Агрегація з'єднання / каналів в стеку • Віддзеркалення портів в стеку • VLAN в стеці
управління:	• Управління та спостереження: - WEB, CLI, Telnet, SSH, послідовний консольний порт - RFC 1157 SNMPv1 / v2c - RFC 2570 SNMPv3 - RFC 1213 MIB-II - RFC 1573 розвиток MIB-II - RFC 1215 TRAP MIB - RFC тисячі чотиреста дев'яносто три міст MIB - RFC 2863 група інтерфейсів MIB - RFC 1 643 Ethernet like MIB - RFC тисяча сімсот п'ятьдесят сім 4 групи RMON: статистика, історія, сигнали, події - RFC 2674 IEEE 802.1Q MIB - RFC +1866 HTML - RFC 2068 HTTP - RFC 854 Telnet - RFC 783 TFTP - LLDP - IEEE 802.1ab - LLDP-MED • Призначення IP-адрес: - RFC 951 / RFC тисяча п'ятсот сорок-два BootP / DHCP ручне - DHCP snooping - RFC 2030 SNTP, Simple Network Time Protocol - Події в системній журналі - Два образи програмного забезпечення
Безпека:	• Безпечне управління: захист логіном і паро-

	лем • SSHv2 для управління через Telnet • SSLv3 для управління через веб-інтерфейс • RFC тисячу чотиреста дев'яносто два TACACS + • RFC 2618 ідентифікація RADIUS • IEEE 802.1x динамічні VLAN • IEEE 802.1x облікові записи RADIUS • IEEE 802.1x режим декількох сесій • IEEE 802.1x дію при порушенні • IEEE 802.1x порушення одного хоста • IEEE 802.1x таймаут гостьових VLAN • IEEE 802.1x ідентифікація не потрібно • Security login banner • RFC 2865 IEEE 802.1x управління мережевим доступом в залежності від портів • Управління мережевим доступом по MAC-адресами • Гостьові VLAN • ACL - списки управління доступом: - IP-адреси - MAC-адреси • Контроль широкомовних штормів
QoS:	• QoS in Layer 2 (клас обслуговування, сумісний з IEEE 802.1p) • Пріоритизація трафіку за допомогою полів IEEE 802.1p, ToS, DSCP • Асоціація пріоритетів IEEE 802.1p і очередей CoS для пріоритизації вихідного трафіку • Суворі черговість і Weighted Round Robin
Мережеві функції:	• VLAN - IEEE 802.1Q VLAN tagging - До 256 активних VLAN - VLAN в залежності від портів - VLAN в залежності від MAC-адрес - Приватні VLAN - GARP VLAN Registration Protocol (GVRP) • IPv6 - IPv6 QoS - IPv6 ACL - Хост IPv6 - RFC 2461 виявлення найближчих IPv6 - RFC 2463 ICMPv6: Internet Control Message - RFC один тисяча дев'ятсот вісімдесят одна виявлення Path MTU - Подвійний стек протоколів IPv4 / IPv6 - Тунелювання IPv6 через IPv4 - Мережеве управління IPv6 - Додатки IPv6: WEB / SSL сервер Telnet / SSH, AAA / Radius, управління ACL, SNMP, PING, TFTP / копіювання, системний журнал

ДОДАТОК Г

Таблиця Г.1 – Технічні характеристики Dell 4032F/24POE

Розміри (ширина x глибина x висота), см	44 x 25.7 x 4.3
Вага, кг:	3,15
Параметри живлення:	Вбудований блок живлення • Вхідна напруга: 100 - 240 В AC • Вихідна напруга: 12 В DC • Струм: 1.5 А • Потужність: 26.5 Вт
Комплектація:	• Комутатор 4032F / 24 • Шнур живлення AC • Набір для установки в стійку • Гумові ніжки для установки на стіл • Кабель RS232 для управління (RJ-45) • Стековий кабель
Порти інтерфейсу:	
Мідні інтерфейси:	24 x RJ-45 10/100
Оптичні інтерфейси:	Об'єднані порти: • 2 x RJ-45 10/100 / 1000T • 2 x SFP 100FX, 1000SX, 1000LX
Інші інтерфейси:	1 x RS232, контакти DB9, тато
МЕРЕЖЕВІ ОСОБЛИВОСТІ:	
Підтримувані стандарти:	• Інтерфейсні стандарти: - IEEE 802.3 10T - IEEE 802.3u 100TX і 100FX - IEEE 802.3z 1000SX - IEEE 802.3ab 1000T • Загальні стандарти: - IEEE 802.1D мостові з'єднання - IEEE 802.3x зворотне тиск / управління по-струмом • Стандарти резервування: - IEEE 802.1D Spanning-Tree Protocol - IEEE 802.1W Rapid Spanning-Tree - IEEE 802.1s Multiple Spanning-Tree BPDU захист - IEEE 802.3ad LACP агрегація з'єднання (до 8 членів на групу і до 8 груп на пристрій) - Канал статичного порту • Стандарти Multicast: - RFC 1112 IGMP snooping (ver. 1) - RFC 2236 IGMP snooping (ver. 2) - RFC 3376 IGMP snooping (ver. 3) - RFC 3376 IGMP querier - Можливість пересилки / фільтрації незареєстрованих MC-кадрів

продуктивність:	• Оперативна пам'ять: 64 МБ • Флеш-пам'ять: 16 МБ • Процесор 400 МГц • VLAN ID: до 4,096 • MAC-адрес: 8,000 • Розмір буфера пакетів: 1 Мбіт • Комутація з провідний швидкістю на всіх портах Ethernet для пакетів всіх розмірів • Пропускна здатність: до 9.52 мільйонів пакетов / с • Комутаційна здатність: 12.8 Гбіт / с • Режим зберігання та пересилання • Неблокована комутація • Автоматичний MDI / MDI-X • Затримка: - 10 Мбіт - 85.71 мкс - 100 Мбіт - 17.30 мкс - 1000 Мбіт / с - 2.72 мкс
стекирование:	• До 6 юнітів • Єдина система управління • Управління через 1 IP-адреса • Майстер резервування • Кільцева топологія резервування в стеці продуктивністю 20 Гбіт / с • Агрегація з'єднання / каналів в стеку • Віддзеркалення портів в стеку • VLAN в стеці
управління:	• Управління та спостереження: - WEB, CLI, Telnet, SSH, послідовний консольний порт - RFC 1157 SNMPv1 / v2c - RFC 2570 SNMPv3 - RFC 1213 MIB-II - RFC 1573 розвиток MIB-II - RFC 1215 TRAP MIB - RFC тисячі чотиреста дев'яносто три міст MIB - RFC 2863 група інтерфейсів MIB - RFC 1 643 Ethernet like MIB - RFC тисяча сімсот п'ятьдесят сім 4 групи RMON: статистика, історія, сигнали, події - RFC 2674 IEEE 802.1Q MIB - RFC +1866 HTML - RFC 2068 HTTP - RFC 854 Telnet - RFC 783 TFTP - LLDP - IEEE 802.1ab - LLDP-MED • Призначення IP-адрес: - RFC 951 / RFC тисяча п'ятсот сорок-два BootP / DHCP ручне - DHCP snooping - RFC 2030 SNTP, Simple Network Time Protocol - Події в системній журналі - Два образи програмного забезпечення
Безпека:	• Безпечне управління: захист логіном і паро-

	лем • SSHv2 для управління через Telnet • SSLv3 для управління через веб-інтерфейс • RFC тисячу чотиреста дев'яносто два TACACS + • RFC 2618 ідентифікація RADIUS • IEEE 802.1x динамічні VLAN • IEEE 802.1x облікові записи RADIUS • IEEE 802.1x режим декількох сесій • IEEE 802.1x дію при порушенні • IEEE 802.1x порушення одного хоста • IEEE 802.1x таймаут гостьових VLAN • IEEE 802.1x ідентифікація не потрібно • Security login banner • RFC 2865 IEEE 802.1x управління мережевим доступом в залежності від портів • Управління мережевим доступом по MAC-адресами • Гостьові VLAN • ACL - списки управління доступом: - IP-адреси - MAC-адреси • Контроль широкомовних штормів
QoS:	• QoS in Layer 2 (клас обслуговування, сумісний з IEEE 802.1p) • Пріоритизація трафіку за допомогою полів IEEE 802.1p, ToS, DSCP • Асоціація пріоритетів IEEE 802.1p і очередей CoS для пріоритизації вихідного трафіку • Суворе чергування і Weighted Round Robin
Мережеві функції:	• VLAN - IEEE 802.1Q VLAN tagging - До 256 активних VLAN - VLAN в залежності від портів - VLAN в залежності від MAC-адрес - Приватні VLAN - GARP VLAN Registration Protocol (GVRP) • IPv6 - IPv6 QoS - IPv6 ACL - Хост IPv6 - RFC 2461 виявлення найближчих IPv6 - RFC 2463 ICMPv6: Internet Control Message - RFC один тисяча дев'ятсот вісімдесят одна виявлення Path MTU - Подвійний стек протоколів IPv4 / IPv6 - Тунелювання IPv6 через IPv4 - Мережеве управління IPv6 - Додатки IPv6: WEB / SSL сервер Telnet / SSH, AAA / Radius, управління ACL, SNMP, PING, TFTP / копіювання, системний журнал

ДОДАТОК Г

Таблиця Г.1 – Технічні характеристики CISCO 2821-SEC / K9

Розміри (ширина x глибина x висота), см	44 x 25.7 x 4.3
Вага, кг:	3,15
Параметри живлення:	Вбудований блок живлення - Вхідна напруга: 100 - 240 В AC - Вихідна напруга: 12 В DC - Струм: 1.5 А - Потужність: 26.5 Вт
Комплектація:	- Комутатор AT-8000S / 24 - Шнур живлення AC - Набір для установки в стійку - Гумові ніжки для установки на стіл - Кабель RS232 для управління (RJ-45) - Стековий кабель
Порти інтерфейсу:	
Мідні інтерфейси:	24 x RJ-45 10/100
Оптичні інтерфейси:	Об'єднані порти: 2 x RJ-45 10/100 / 1000T 2 x SFP 100FX, 1000SX, 1000LX
Інші інтерфейси:	1 x RS232, контакти DB9, тато
МЕРЕЖЕВІ ОСОБЛИВОСТІ:	
Підтримувані стандарти:	- Інтерфейсні стандарти: - IEEE 802.3 10T - IEEE 802.3u 100TX i 100FX - IEEE 802.3z 1000SX - IEEE 802.3ab 1000T - Загальні стандарти: - IEEE 802.1D мостові з'єднання - IEEE 802.3x зворотне тиск / управління по-струмом - Стандарти резервування: - IEEE 802.1D Spanning-Tree Protocol - IEEE 802.1W Rapid Spanning-Tree - IEEE 802.1s Multiple Spanning-Tree BPDU захист - IEEE 802.3ad LACP агрегація з'єднання (до 8 членів на групу і до 8 груп на пристрій) - Канал статичного порту - Стандарти Multicast: - RFC 1112 IGMP snooping (ver. 1) - RFC 2236 IGMP snooping (ver. 2) - RFC 3376 IGMP snooping (ver. 3) - RFC 3376 IGMP querier - Можливість пересилки / фільтрації незареєстрованих MC-кадрів

продуктивність:	• Оперативна пам'ять: 64 МБ • Флеш-пам'ять: 16 МБ • Процесор 400 МГц • VLAN ID: до 4,096 • MAC-адрес: 8,000 • Розмір буфера пакетів: 1 Мбіт • Комутація з провідний швидкістю на всіх портах Ethernet для пакетів всіх розмірів • Пропускна здатність: до 9.52 мільйонів пакетов / с • Комутаційна здатність: 12.8 Гбіт / с • Режим зберігання та пересилання • Неблокована комутація • Автоматичний MDI / MDI-X • Затримка: - 10 Мбіт - 85.71 мкс - 100 Мбіт - 17.30 мкс - 1000 Мбіт / с - 2.72 мкс
стекирование:	• До 6 юнітів • Єдина система управління • Управління через 1 IP-адреса • Майстер резервування • Кільцева топологія резервування в стеці продуктивністю 20 Гбіт / с • Агрегація з'єднання / каналів в стеку • Віддзеркалення портів в стеку • VLAN в стеці
управління:	• Управління та спостереження: - WEB, CLI, Telnet, SSH, послідовний консольний порт - RFC 1157 SNMPv1 / v2c - RFC 2570 SNMPv3 - RFC 1213 MIB-II - RFC 1573 розвиток MIB-II - RFC 1215 TRAP MIB - RFC тисячі чотиреста дев'яносто три міст MIB - RFC 2863 група інтерфейсів MIB - RFC 1 643 Ethernet like MIB - RFC тисяча сімсот п'ятьдесят сім 4 групи RMON: статистика, історія, сигнали, події - RFC 2674 IEEE 802.1Q MIB - RFC +1866 HTML - RFC 2068 HTTP - RFC 854 Telnet - RFC 783 TFTP - LLDP - IEEE 802.1ab - LLDP-MED • Призначення IP-адрес: - RFC 951 / RFC тисяча п'ятсот сорок-два BootP / DHCP ручне - DHCP snooping - RFC 2030 SNTP, Simple Network Time Protocol - Події в системній журналі - Два образи програмного забезпечення
Безпека:	• Безпечне управління: захист логіном і паролем • SSHv2 для управління через Telnet • SSLv3 для управління через веб-інтерфейс

	• RFC тисячу чотиреста дев'яносто два TACACS + • RFC 2618 ідентифікація RADIUS • IEEE 802.1x динамічні VLAN • IEEE 802.1x облікові записи RADIUS • IEEE 802.1x режим декількох сесій • IEEE 802.1x дію при порушенні • IEEE 802.1x порушення одного хоста • IEEE 802.1x таймаут гостьових VLAN • IEEE 802.1x ідентифікація не потрібно • Security login banner • RFC 2865 IEEE 802.1x управління мережевим доступом в залежності від портів • Управління мережевим доступом по MAC-адресами • Гостьові VLAN • ACL - списки управління доступом: - IP-адреси - MAC-адреси • Контроль широкомовних штормів
QoS:	• QoS in Layer 2 (клас обслуговування, сумісний з IEEE 802.1p) • Пріоритизація трафіку за допомогою полів IEEE802.1p, ToS, DSCP • Асоціація пріоритетів IEEE 802.1p і очередей CoS для пріоритизації вихідного трафіку • Суворі черговість і Weighted Round Robin
Мережеві функції:	• VLAN - IEEE 802.1Q VLAN tagging - До 256 активних VLAN - VLAN в залежності від портів - VLAN в залежності від MAC-адрес - Приватні VLAN - GARP VLAN Registration Protocol (GVRP) • IPv6 - IPv6 QoS - IPv6 ACL - Хост IPv6 - RFC 2461 виявлення найближчих IPv6 - RFC 2463 ICMPv6: Internet Control Message - RFC один тисяча дев'ятсот вісімдесят одна виявлення Path MTU - Подвійний стек протоколів IPv4 / IPv6 - Тунелювання IPv6 через IPv4 - Мережеве управління IPv6 - Додатки IPv6: WEB / SSL сервер Telnet / SSH, AAA / Radius, управління ACL, SNMP, PING, TFTP / копіювання, системний журнал

ДОДАТОК Д

Таблиця Д.1 – Параметри лінійного інтерфейсу G.SHDSL

Тип інтерфейса:	G.SHDSL (рекоменд. ITU-T G.991.2.bis);
Тип соединения:	точка-точка;
Количество проводов линии связи:	2 (одна пара);
Скорость передачи, кбит/с:	192-15296, по одной витой паре;
Линейный код:	ТС-РАМ;
Вид связи:	полный дуплекс.
Параметры интерфейса Ethernet:	Тип интерфейса: 10/100 BaseT; Количество портов: 1; Режим работы: Полу- и полнодуп-лексный; Совместимость: ANSI/IEEE Std 802.3; Автоопределение MDI/MDI-X: есть.
Питание:	Дистанционное питание по инфор-мационной паре, VDC: 100...240; Потребляемая мощность, Вт: не более 2. Питание подключаемых устройств: PoE: class 2; Дополнительный выход, VDC: 48 для подключения устройств не под-держивающих технологию PoE с потребляемой мощностью до 6 Вт.
Условия эксплуатации:	Температура воздуха: 10 .. 80 °С.

ДОДАТОК Е

Таблиця Е.1 – Технічні характеристики Allied Telesis AT-FS202

Розміри (ширина x глибина x висота), см	44 x 25.7 x 4.3
Вага, кг:	3,15
Параметри живлення:	Вбудований блок живлення • Вхідна напруга: 100 - 240 В АС • Вихідна напруга: 12 В ВС • Струм: 1.5 А • Потужність: 26.5 Вт
Комплектація:	• Комутатор AT-8000S / 24 • Шнур живлення АС • Набір для установки в стійку • Гумові ніжки для установки на стіл • Кабель RS232 для управління (RJ-45) • Стековий кабель
Порти інтерфейсу:	
Мідні інтерфейси:	24 x RJ-45 10/100
Оптичні інтерфейси:	Об'єднані порти: • 2 x RJ-45 10/100 / 1000T • 2 x SFP 100FX, 1000SX, 1000LX
Інші інтерфейси:	1 x RS232, контакти DB9, тато
МЕРЕЖЕВІ ОСОБЛИВОСТІ:	
Підтримувані стандарти:	• Інтерфейсні стандарти: - IEEE 802.3 10T - IEEE 802.3u 100TX i 100FX - IEEE 802.3z 1000SX - IEEE 802.3ab 1000T • Загальні стандарти: - IEEE 802.1D мостові з'єднання - IEEE 802.3x зворотне тиск / управління по-струмом • Стандарти резервування: - IEEE 802.1D Spanning-Tree Protocol - IEEE 802.1W Rapid Spanning-Tree - IEEE 802.1s Multiple Spanning-Tree BPDU захист - IEEE 802.3ad LACP агрегація з'єднання (до 8 членів на групу і до 8 груп на пристрій) - Канал статичного порту • Стандарти Multicast: - RFC 1112 IGMP snooping (ver. 1) - RFC 2236 IGMP snooping (ver. 2) - RFC 3376 IGMP snooping (ver. 3) - RFC 3376 IGMP querier • Можливість пересилки / фільтрації незарегі-

	стрировать МС-кадрів
продуктивність:	• Оперативна пам'ять: 64 МБ • Флеш-пам'ять: 16 МБ • Процесор 400 МГц • VLAN ID: до 4,096 • MAC-адрес: 8,000 • Розмір буфера пакетів: 1 Мбіт • Комутація з провідний швидкістю на всіх портах Ethernet для пакетів всіх розмірів • Пропускна здатність: до 9.52 мільйонів пакетов / с • Комутаційна здатність: 12.8 Гбіт / с • Режим зберігання та пересилання • Неблокована комутація • Автоматичний MDI / MDI-X • Затримка: - 10 Мбіт - 85.71 мкс - 100 Мбіт - 17.30 мкс - 1000 Мбіт / с - 2.72 мкс
стекирование:	• До 6 юнітів • Єдина система управління • Управління через 1 IP-адреса • Майстер резервування • Кільцева топологія резервування в стеці продуктивністю 20 Гбіт / с • Агрегація з'єднання / каналів в стеку • Віддзеркалення портів в стеку • VLAN в стеці
управління:	• Управління та спостереження: - WEB, CLI, Telnet, SSH, послідовний консольний порт - RFC 1157 SNMPv1 / v2c - RFC 2570 SNMPv3 - RFC 1213 MIB-II - RFC 1573 розвиток MIB-II - RFC 1215 TRAP MIB - RFC тисячі чотиреста дев'яносто три міст MIB - RFC 2863 група інтерфейсів MIB - RFC 1 643 Ethernet like MIB - RFC тисяча сімсот п'ятьдесят сім 4 групи RMON: статистика, історія, сигнали, події - RFC 2674 IEEE 802.1Q MIB - RFC +1866 HTML - RFC 2068 HTTP - RFC 854 Telnet - RFC 783 TFTP - LLDP - IEEE 802.1ab - LLDP-MED • Призначення IP-адрес: - RFC 951 / RFC тисяча п'ятсот сорок-два BootP / DHCP ручне - DHCP snooping - RFC 2030 SNTP, Simple Network Time Protocol - Події в системній журналі - Два образи програмного забезпечення

Безпека:	• Безпечне управління: захист логіном і паролем • SSHv2 для управління через Telnet • SSLv3 для управління через веб-інтерфейс • RFC тисячу чотиреста дев'яносто два TACACS + • RFC 2618 ідентифікація RADIUS • IEEE 802.1x динамічні VLAN • IEEE 802.1x облікові записи RADIUS • IEEE 802.1x режим декількох сесій • IEEE 802.1x дію при порушенні • IEEE 802.1x порушення одного хоста • IEEE 802.1x таймаут гостьових VLAN • IEEE 802.1x ідентифікація не потрібно • Security login banner • RFC 2865 IEEE 802.1x управління мережевим доступом в залежності від портів • Управління мережевим доступом по MAC-адресами • Гостьові VLAN • ACL - списки управління доступом: - IP-адреси - MAC-адреси • Контроль широкомовних штормів
QoS:	• QoS in Layer 2 (клас обслуговування, сумісний з IEEE 802.1p) • Пріоритизація трафіку за допомогою полів IEEE 802.1p, ToS, DSCP • Асоціація пріоритетів IEEE 802.1p і очердей CoS для пріоритизації вихідного трафіку • Суворе черговість і Weighted Round Robin
Мережеві функції:	• VLAN - IEEE 802.1Q VLAN tagging - До 256 активних VLAN - VLAN в залежності від портів - VLAN в залежності від MAC-адрес - Приватні VLAN - GARP VLAN Registration Protocol (GVRP) • IPv6 - IPv6 QoS - IPv6 ACL - Хост IPv6 - RFC 2461 виявлення найближчих IPv6 - RFC 2463 ICMPv6: Internet Control Message - RFC один тисяча дев'ятсот вісімдесят одна виявлення Path MTU - Подвійний стек протоколів IPv4 / IPv6 - Тунелювання IPv6 через IPv4 - Мережеве управління IPv6 - Додатки IPv6: WEB / SSL сервер Telnet / SSH, AAA / Radius, управління ACL, SNMP, PING, TFTP / копіювання, системний журнал

ДОДАТОК Є

Таблиця Є.1 – Різновиди Ethernet і їх фізичні характеристики

Стандарт	Фізична специфікація	Кабелі роз'єми	Обмеження на довжину фіз. сегмента, м	Макс. число повторювачів	Макс. число станцій	мережі, м
Ethernet (IEEE 802.3i)	10Base5 (Thicknet)	Толстий коаксиал RG-8/11, роз'єми AUI	500 min 2,5 м	4 (2 сегмента без узлов)	100	2500
	10Base2 (Cheapernet)	Тонкий коаксиал RG-58A/U, роз'єми BNC	185 (200) min 0,5 м		30	925
	10BaseTX	2ВП UTP3-4-5, RJ-45	100	4	1024	500
	10BaseF	ОМ ОВ / ММ ОВ 62.5, роз'єми ST	1000/5000	-	2	1000/5000
Gigabit Ethernet (802.3z)	1000BaseLX	ММ ОВ / ОМ ОВ, роз'єми ST, SC	316 (550/3000)	-	2	550/3000
	1000BaseSX	ММ ОВ 62.5/50 мкм роз'єми ST, SC	275 (300/550)	-		300/550
	1000BaseCX	коаксиал, (ВП STP), RJ-45	25	-		25
(802.3ab)	1000BaseT	ВП STP5-6 RJ-45	100	-		100
Fast Ethernet (IEEE 802.3u)	100BaseTX	2ВП UTP, STP Type 1, роз'єми RJ-45	100	1 класу І 2 класу ІІ (кабель между повторит. – до 5 м)	1024	200-320
	100BaseFX	ММ ОВ 62.5, 125 (кабель между мкм, роз'єми ST, SC)	160 (реп) /412 (полудуплекс) / 2000 (полнодуплексн)			
	100BaseT4	4ВП UTP3-4-5, RJ-45	100			

Умовні скорочення: 2ВП - 2-жильна, 4ВП - 4-жильна кручена пара;
ОВ - оптоволокно, ММ - многомодове, ОМ - одномодове.

ДОДАТОК Ж



Рисунок Ж.1 – Графіки мережевого трафіку з кінцевих пристроїв в мережі

ДОДАТОК 3

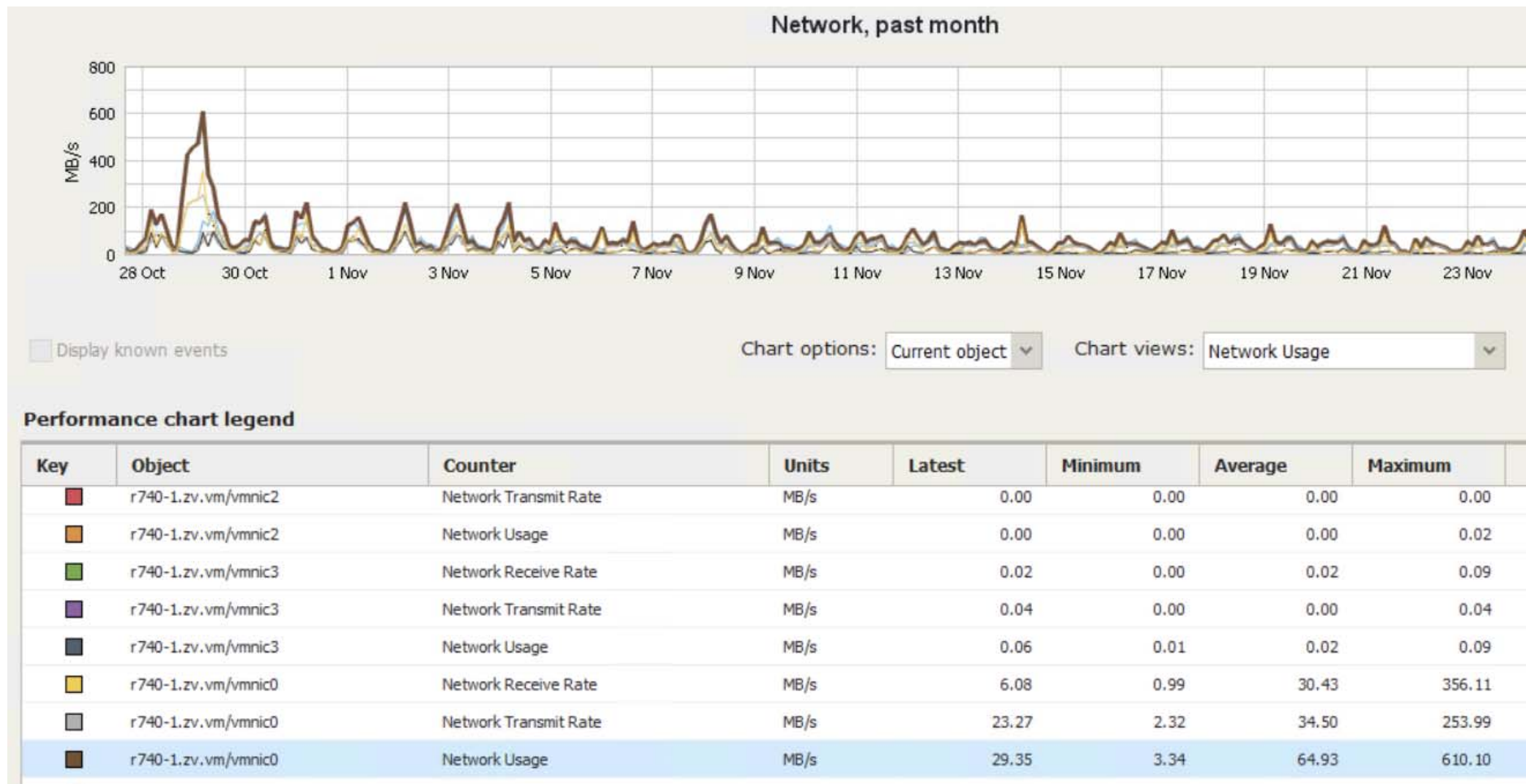


Рисунок 3.1 – Пікові навантаження на кінцевих пристроях в мережі