Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних систем та технологій
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента Міненко Владлена В'ячеславовича
(П.І.Б.)
академічної групи 123-17ск-1
(шифр)
спеціальності 123 Комп'ютерна інженерія
(код і назва спеціальності)
за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)
на тему "Комп'ютерна система правління підприємства ПГОК з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі"
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
кваліфікаційної роботи	ас. Бешта Д.О.			
розділів:				
апаратний розділ	доц. Ткаченко С.М.			
розрахунок мережі	ас. Панферова Д.О.			
економічний розділ	ст. викл. Яремчук І.О.			
охорона праці	доц. Іконніков М.Ю.			
Рецензент				
Нормоконтролер	Проф. Цвіркун Л.І.			

Дніпро
2020

ЗАТВЕРДЖЕНО:
завідувач кафедри
інформаційних систем
та технологій
(повна назва)
_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)

"27" січня 2020 року.

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавр

студента _Міненко В.В._ **академічної групи**_123-17ск-1_
(прізвище, ініціали) (шифр)

спеціальності _____123 Комп'ютерна інженерія_____
(код і назва спеціальності)

за освітньо-професійною програмою____123 Комп'ютерна інженерія_____
(офіційна назва)

на тему__"Комп'ютерна система правління підприємства ПГОК з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі"__

затвержена наказом ректора НТУ «Дніпровська політехніка» від 21.05.2020 № 771-Л

Розділ	Зміст завдання	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати завдання, конкретизувати предмет та мету роботи	18.05.2020
Технічні вимоги до комп'ютерної системи	На основі матеріалів виробничих практик, інших науково-технічних джерел сформулювати технічні вимоги до розробки комп'ютерної системи	25.05.2020
Спеціальна частина	Розв'язати завдання з розробки комп'ютерної системи з опрацюванням побудови і захисту інформації та налаштуванням корпоративної мережі	01.06.2020
Економічна частина	Економічно обгрунтувати доцільність витрат на створення та дослідження системи	05.06.2020
Охорона праці	Розробити організаційно-технічні заходи, щодо реалізації правил безпеки при експлуатації системи	10.06.2020

Завдання видано _____ ас. Бешта Д.О.
(підпис керівника) (прізвище та ініціали)

Дата видачі _20.04.2020 р._

Дата подання до атестаційної комісії __16.06.2020 р.__

Прийнято до виконання _____ Міненко В.В.

РЕФЕРАТ

Пояснювальна записка: 97 с., 23 рис., 10 табл., 1 додаток, 15 джерел.

Об’єкт розробки: комп'ютерна система правління підприємства ПГОК з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі.

Мета: створення комп’ютерної системи та мережі для адміністративних підрозділів підприємства ПГОК.

Розроблена комп’ютерна система з можливістю гнучкої зміни числа і набору виконуваних функцій шляхом перепрограмування, орієнтована на побудову мережі для адміністративних підрозділів підприємства ПГОК, а також для збору, пересиланню та підготовки статистичної інформації.

Система виконана відкритою і дозволяє здійснювати технічну і програмну модернізацію системи, а так само забезпечує виконання функцій з об’єднання підрозділів у мережу; збір обробку, накопичення інформації у базах даних; комунікацію між кінцевими споживачами у різних підрозділах та доступ до загальних ресурсів.

Розробка комп’ютерної мережі виконана відповідно до завдання на дипломну роботу бакалавра.

Розроблена схема мережі реалізована у вигляді моделі на симуляторі Cisco Packet Tracer і перевірена її робота.

Результати перевірки у вигляді таблиць, графіків описані і наводяться у пояснювальній записці або додатках.

СИСТЕМА, МЕРЕЖА, ЛОКАЛЬНА МЕРЕЖА, МЕРЕЖЕВІ ЗАСОБИ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

КС – комп’ютерна система;

ПК – персональний комп’ютер;

Ethernet – технологія передачі даних по мережі;

UTP –не екранована кручена пара;

FTP –екранована кручена пара;

WAN – (Wide Area Network) це глобальна комп'ютерна мережа;

VPN – (Virtual Private Network) віртуальна приватна мережа;

QoS – (Quality of Service) технологія надання різних класів трафіку різних пріоритетів в обслуговуванні;

WiFi – технологія бездротової локальної мережі з пристроями на основі стандартів IEEE 802.11;

GSM – (Global System for Mobile Communications) глобальний стандарт цифрового мобільного стільникового зв'язку з розділенням каналів за часом та частотою

ВСТУП

Робота гірничих підприємств характеризується великими обсягами видобувних і підготовчих робіт для підземних розробок, розкривних і видобувних для відкритих розробок, а також переробки і транспортування гірничої маси. Для цього використовується велика кількість різноманітного обладнання, характерного для певних гірничо-геологічних, метеорологічних і кліматичних умов, споживані потужності якого коливаються у великих межах.

Всі виробничі процеси на гірничих підприємствах діляться на основні та допоміжні, пов'язані між собою в просторі і в часі єдиної технологічної схеми, призначеної для випуску продукції (вугілля і руди). Операції виконуються послідовно різними машинами в певному темпі на основі збереження безперервності загального процесу.

Машини та механізми, що використовуються при організації робіт на гірничих підприємствах, утворюють технологічний комплекс, тобто технологічно пов'язану сукупність гірських машин і транспортних засобів, що забезпечують максимальну продуктивність видобувних машин, починаючи з підготовки гірських робіт до виїмки і закінчуючи переробкою корисних копалин.

Виробничий процес полягає в дії людей і знарядь виробництва з видобутку і переробці корисних копалин, отже, до складу виробничого процесу входить не тільки монтаж і експлуатація обладнання, а й роботи з підтримки його в справному стані.

Високу продуктивність праці при використанні гірських машин і устаткування можна досягти тільки за умови високоякісного монтажу, технічного обслуговування і ремонту, що гарантують надійну і довговічну роботу.

1 СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Стисла характеристика гірничо-збагачувальної галузі

Гірничо-збагачувальний комбінат (скорочено ГЗК) - комплексне гірниче підприємство з видобутку та переробки твердих корисних копалин.

На ГЗК видобувається і переробляється частіше один вид корисної копалини: залізна руда, марганцева руда, азбестова руда, апатитова руда та інші, проте можуть добувати кілька видів руди: мідна та нікелева, руди поліметалів.

Кінцевою продукцією гірничо-збагачувального комбінату є концентрат, агломерат або окатиші, які направляються для подальшої переробки (наприклад, в металургійне виробництво) або використання (наприклад в якості добрива в сільському господарстві).

1.2 Характеристика і структура підприємства ПГЗК

ВАТ «Полтавський ГЗК» - найбільший в Україні виробник і експортер залізорудних окатишів, які використовуються в чорній металургії і виробництві сталі. Розташований в місті Горішні плавні (Полтавська область). Введено в експлуатацію в 1970 році під назвою Дніпровський ГЗК.

Продуктивність комбінату в різний час становить від 8,6 млн до 12 млн тонн окатишів на рік, з яких близько 90% йдуть на експорт.

Полтавський ГЗК має повний технологічний цикл - від видобутку сирої руди до виробництва залізорудних окатишів - підготовленої сировини для металургійних заводів.

Переробка руди, виробництво концентрату і окатишів виробляється на переробному комплексі, що складається з дробильної, збагачувальної фабрик і цеху виробництва окатишів.

Сировинна база комбінату - два родовища Кременчуцької магнітної аномалії (Горішнє Плавнінського і Лавриківського), що розробляються одним кар'єром Дніпровського рудника.

Комбінат має наступну структуру:

– дніпровське рудоуправління;

- гірничо-транспортний цех;
- залізничний цех;
- дробильна фабрика;
- збагачувальна фабрика;
- цех виробництва окатишів;
- цех шламового господарства.

Схема організаційної структури підприємства ПГЗК зображена на рисунку 1.1.

До складу дніпровського рудоуправління відносяться такі основні відділи:

1) керуючий директор;
2) відділ безпеки;
3) відділ технічного контролю;
4) відділ кадрів;
5) відділ первинного обліку;
6) відділ роботи з персоналом;
7) виробничій відділ;
8) відділ соціальних питань;
9) відділ охорони зовнішнього середовища;
10) відділ постачання;
11) відділ капітального будування;
12) відділ збуту;
13) відділ головного механіка
14) відділ фінансів та економіки;
15) відділ ОП, ТБ і ПК;
16) відділ інформаційних технологій;
17) відділ гірничої справи;
18) другий відділ;
19) відділ агломерування;
20) відділ управління справами;
21) відділ збагачення;
22) відділ документації.
23) відділ енергетики;

1.3 Топологічне розміщення структурних підрозділів правління підприємства та технології збору та передачі інформації

Топологічна схема розміщення структурних підрозділів підприємства ПГЗК представлена на рисунку 1.2. Будівлі правління комбінатом розташовані на площі з радіусом 200 метрів. До загального складу входять дев’ять будівель:

- (I) – головна будівля правління, чотири поверхи;
- (II-IV) – адміністративні корпуси, два поверхи кожний;
- (V) – корпус з актовою залою та їдальнею, два поверхи;

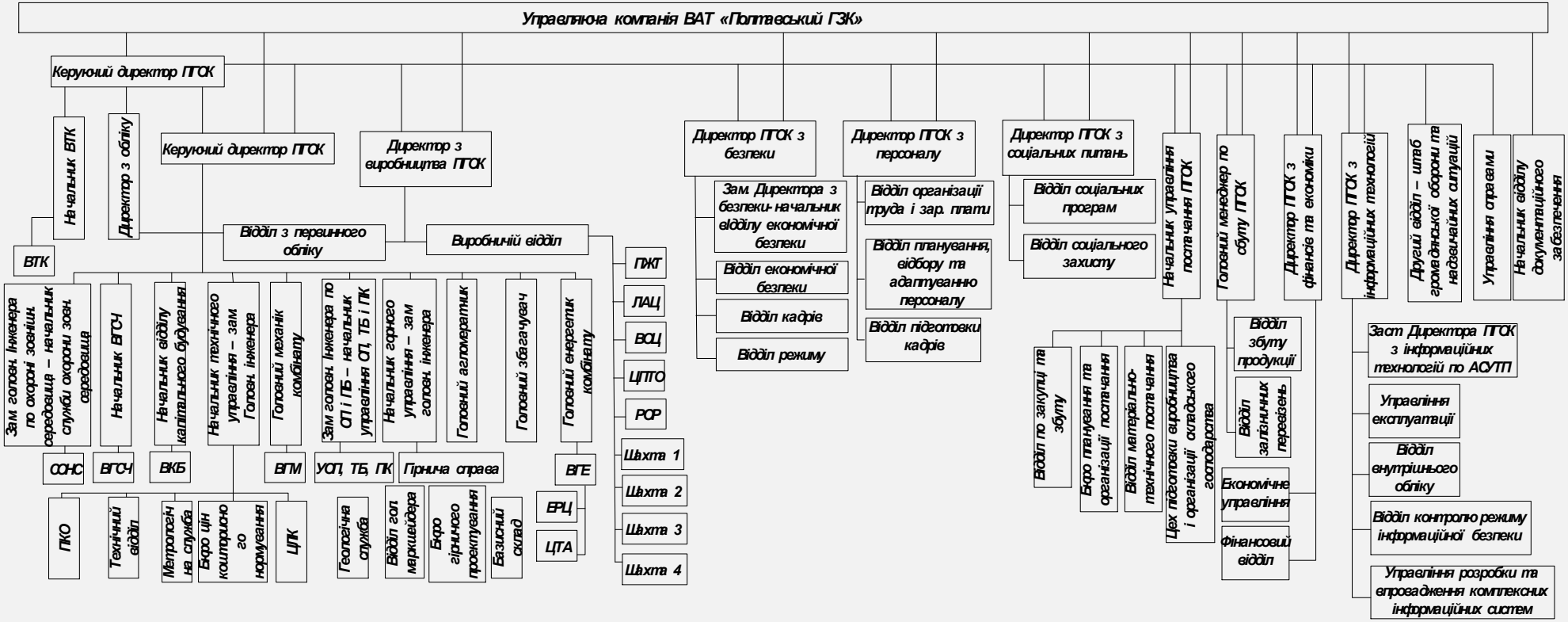

Рисунок 1.1 − Схема організаційної структури підприємства ПГЗК

Рисунок 1.2 − Топологічна схема розміщення структурних підрозділів підприємства ПГЗК

– (VI, VII) – корпуса проектного бюро, три поверхи кожний;
– (VIII, IX) – корпуса ТОВ «Єристівський гірничо-збагачувальний комбінат», два поверхи кожний.

Розташування відділів по будівлях вказано у таблиці 1.1 нумерація будівель та відділів згідно вищеописаної.

Таблиця 1.1 Розташування відділів у будівлях.

Номер будівлі	Номер відділу
I	1,3,4,5,6,8,9,12,14,16
II	2,13,15,22
III	10,17,19,21
IV	7,18,20,22
V	-
VI	11
VII	-
VIII	-
IX	-

Загальні дані про відстані між об’єктами вказано на рисунку 1.3

Збір даних на підприємстві забезпечується технічними засобами, що дозволяють здійснювати збір швидко і високоякісно і підтримують операції введення інформації і представлення даних в електронній формі. Як засоби збору в інформаційній системі підприємства виступають агрегати, що представляють собою сукупність пристроїв і програмного забезпечення до них, які служать для перетворення інформації, представленої в неелектронній формі, в електронну для її подальшого використання в системі.

Зібрана інформація, перекладена в електронну форму, підлягає правильному зберіганню і вимагає забезпечення до неї доступу.

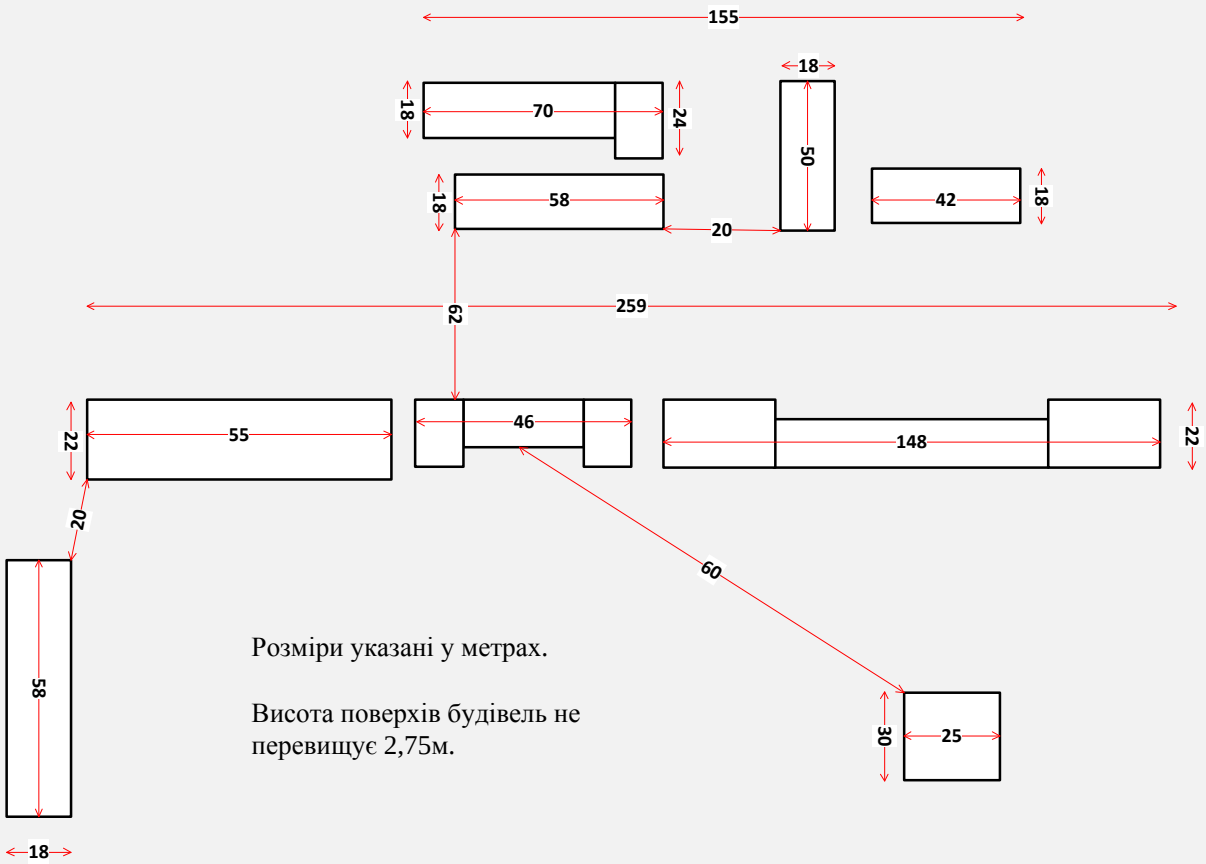

Рисунок 1.3 − Загальні дані про відстані між об’єктами

В ролі структур зберігання даних виступають бази даних, банки даних або сховища даних які розміщено на локальних або глобальних серверах підприємства.

Слід зазначити, що система зберігання даних забезпечує резервне копіювання, архівування, структурованого зберігання і відновлення даних в необхідні терміни.

На підприємстві використовується технологічний процес обробки інформації у певна послідовність взаємопов'язаних процедур, що виконуються для перетворення первинної інформації з моменту її виникнення до отримання необхідного результату.

Сукупність процедур залежить від таких факторів: характер і складність розв'язуваної задачі; алгоритм перетворення інформації; використовувані технічні засоби; терміни обробки даних; використовувані системи контролю; число користувачів і т.і.

Передача інформації здійснюється через канал передачі, який забезпечує необхідну ємність каналу.

Відтворення та відображення інформації відбувається за допомогою технічних засобів для безпосереднього сприйняття працівниками.

1.4 Принципи, технічні способи та математичні методи інформаційного забезпечення об’єкта впровадження

Існуюча мережа правління підприємства має архітектуру, яка відображена на рисунку 1.4.

Основні комунікаційні вузли, на яких базується мережа є обладнанням торгової марки Cisco. Мережа має розподілену структуру.

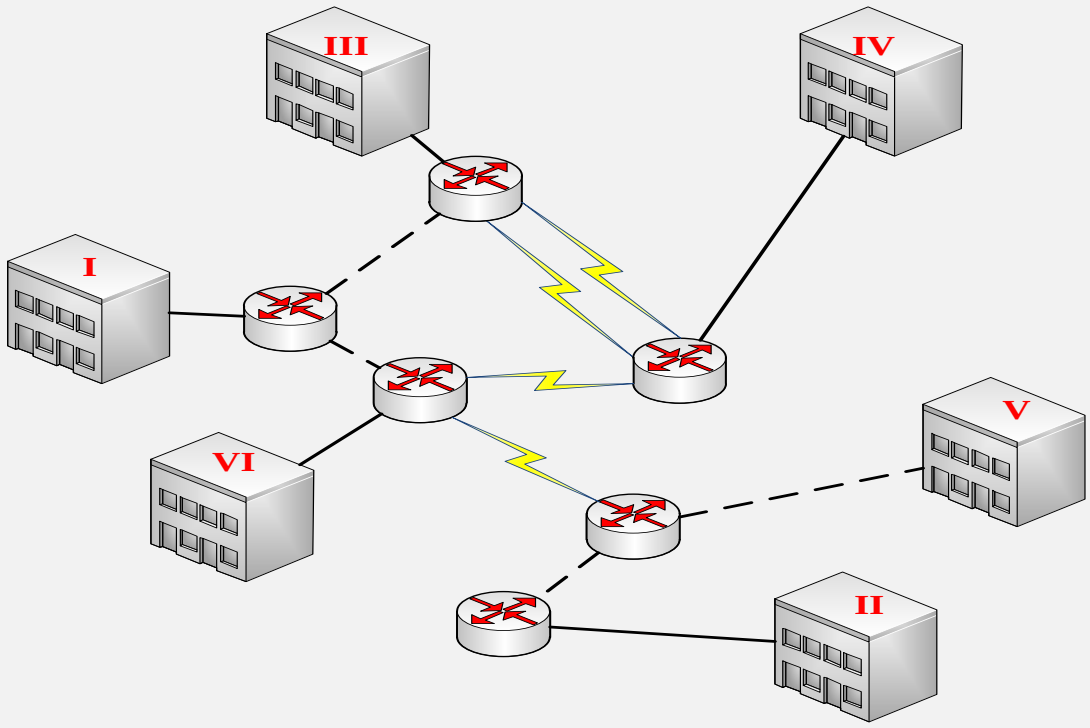

Рисунок 1.4 − Архітектура мережі підприємства

До математичного забезпечення віднесено сукупність математичних методів, моделей і алгоритмів розв'язування завдань, які застосовуються в системі та мережі; моделі та алгоритми, що входять до цього забезпечення як інструмент подальшої розробки програмних засобів. Моделі системи та мережі належать до організаційного забезпечення.

1.5 Аналітичний огляд існуючих способів обробки та передачі інформації, принципів побудови об’єкта проектування, відомих рішень у галузі

Розглянемо варіанти вирішення завдання організації доступу до сервісів корпоративної мережі з Інтернет.

Варіант 1. Плоска мережа. В даному варіанті всі вузли корпоративної мережі містяться в одній, загальнії для всіх мережі («Внутрішня мережа»), в рамках якої комунікації між ними не обмежуються. Мережа підключена до Інтернет через прикордонний маршрутизатор/міжмережевий екран (далі - IFW).

Плюси варіанту: мінімальні вимоги до функціоналу IFW (можна зробити практично на будь-якому, навіть домашньому роутере); мінімальні вимоги до знань спеціаліста, який здійснює реалізацію варіанту.

Мінуси варіанту: мінімальний рівень безпеки. У разі злому, при якому порушник отримає контроль над одним з опублікованих в Інтернеті серверів, йому для подальшої атаки стають доступні всі інші вузли і канали зв'язку корпоративної мережі.

Варіант 2. DMZ. Для усунення зазначеної раніше нестачі - вузли мережі, доступні з Інтернет, поміщають в спеціально виділений сегмент - демілітаризовану зону (DMZ). DMZ організовується за допомогою міжмережевих екранів, що відокремлюють її від Інтернет (IFW) і від внутрішньої мережі (DFW).

При цьому правила фільтрації міжмережевих екранів виглядають наступним чином:

З внутрішньої мережі можна ініціювати з'єднання в DMZ і в WAN (Wide Area Network).

З DMZ можна ініціювати з'єднання в WAN.

З WAN можна ініціювати з'єднання в DMZ.

Ініціація з'єднань з WAN і DMZ до внутрішньої мережі заборонена.

Плюси варіанту: підвищена захищеність мережі від зломів окремих сервісів. Навіть якщо один з серверів буде зламаний, порушник не зможе отримати доступ до ресурсів, що знаходяться у внутрішній мережі (наприклад, мережевих принтерів, систем відеоспостереження і т.д.).

Мінуси варіанту: само по собі винесення серверів в DMZ не підвищує їх захищеність. Необхідний додатковий МЕ для відділення DMZ від внутрішньої мережі.

Варіант 3. Поділ сервісів на Front-End і Back-End. Як вже зазначалося раніше, розміщення сервера в DMZ жодним чином не покращує безпеку самого сервісу. Одним з варіантів виправлення ситуації є поділ функціоналу сервісу на дві частини: Front-End і Back-End. При цьому кожна частина розташовується на окремому сервері, між якими організовується мережева взаємодія. Сервера Front-End, що реалізують функціонал взаємодії з клієнтами, що знаходяться в Інтернет, розміщують в DMZ, а сервера Back-End, що реалізують решті функціонал, залишають у внутрішній мережі. Для взаємодії між ними на DFW створюють правила, що дозволяють ініціацію підключень від Front-End до Back-End.

Як приклад розглянемо корпоративний поштовий сервіс, який обслуговує клієнтів як зсередини мережі, так і з Інтернет. Клієнти зсередини використовують POP3/SMTP, а клієнти з Інтернет працюють через Web-інтерфейс. Зазвичай на етапі впровадження компанії вибирають найбільш простий спосіб розгортання сервісу і ставлять все його компоненти на один сервер. Потім, у міру усвідомлення необхідності забезпечення інформаційної безпеки, функціонал сервісу поділяють на частини, і та частина, що відповідає за обслуговування клієнтів з Інтернет (Front-End), виноситься на окремий сервер, який по мережі взаємодіє з сервером, які реалізують залишився функціонал (Back -End). При цьому Front-End розміщують в DMZ, а Back-End залишається у внутрішньому сегменті. Для зв'язку між Front-End і Back-End на DFW створюють правило, яке дозволяє, ініціацію з'єднань від Front-End до Back-End.

Плюси варіанту: у загальному випадку атаки, спрямовані проти захищається сервісу, можуть «спіткнутися» про Front-End, що дозволить нейтралізувати або істотно знизити можливі збитки. Наприклад, атаки типу TCP SYN Flood або slow http read, спрямовані на сервіс, приведуть до того, що Front-End сервер може виявитися недоступним, в той час як Back-End буде продовжувати нормально функціонувати і обслуговувати користувачів. У загальному випадку на Back-End сервері може не бути доступу в Інтернет, що в разі його злому (наприклад, локально запущеним шкідливим кодом) утруднить віддалене керування ним з Інтернет. Front-End добре підходить для розміщення на ньому брандмауера рівня додатків (наприклад, Web application firewall) або системи запобігання вторгнень (IPS, наприклад snort).

Мінуси варіанту: для зв'язку між Front-End і Back-End на DFW створюється правило, яке дозволяє ініціацію з'єднання з DMZ у внутрішню мережу, що породжує загрози, пов'язані з використанням даного правила з боку інших вузлів в DMZ (наприклад, за рахунок реалізації атак IP spoofing, ARP poisoning і т. д.) Не всі сервіси можуть бути розділені на Front-End і Back-End. У компанії повинні бути реалізовані бізнес-процеси актуалізації правил міжмережевого екранування. У компанії повинні бути реалізовані механізми захисту від атак з боку Порушників, які отримали доступ до сервера в DMZ.

Варіант 4. Захищений DMZ. DMZ це частина мережі, доступна з Internet, і, як наслідок, підвладна максимального ризику компрометації вузлів. Дизайн DMZ і приємним в ній підходи повинні забезпечувати максимальну живучість в умовах, коли Порушник отримав контроль над одним з вузлів в DMZ. В якості можливих атак розглянемо атаки, до яких схильні практично всі інформаційні системи, що працюють з настройками за замовчуванням.

Більша частина атак базується на вразливості архітектури сучасних Ethernet/IP мереж, що полягають в можливості Порушника підробляти в

мережевих пакетах MAC і IP адреси. Експлуатацію даних вразливостей іноді виділяють в окремий види атак: MAC spoofing; IP spoofing.

Перелік захисних заходів за цим варіантом:

DMZ розділяється на IP-підмережі з розрахунку окрема підмережа для кожного вузла.

IP адреси призначаються вручну адміністраторами. DHCP не використовується.

На мережеві інтерфейси, до яких підключені вузли DMZ, активується MAC і IP фільтрація, обмеження по інтенсивності широкомовного трафіка і трафіку, що містить TCP SYN запити.

На комутаторах відключається автоматичне узгодження типів портів, забороняється використання native VLAN.

На вузлах DMZ і серверах внутрішньої мережі, до яких дані вузли підключаються, налаштовується TCP SYN Cookie.

Відносно вузлів DMZ (і бажано іншої мережі) впроваджується управління уразливими ПО.

У DMZ-сегменті впроваджуються системи виявлення та запобігання вторгнень IDS / IPS.

Плюси варіанту: високий ступінь безпеки.

Мінуси варіанту: підвищені вимоги до функціональних можливостей обладнання. Трудовитрати у впровадженні та підтримці.

Варіант 5. Back connect. Розглянуті в попередньому варіанті заходи захисту були засновані на тому, що в мережі було присутнє пристрій (комутатор / маршрутизатор / міжмережевий екран), здатне їх реалізовувати. Але на практиці, наприклад, при використанні віртуальної інфраструктури (віртуальні комутатори часто мають дуже обмежені можливості), подібного пристрою може і не бути.

Загальна схема роботи даного варіанту виглядає наступним чином:

На сервер в DMZ інсталюється SSH / VPN сервер, а на сервер у внутрішній мережі інсталюється SSH / VPN клієнт.

Сервер внутрішньої мережі ініціює побудову мережевого тунелю до сервера в DMZ. Тунель будується з взаємною аутентифікацією клієнта і сервера.

Сервер з DMZ в рамках побудованого тунелю ініціює з'єднання до сервера у внутрішній мережі, по якій передаються захищаються дані.

На сервері внутрішньої мережі налаштовується локальний міжмережевий екран, фільтруючий трафік, що проходить по тунелю.

Використання даного варіанта на практиці показало, що мережеві тунелі зручно будувати за допомогою OpenVPN, оскільки він володіє наступними важливими властивостями: кросплатформеність (можна організовувати зв'язок на серверах з різними операційними системами); можливість побудови тунелів з взаємною аутентифікацією клієнта і сервера; можливість використання сертифікованої криптографії.

Плюси варіанту: архітектурне зменшення кількості векторів атак на захищається сервер внутрішньої мережі. Забезпечення безпеки в умовах відсутності фільтрації мережевого трафіку. Захист даних, що передаються по мережі, від несанкціонованого перегляду та зміни. Можливість виборчого підвищення рівня безпеки сервісів. Можливість реалізації двухконтурной системи захисту, де перший контур забезпечується за допомогою міжмережевого екранування, а другий організовується на базі даного варіанту.

Мінуси варіанту: впровадження і супровід даного варіанту захисту вимагає додаткових трудових витрат. Несумісність з мережевими системами виявлення та запобігання вторгнень (IDS / IPS). Додаткова обчислювальна навантаження на сервера.

1.6 Завдання і мета роботи

Завданням даної кваліфікаційної роботи є розробка комп’ютерної системи підприємства з детальною проробкою мережі підприємства.

Ураховуючи існуючу на підприємстві архітектуру мережі з попередньою кількістю підмереж, їх взаємозв’язками і кількістю комп’ютерів та обладнанням необхідно виконати розрахунок налаштувань для заданої топології мережі, вибір інтерфейсу каналів зв’язку та протоколу обміну, розрахунок топологічної схеми комп’ютерної системи, розрахунок налаштувань маршрутизації комп’ютерної мережі, а також виконати подальше моделювання і перевірки роботи комп’ютерної системи.

Окрім того необхідно провести аналіз об’єкту за для проектування нової мережі підрозділу підприємства та розробити специфікацію апаратних засобів комп’ютерної системи, у тому числі засобів збору та передачі даних. Виконати вибір відповідного фізичного середовища, кабелів, портів і з'єднувачів для підключення мережевих пристроїв до інших пристроїв мережі і вузлів, вибір мережевих пристроїв і компонентів, необхідних для задоволення технічних вимог мережі і аналітичні розрахунки споживаної потужності, об’ємів і швидкостей передачі даних каналами мережі з урахуванням вибраних апаратних засобів, затримок на обробку даних на вузлах мережі.

1.7 Визначення можливих напрямків рішення поставлених завдань

Варіанти реалізації функцій системи мають засновуватися на основі відомих технічних рішень, що дозволяє підібрати найбільш придатний варіант з числа відомих розробок, які базуються на рішеннях з науково-технічних і патентних джерел, науково-технічних звітах, літературі, та ін. джерел доступних широкому колу осіб.

Комплекс технічних засобів передачі зберігання та обслуговування інформації має вибиратися орієнтуючись на серійні комп’ютерні засоби та апаратуру на сучасній елементній базі.

2 ТЕХНІЧНІ ВИМОГИ ДО КОМПЮТЕРНОЇ СИСТЕМИ

2.1 Вимоги до Системи в цілому

2.1.1 Вимоги до структури та функціонування Системи

Система являє собою корпоративну мережу та призначена для організації середовища передачі інформації між відділами правління підприємства ПГОК.

Описані в технічні вимоги повинні використовуватися в якості основи при проектуванні локальної обчислювальної мережі для правління підприємства ПГОК.

Структура комп’ютерної мережі підприємства складається з 5 підмереж об’єднаних у загальну мережу підприємства.

Окремі під мережі мають організовувати віртуальні підмережі та підмережі з резервуванням каналів.

Загальна комп’ютерна мережа підприємства має забезпечувати можливість розширення для подальшого розвитку.

Канали звязку мають бути розраховані на максимальну завантаженість при пересиланні даних по мережі.

Функціональна робота спроможність має бути налаштована згідно з вимог, які визначаються потребами підприємства.

Для захисту інформації в комп’ютерній системі від несанкціонованого доступу мають бути розроблені відповідні методи.

2.1.2 Вимоги до чисельності та кваліфікації персоналу, який обслуговує Систему і режим його роботи

Кількість і кваліфікація технологічного персоналу визначається чинним штатним розкладом.

Перед введенням Системи в експлуатацію обслуговуючий персонал повинен пройти відповідне навчання.

2.1.3 Показники призначення

Комп'ютерна система правління підприємства ПГОК призначена для організації середовища передачі інформації між відділами підприємства з виконанням вимог до функціонування та безпеки корпоративної мережі.

2.1.4 Вимоги до надійності системи

Надійність Системи загалом визначається надійністю кожного елементу Системи. Надійність елементів Системи (мережеве обладнання, кабельні траси, станції кінцевих споживачів тощо) визначаються надійністю гарантованою виробником того чи іншого елементу за паспортними характеристиками.

Для забезпечення гарячої заміни обладнання при умови виходу його з ладу підприємство має тримати ЗІП на найбільш важливі елементи.

2.1.5 Вимоги до безпеки

Для Системи мають виконуватися наступні вимоги з безпеки:

- мінімально допустиме навантаження для серверних шаф 750 кг, телекомунікаційних - 450 кг;
- з техніки безпеки двері обов'язково повинні відкриватися назовні, не мати центральний упор і поріг. Розмір двері: висота не менше 200 см, ширина - 91 см;
- повинен бути передбачений доступ до спільного електрода системи заземлення.
- всі елементи металевої конструкції повинні бути заземлені;
- в конструкції стель не використовуються фальш-панелі;
- каркас вироби повинен витримувати значні навантаження.

Розподільні шафи відповідно до міжнародного стандарту ANSI/NECA /BICSI 568-2001 заземлюються мідним провідником з площею розтину не менше 16,8 мм^2.

Комфортні умови роботи персоналу повинні відповідати чинним санітарним нормам по СанПіН 2.2.2 / 2.4.1340-03 "Гігієнічні вимоги до персональних електронних обчислювальних машин і організації роботи. Санітарно - епідеміологічні правила і нормативи".

Рівень шуму і звукової потужності в місцях розташування персоналу не повинні перевищувати значень, встановлених ГОСТом 12.1.003 ССБТ "Шум. Общие требования безопасности", і санітарними нормами. При цьому повинні бути враховані рівні шумів і звукової потужності, створювані всіма джерелами.

Вимоги безпеки при монтажі, наладці, експлуатації, обслуговуванні і ремонті технічних засобів Системи повинні бути приведені в Документації на технічні засоби.

2.1.6 Вимоги по ергономіки та технічної естетики

Серверні шафи призначаються, відповідно до стандарту, для комунікаційних вузлів і засобів підтримки. На одному поверсі рекомендується розміщувати не менше одного пристрою для зберігання.

До телекомунікаційних серверних шаф мають виконуватися вимоги стандарту (TIA-569-A):

- в робочій зоні рівень освітлення шафи повинен бути на відстані 1 метра від підлоги і не менше 540 лк;
- слід передбачати не менше 2 дуплексних виділених розеток, при цьому живлення вони отримують з окремого фідера;
- з техніки безпеки двері обов'язково повинні відкриватися назовні, не мати центральний упор і поріг. Розмір двері: висота не менше 200 см, ширина - 91 см.
- для точного горизонтального розміщення передбачаються регульовані опори;
- конструкція шафи повинна передбачати легкий доступ до встановлених компонентів.

При установці комунікаційних приладів в розподільних шафах апаратура розміщується так, щоб полегшити доступ технічних фахівців до фронтальним і заднім панелям. Щоб правильно помістити обладнання, дотримуються правил:

- сервера і джерела безперебійного живлення встановлюються вниз;
- у верхній зоні монтується обладнання з оптичними портами;
- патч-панелі встановлюються посередині, кросова техніка - на рівні очей;

Якщо шафи встановлюються в один ряд, то їх скріплюють в єдину модульну конструкцію, поєднуючи кріпленнями бічні частини каркаса. Розподільні шафи відповідно до міжнародного стандарту ANSI / NECA / BICSI 568-2001 заземлюються мідним провідником з площею розтину не менше 16,8 мм^2.

2.1.7 Вимоги до транспортабельності (для рухливих Систем)

Система не є рухливою. Особливих вимог не потребує.

2.1.8 Вимоги до експлуатації, технічного обслуговування, ремонту і збереженню компонентів Системи

Функціонування Системи повинно бути розраховане на цілодобовий режим роботи, з вимиканням необхідного сегменту на профілактику не частіше, ніж 1 раз на рік.

Види, періодичність і регламент обслуговування технічних засобів повинні бути вказані у відповідних інструкціях по експлуатації.

Відповідно до ГОСТу 21552-84 "Засоби обчислювальної техніки. Загальні технічні вимоги, правила приймання, методи випробувань, маркування, упаковка, транспортування і зберігання" і ГОСТом 12.1.005-88 ССБТ "Загальні санітарно-гігієнічні вимоги до повітря робочої зони", для нормального функціонування обчислювальної техніки в цих приміщеннях повинні бути забезпечені наступні умови:

- температура навколишнього повітря (20 ± 5) ° С;

- відносна вологість навколишнього повітря (60 ± 15)%;
- атмосферний тиск від 84 до 107 кПа (680-800 мм. Рт. Ст.);
- запиленість повітря в приміщенні - не більше 1 мг / куб. м при розмірі часток не більше 3 мкм;
- напруженість зовнішнього електричного поля повинна бути не більше 0.3 V / m;
- напруженість зовнішнього магнітного поля повинна бути не більше 5.0 А / м;
- частота вібрації повинна бути не більше 25 Гц при амплітуді зсувів не більше 0.1 мм.

У повітрі приміщень не повинно бути агресивних речовин, що викликають корозію. Необхідно забезпечити контроль температури, відносної вологості та атмосферного тиску в приміщеннях постійного перебування оперативного та обслуговуючого персоналу.

Уведення змінної напруги повинні здійснюватися через фільтри придушення перешкод. Нормально допустимі і гранично допустимі значення усталеного відхилення напруги на висновках приймачів електричної енергії дорівнюють відповідно ± 5 і ± 10% від номінальної напруги електричної мережі по ГОСТ 21128 (номінальну напругу).

Чинне значення напруги 220V ± 5% (гранично ± 10%), частота 50 ± 0,2 Гц (гранично ± 0,4 Гц), коефіцієнт несинусоїдальності - нормально до 8% і гранично-до 12% (ГОСТ 13109-97).

Обладнання Системи повинно бути забезпечено комплектом ЗІП на весь гарантійний термін. Протягом всього терміну служби Системи комплект ЗІП повинен поповнюватися відповідно до умов договору на сервісне обслуговування.

2.1.9 Вимоги до захисту інформації від несанкціонованого доступу

Захисту інформації, що обробляється в системах різного рівня і призначення, повинна передбачати комплекс організаційних, програмних,

технічних та, при необхідності, криптографічних засобів і заходів щодо захисту інформації при її автоматизованій обробці, зберіганні і передачі по каналах зв'язку.

Основними напрямками захисту інформації є:

- забезпечення захисту інформації від розкрадання, втрати, витоку, знищення, спотворення і підробки в результаті несанкціонованого доступу і спеціальних впливів;
- забезпечення захисту інформації від витоку технічними каналами при її обробці, зберіганні і передачі по каналах зв'язку.

В якості основних заходів захисту інформації рекомендуються:

- документальне оформлення переліку відомостей конфіденційного характеру з урахуванням відомчої та галузевої специфіки цих відомостей;
- реалізація дозвільної системи допуску виконавців (користувачів, обслуговуючого персоналу) до інформації і пов'язаним з її використанням робіт і документів;
- обмеження доступу персоналу та сторонніх осіб в захищаються приміщення і приміщення, де розміщені кошти інформатизації та комунікації і зберігаються носії інформації;
- розмежування доступу користувачів і обслуговуючого персоналу до інформаційних ресурсів, програмних засобів обробки (передачі) і захисту інформації;
- реєстрація дій користувачів Системи і обслуговуючого персоналу, контроль за діями користувачів, обслуговуючого персоналу і сторонніх осіб;
- облік і надійне зберігання машинних носіїв інформації, ключів (ключової документації) і їх обіг, що виключає їх розкрадання, підміну і знищення;

- необхідне резервування технічних засобів і дублювання масивів і носіїв інформації;
- використання сертифікованих технічних засобів, що серійно випускаються в захищеному виконанні для обробки, передачі і зберігання інформації;
- використання технічних засобів, які відповідають вимогам стандартів з електромагнітної сумісності;
- використання сертифікованих засобів захисту інформації;
- розв'язка ланцюгів електроживлення об'єктів захисту за допомогою захисних фільтрів, які блокують (пригнічують) інформативний сигнал;
- використання захищених каналів зв'язку і криптографічних засобів захисту інформації;
- розміщення дисплеїв і інших засобів відображення інформації, що виключає несанкціонований перегляд інформації;
- організація фізичного захисту приміщень та власне технічних засобів за допомогою сил охорони і технічних засобів, що запобігають або істотно ускладнюють проникнення в приміщення сторонніх осіб, розкрадання документів і інформаційних носіїв, самих засобів інформатизації, що виключають знаходження всередині контрольованої зони технічних засобів розвідки або промислового шпигунства;
- криптографічне перетворення інформації, що обробляється і передається засобами обчислювальної техніки і зв'язку;
- запобігання впровадження в Систему програм-вірусів і програмних закладок.

Особи, допущені до автоматизованої обробки конфіденційної інформації, несуть відповідальність за дотримання встановленого в установі (на підприємстві) порядку забезпечення захисту цієї інформації.

2.1.10 Вимоги до схоронності інформації при аваріях

Тимчасова відмова технічних засобів або втрата електроживлення не повинні призводити до знищення або втрати накопиченої інформації.

2.1.11 Вимоги до захисту від впливу зовнішніх чинників

У серверній кімнаті не повинні бути розміщені трубопроводи і дренажна система, якщо вони не призначені для роботи обладнання і спеціальних систем, розміщених в серверному приміщенні.

Якщо існує ймовірність протікання води в серверне приміщення, то рекомендується встановити дренаж.

Якщо в серверному приміщенні встановлюються сплінкери, то під трубопроводами, придатними до сплінкерів, рекомендується встановити дренажні канали, щоб захистити обладнання від можливої протікання.

У серверних приміщеннях не має бути вікон.

Стіни, стеля та підлога повинні мати покриття, яке ускладнює виділення, осідання і накопичення пилу на поверхні.

Стеля повинен мати гідроізоляцію, щоб виключити протікання води.

Стіни повинні бути пофарбовані світлою фарбою.

Система контролю і керування мікрокліматом повинна забезпечити в серверному приміщенні заданий рівень вологості і температури необхідний для нормального функціонування активного обладнання.

Система мікроклімату повинна забезпечити підтримку температурного режиму не тільки влітку, а й взимку і розрахована на цілодобову безперервну роботу.

Якщо централізована система мікроклімату в будівлі не може забезпечити безперервну роботу і заданий рівень температури і вологості, то необхідно встановити автономну систему в серверному приміщенні.

Рекомендована температура: 18-27°C; рекомендована відносна вологість: 40-55%.

При повітряному охолодженні вимір температури і вологості має здійснюватися при працюючому активному обладнанні на висоті 1.5 метра від рівня підлоги в зоні подачі холодного потоку повітря. При водяному охолодженні вимір температури і вологості має здійснюватися при працюючому активному обладнанні в монтажному конструктиві.

Потрібно забезпечити повітряний тиск в серверному приміщенні більше, ніж в прилеглих приміщеннях.

Рекомендується зміна повітря в серверному приміщенні не рідше 1 разу на годину, якщо в приміщенні постійно працює обслуговуючий персонал.

Рекомендується використовувати систему очищення і фільтрації повітря, що поступає в апаратне приміщення.

Якщо в будинку встановлена система резервного електроживлення, то система підтримки мікроклімату в серверному приміщенні повинні бути підключена до системи резервного електроживлення.

Серверні приміщення повинні бути захищене від пилу і шкідливих речовин, які можуть негативно впливати на роботу обладнання та на матеріали обладнання.

Концентрація шкідливої речовини в серверному приміщенні не повинна перевищувати гранично допустиму норму.

Вібрація негативно впливає на роботу активного обладнання, контакти і з'єднання. В діапазоні частот до 25 Гц амплітуда коливань не повинна перевищувати 0.1 мм.

Серверне приміщення потрібно розмістити в стороні від джерел електромагнітних завад на такій відстані, щоб напруженість електричного поля в серверному приміщенні не перевищувала 3В/м у всьому спектрі частот.

2.1.12 Вимоги до патентної чистоти

Розробляється Система не призначається на експорт, тому обмеження по патентної чистоті не накладаються. Однак Замовнику необхідно пам'ятати,

що в даний час авторські права фірм-виробників обладнання та розробників програмного забезпечення охороняються не тільки міжнародним, але й Українським законодавством, тому і обладнання, і програмне забезпечення Системи як цілком, так і в будь-якої її частини, може застосовуватися тільки для цільового використання, визначеного Договорами з Генпідрядником, Постачальником обладнання або Розробником Системи, і не може бути передано третій стороні без письмового дозволу Генпідрядника, Постачальника обладнання або Розробника програмного забезпечення.

2.1.13 Вимоги до стандартизації й уніфікації

Система, що розробляється повинна бути універсальною, забезпечувати можливість її використання та розширення за необхідності. Система має відповідати досягнутому світовому рівню в області створення комп'ютерних систем за функціональним розвитком, зручністю експлуатації та обслуговуванню.

2.1.14 Додаткові вимоги

Усі елементи Системи повинні мати захист не нижче IP30 для використання як у серверних приміщеннях так і у звичайних приміщеннях.

Активне обладнання має забезпечувати мережеве з'єднання станцій існуючих кінцевих споживачів та мати запас мінімум у 10% по портах.

Встановлення активного обладнання має бути у стійках якщо розміщено у серверній кімнаті або на стінах згідно запроектованого розміщення у кімнатах загального користування.

За технічними характеристиками обладнання має забезпечувати безперебійне з'єднання, потрібну пропускну спроможність та резерв по входах, згідно проектним розрахункам.

Кабель-канали мають бути закритого типу. Місця встановлення та розміри кабель-каналів мають відповідати проектним розрахункам та показанням.

Кількість та розміщення інформаційних розеток має відповідати розрахованій кількості у проекті та мати запас у 10% для можливості розширення.

Кількість та розміщення електричних розеток має забезпечувати індивідуальне підключення як мережевого обладнання так і робочих станцій або ін. Запас по кількості електричних розеток має складати 20%.

Комунікаційне обладнання, яке вже існує на підприємстві, має бути розташоване згідно з його паспортних характеристик, рекомендацій та призначення.

Для комунікаційного обладнання, яке розміщується у стійці має бути запропонована у проекті відповідна специфікація. Шафи-стійки мають відповідати сучасним вимогам до побудови аналогічних систем.

Сигнальні дроти мають підводитись у серверну кімнату та безпосередньо у шафи-стійки з-під фальш-підлоги. Для загальних кімнат сигнальні дроти мають розміщатися у коробах на стінах.

Міжкімнатні та міжповерхові кабельні траси можуть бути прокладені як у коробах так і у лотках у верхній частині стелі вздовж стелі.

Розташування обладнання в середині шафи має відповідати вимогам з ергономіки дійсних технічних вимог.

Тип кабелів має відповідати проектним розрахункам та може бути як мідна вита-пара з екранованою оболонкою так і оптоволокно.

Роз’єми для під’єднання мають відповідати запроектованим рішенням.

При проектуванні потрібно закласти можливість для розширення Системи.

Система має забезпечувати резервування даних, що мають стратегічне та економічне значення для підприємства на апаратному рівні.

2.2 Вимоги до функцій (задач), виконуваних Системою

Система має складатися з п’яти сегментів LAN1-LAN5.

Кількість вузлів для кожного сегменту має складати 45, 40, 65, 20, 140 одиниць відповідно.

Блок адрес для виділення підмереж має бути: 172.16.IPn.0/22, де IPn=68.

Врахувати, що інтенсивність трафіку μ=208 кадрів/с.

Виходячи з вищеописаних вимог має бути розроблена адресація для вузлів корпоративної мережі.

Під час розрахунку необхідно:

− застосовувати блок адрес версії IPv4;

− для каналів між маршрутизаторами застосувати блок адрес 10.0.№.0/24, де № =9;

− врахувати кількість вузлів в підмережах;

− перші можливі для використання IP-адреси призначати інтерфейсам і підінтерфейсам маршрутизаторів у LAN;

− другі з можливих IP-адрес призначати комутаторам у LAN;

− серверам привласнити IP-адреса за правилом: IP-адрес дорівнює першому можливому адресу у мережі+9+№, де № =9;

− останні з використовуваних IP-адрес призначати вузлам;

− в мережах VLAN використовувати адресацію кінцевих пристроїв за протоколом DHCP.

Повинно бути виконано базове налаштування конфігурації пристроїв, а саме:

− назначити назви пристроям за наступним правилом: Minenko_тип пристрою_номер пристрою;

− на всіх пристроях назначити пароль cisco до консолі і vty;

− на всіх пристроях назначити пароль class до привілейованого режиму;

− усі паролі, що зберігаються у відкритому вигляді, пропонується під час налаштування моделі комп’ютерної системи зашифрувати;

− розробити банер MOTD;

− назначити на усіх лініях vty використання протоколу ssh;

− призначити на всіх пристроях користувача за правилом: 12317sk_Minenko, з паролем admincisco;

− в якості імені домена використати ім'я пристрою. Для шифрування даних створювати ключ RSA завдовжки 1024 біт;

− на DCE-інтерфейсах маршрутизаторів призначити встановлення значення тактової частоти – 128000.

− налаштувати аудит і відправку повідомлень про початок і завершення процесу exec, з використанням локальної бази.

ACL має забороняти протоколи ICMP і Telnet, але має дозволяти усі інші види трафіку між VLAN10 і LAN2.

В мережі LAN2 тільки сервер DNS має мати вихід в інтернет.

Тільки мережа LAN5 має мати доступ до LAN3.

2.3 Вимоги до видів забезпечення

2.3.1 Вимоги інформаційного забезпечення Системи

Інформаційне забезпечення мережі має являти собою єдиний інформаційний фонд, орієнтований на завдання, які вирішуються в мережі, і містить масиви даних загального використання, доступні всім абонентам мережі, і масиви індивідуального використання, доступні окремим абонентам. До складу інформаційного забезпечення входять бази даних і знань, локальні, що зберігаються на сервері або на одному комп'ютері, і розподілені, що зберігаються на декількох серверах або комп'ютерах, індивідуального та колективного використання.

Для роботи з мережевими базами даних мають застосовуватися звичайні СУБД і мережеві СУРБД на платформі SQL або споріднених баз.

2.3.2 Вимоги до програмного забезпечення Системи

Програмне забезпечення Системи має складатися з загального, системного та спеціального.

Загальне програмне забезпечення має встановлюватися на робочих станціях кінцевих користувачів для забезпечення продуктивної праці.

Системне програмне забезпечення встановлюється як на станціях користувачів за для можливості діагностування так і на серверних станціях. У якості ОС кінцевих користувачів бажано використовувати windows10. У якості ОС серверних станцій – windows server або ОС Linux.

У якості спеціального ПЗ є спеціалізоване програмне забезпечення, для мережевого обладнання, яке йде у комплекті.

3 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ

3.1 Обстеження об’єкту розробки з метою аналізу всіх способів внутрішнього і зовнішнього доступу до інфраструктури мережі

Розглянемо схему будівлі для розміщення проектного бюро.

Будівля триповерхова та має план, як зазначено на рисунку 3.1. План розміщення кімнат однаковий для кожного з поверхів.

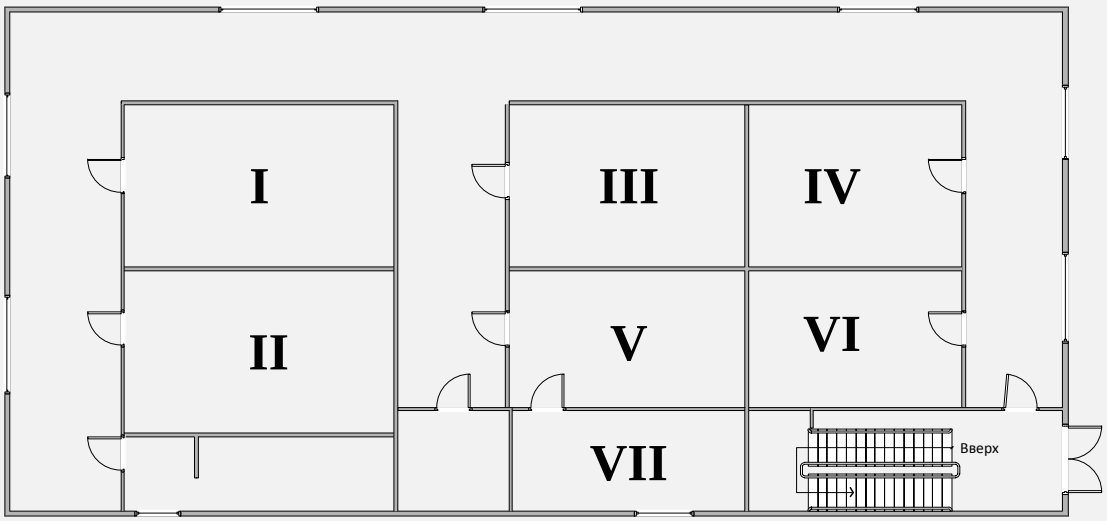

Рисунок 3.1 – План поверхів для будівлі проектного бюро

Виходячи з розміщення персоналу по кімнатах будівлі потребується організація 8 робочих місць у кімнатах III-IV на першому поверсі; 8 і 16 робочих місць у кімнатах I-II та III-VI відповідно на другому поверсі; 8 робочих місць у кімнатах I-II на третьому поверсі.

Для цього доцільно встановити по одному комутатору на першому та третьому поверхах та два комутаторі на второчу поверсі.

Згідно з огляду існуючої топології мережі підприємства та Технічними вимогами, що до проектування, з урахуванням створення нової підмережі у складі мережі підприємства загальна архітектура виглядає, як зображено на рисунку 3.2.

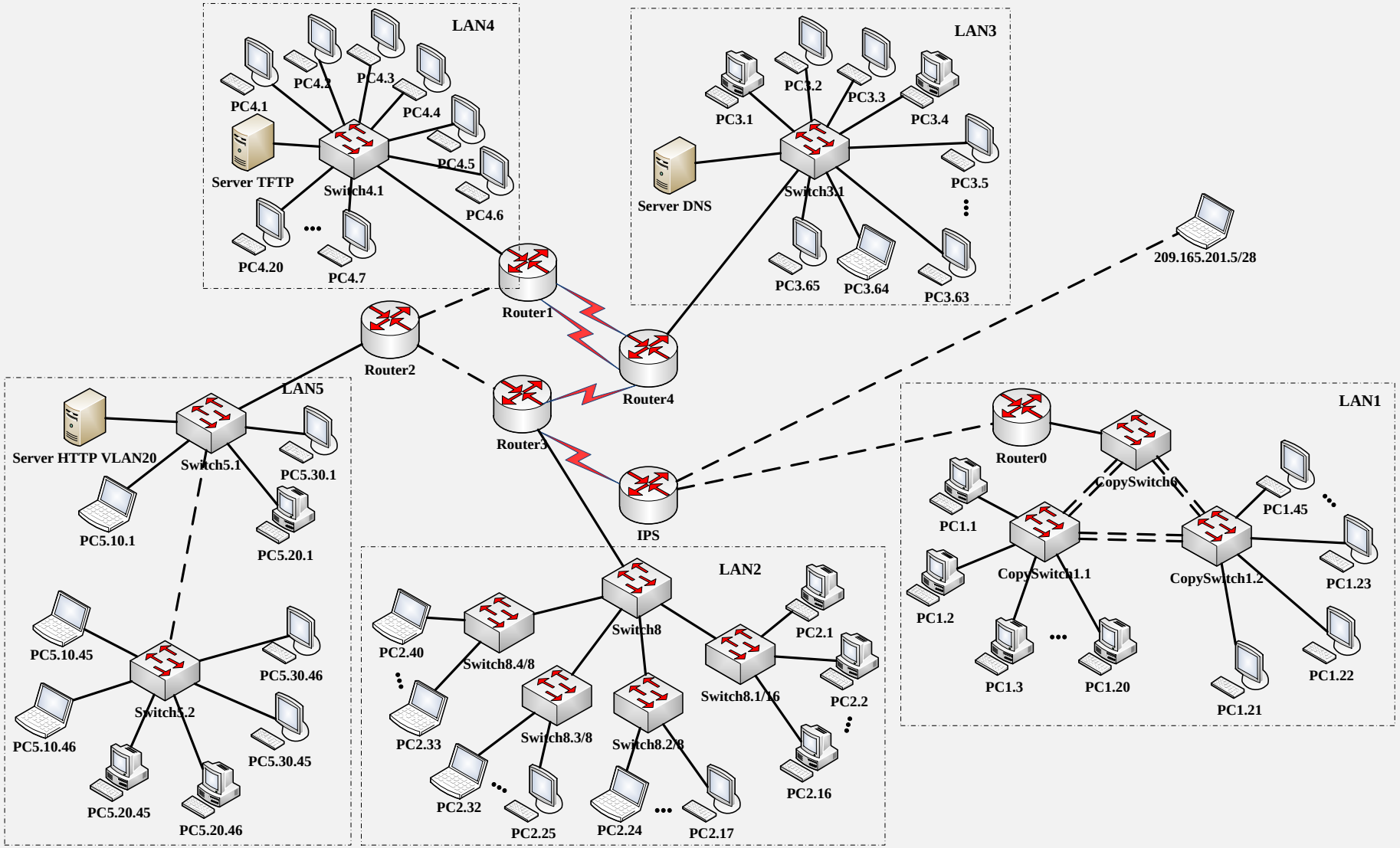

Рисунок 3.2 – Загальна архітектура мережі підприємства

3.2 Вибір і обґрунтування структурної схеми комплексу технічних засобів комп’ютерної системи

Корпоративна мережа підприємства є взаємопов'язаною структурою, що складається з робочих станцій, серверного обладнання, загальних ресурсів, маршрутизаторів і мережевих комунікацій для фізичної передачі інформаційних пакетів. Головною функцією корпоративної мережі є забезпечення безперебійного доступу до мережі інтернет, а також взаємопов'язана робота всіх співробітників компанії разом з керівництвом.

Побудова комп’ютерної мережі виконується згідно з технічними вимог на КС підприємства.

Комп’ютерна система правління підприємства ПГОК дозволяє створити єдину для всіх підрозділів базу даних, вести електронний документообіг, організувати селекторні наради і проводити відеоконференції доступі в Інтернет і інші інтерактивні мережі. Все це зменшує час реакції на зміни, що відбуваються в компанії, і забезпечує оптимальне управління всіма процесами в реальному масштабі часу.

На рисунку 3.3 представлена структурна схема комплексу технічних засобів комп’ютерної системи правління підприємства ПГОК.

На структурній схемі наведено такі основні пристрої:

- маршрутизатор. Мережний пристрій, на підставі інформації про топологію мережі і певних правил приймає рішення про пересилку пакетів мережевого рівня між різними сегментами мережі;
- комутатор рівня доступу. Пристрій, призначений для з'єднання декількох вузлів комп'ютерної мережі в межах одного або декількох сегментів мережі. Комутатор передає дані лише безпосередньо отримувачу. Це підвищує продуктивність і безпеку мережі, позбавляючи інші сегменти мережі від необхідності (і можливості) обробляти дані, які їм не призначалися;

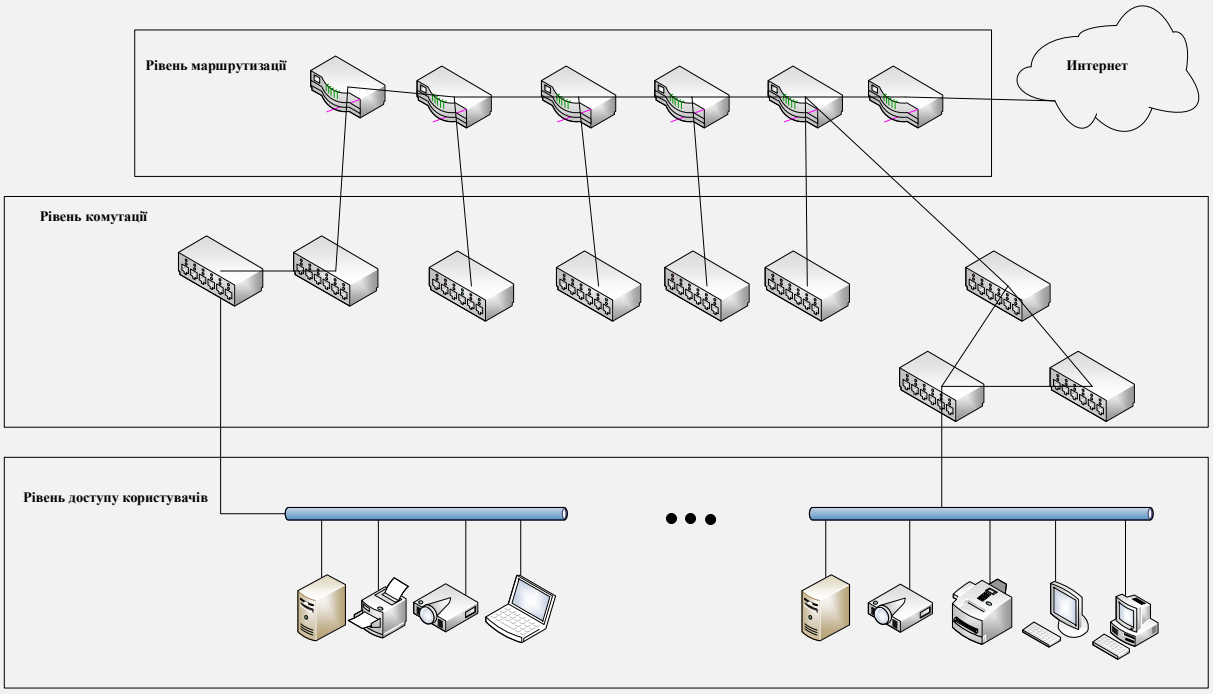

Рисунок 3.1 – Структурна схеми комплексу технічних засобів комп’ютерної системи правління підприємства ПГОК

− комп'ютер або інший мережевий пристрій кінцевого користування. Найчастіше підключений до локальної мережі через кабель типу UTP, FTP. На комп'ютері встановлено ПО необхідне для роботи персоналу (офісні додатки, 1С, поштові агенти та т.п.), а також засоби для віддаленого адміністрування;

− файловий сервер TFTP. Це виділений сервер, оптимізований для виконання файлових операцій введення-виведення. Призначений для зберігання файлів будь-якого типу. Має великий обсяг дискового простору, і, як правило, файл-сервер обладнаний RAID контролером для забезпечення швидкого запису і читання даних;

− web-сервер HTTP. Це сервер, який приймає HTTP-запити від клієнтів, зазвичай веб-браузерів, і видає їм HTTP-відповіді, зазвичай разом з HTML-сторінкою, зображенням, файлом, медіа-потоком або іншими даними. На ньому розташований корпоративний сайт та інші веб-сервіс;

− сервер DNS. DNS-сервер – хост, на якому запущено відповідний сервіс. Сервіс DNS-сервера відповідає за перетворення доменних адрес в IP-

адреси. Якщо домен з якоїсь причини не перетворився в IP-адресу, то сайт не відчиняться в браузері.

В КС правління підприємства ПГОК використовується 9 комутаторів. Комутатори рівня доступу підключається до маршрутизаторів ядра мережі.

Враховуючи невеликий розмір мережі, рівень ядра і розподілу будуть поєднуватися в маршрутизаторах КС підприємства ПГОК. Через прикордонний маршрутизатор ядра виконується підключення проектованої мережі до Інтернет.

3.3 Розробка специфікації апаратних засобів комп'ютерної системи

Грунтуючись на розробленій структурній схемі комплексу технічних засобів комп'ютерної системи розробляємо специфікацію, як для існуючих апаратних засобів, так і для тих що вносяться до Системи вперше.

Загальна специфікація обладнання наведена у таблиці 3.1.

Таблиця 3.1 – Загальна специфікація обладнання

Позиція	Найменування і технічна характеристика	Тип, марка, позначення документа, опитувального листа	Одиниці виміру	Кількість	Примітки
1	2	3	4	5	6
1.	Маршрутизатор. 2 порти Fast Ethernet; 4 модульних порту HWIC; 2 роз'єми: Advanced Integration Module; брандмауер Cisco IOS; система запобігання вторгнень NAC; IPSec VPN, до 1500 тунелів; Advanced QoS; 802.1Q, 802.1X; 2 слота PVDM; опціонально: Call Manager Express, SRST, голосова почтаPoE; 1 порт NME	Cisco 2811	од.	6	існуючий

Продовження таблиці 3.1

2.	Комутатор. Рівень: 2+; Порти доступу Ethernet: 24 x FE RJ-45; Порти агрегації Ethernet: 2 x GE RJ-45; Матриця комутації: 16 Гбіт/с; Таблиця MAC адрес: 8000 MAC адрес; Число активних VLAN: 255 VLAN; Комутація Мпакетов/с (MPPS): 6,5 MPPS; Максимальний VLAN ID: 4096; Порти живлення PoE: немає; Порти консольні: RJ-45 (RS232); Тип Cisco IOS: LAN Base; Споживана потужність номінальна/максиальна: 20/30 Ватт; Память FLASH: 64 Мб Робота у кластері: до 16 комутаторів на кластер; Протоколи VLAN: 802.1Q/Private VLAN(Edge)/ Voice VLAN/VTP/URT/VMPS Тип живлення: AC 220B	Cisco Catalyst 2948-24TT	од.	5	Існуючий LAN5, LAN1
3.	Комутатор. Характеристики див. п.2	Cisco Catalyst 2948-24TT	од.	3	За проектом LAN4, LAN3, LAN2

Продовження таблиці 3.1

4.	Комутатор. 9 x Fast Ethernet (10/100 Мбит/с) Підтримка PoE: присутня; Можливість віддаленого керування: некерований	FoxGate S6009 (DS157558)	од.	3	За проектом LAN2
5.	Комутатор. Порти 16 x Fast Ethernet (10/100 Мбіт/с) 2 x combo10/100/1000BASE-T/SFP; Підтримка PoE: присутня; Можливість віддаленого керування: некерований	D-Link DES-1018P	од.	1	За проектом LAN2
6.	Робоча станція. Моноблок ASUS Vivo AiO V222UA 21.5" ; 1920 x 1080; Vivo AiO; Intel Celeron 3867U (1.8 ГГц) / 2 – ядра; 4 ГБ ОЗУ; video Intel UHD Graphics 610; 256 ГБ SSD; 4 x USB 3.1 Type-A, USB 2.0; Wi-Fi 802.11ac; Bluetooth 4.1; 1 x HDMI, 1 x Audio; camera 1 МП; Endless OS	ASUS Vivo AiO V222UA	од.	40	За проектом LAN2
7.	Кабель канал пластиковий 40х60	«Імпакт»	м	738	За проектом LAN2
8.	Кабель канал пластиковий 20х40	«Імпакт»	м	228	За проектом LAN2
9.	Розетка мережева 1порт экранована RJ45 STP біла 5E	EServer™ RJ45 STP	од.	44	За проектом LAN2
10.	Розетка живлення наружна, Forix 2+2К+3 без шторок, IP44	Legrand Forix	од.	24	За проектом LAN2

Продовження таблиці 3.1

11.	Кабель F/UTP кручена пара cat-5e для внутрішньої прокладки PBX, V.11, X.21, ISDN, Ethernet (10Base-T), ATM-25/52/155 Мбіт/с, 100VG-AnyLAN, Fast Ethernet (100BASE-TX), Token Ring 16/100 Мбіт/с , Gigabit Ethernet (1000BASE-T), Firewire 100 Мбіт/с.	Vago КГПВЕ-ВП (100) 4*2* 0,51 (F/UTP-cat.5E patch 20)	м	966	За проектом LAN2

3.4 Розрахунок інтенсивності вихідного трафіку найбільшої локальної мережі підприємства

Лінія вихідного каналу має пропускну здатність 1000Мбіт/с.

Для того, не було перенасичення каналу, швидкість надходження пакетів не повинна перевищувати швидкості їх відправлення. Вважаємо, що послугами одночасно користуються 100% користувачів. Середня інтенсивність трафіку μ=208 (кадрів/с), а середня довжина повідомлення – 650 байт.

Розрахуємо пропускну здатність мережі адміністративної будівлі допускаючи, що послугами одночасно користуються 100% користувачів. Пропускна здатність мережі розраховується наступним чином. Так як в нас 2 комутатори рівня доступу, а загальна кількість користувачів дорівнює 310, то пропускна здатність мережі на рівні доступу буде дорівнює:

Рр.р= μ*l*N*8=208*650*310*8= 335,3 (Мбіт/с), де

N – кількість вузлів в мережі.

Отримані при розрахунку результати не перевищують задані параметри мережі. Отже, перевантажень на обраному обладнанні не буде.

Комутатор рівня доступу пересилає трафік на маршрутизатор через вихідну лінію з пропускною здатністю 1000Мбіт/с.

Загальне навантаження на комутатор не повинно перевищувати:

$\mu_{вих}$=1000 000 000/(650*8)=192308 пакетів/с

Оскільки кожне джерело виробляє в середньому 208 пакетів/с, то ми обмежені приєднанням до комутатора рівня доступу максимум:

N=192308 /208=925 джерел.

Що задовольняє нашу мережу на 310 ПК.

Кожен з 310 ПК посилає потік заявок з інтенсивністю 208 кадрів/с. Інтенсивність вихідного трафіку від всіх користувачів:

λ=N*μ= 310*208 = 64480 (пакетів/с)

Коефіцієнт затримки на рівні розподілу, тобто показник завантаженості вихідного каналу зв'язку, який впливає на час стояння в черзі:

$\rho = \lambda / \mu_{вих}$=64480/192308 =0,34 (3.1)

Коефіцієнт зайнятості комутатора рівня розподілу:

$r= \rho/(1- \rho)=0,34/(1-0,34)=0,52$ (3.1)

Середня затримка кадру, пов'язана з чергою M/M/1, дорівнює:

$T=1/(\mu – \lambda)=1/(192308 – 64480) =7,82*10^{-6}$с (3.2)

Середня довжина черги:

$\zeta_{чер}= \rho^2/(1- \rho)=0,34^2/(1-0,34)=0,175$ (3.3)

Ця цифра може бути корисною при налаштуванні черг на обладнанні – в апаратурі можна вказувати максимальний розмір черги пакетів. В даному випадку в системі на обслуговуванні менше 1 пакету, значення досить умовне; воно свідчить про те, що система працює з дуже великим запасом по продуктивності.

Середній час перебування пакета в черзі:

$T_{оч}= \zeta_{чер/} \lambda=0,175/64480=2,71$мкс (3.5)

Це значення менше необхідного значення 6 мс, що задовольняє вимогам.

Пропускна здатність каналу:

$$\lambda = \frac{\text{пропускна здатність}}{\text{довжина кадру}} = \frac{b}{l}$$

$b=\lambda* l =64480*650*8= 335296000$ біт/с = 335,3 Мбіт/с

Що задовольняє пропускній здатності вихідного каналу в 1000Мбіт/с.

4 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ТА ПЕРЕВІРКА РОБОТИ КОМП'ЮТЕРНОЇ СИСТЕМИ ПІДПРИЄМСТВА

4.1 Розрахунок схеми адресації корпоративної мережі

Для побудови мережі правління підприємства ПГОК, відповідно до технічних вимог, використаний адресний простір 172.16.68.0/22.

IP-адреса використовується на мережному рівні. Вона призначається адміністратором під час конфігурування комп'ютерів і маршрутизаторів. IP-адреса складається з двох частин: номера мережі і номера вузла. Для проектування корпоративної мережі необхідно розробити адресацію з критеріями − найкраща суммарізація, мінімальна витрата адрес. Розрахунок IP-адрес підмереж будемо виконувати методом VLSM. Це дозволить використання більш ніж однієї мережевої маски в межах одного адресного простору. VLSM максимізує використання адресного простору і його використовують для сегментування локальних мереж. VLSM дає можливість більш ефективно використовувати IP-адреси, ніж звичайний поділ на підмережі з використанням класової адресації.

При використанні VLSM довжина маски підмережі залежить від числа бітів, запозичених для окремої підмережі від частини ідентифікатора хоста адреси для створення ID підмережі. Тобто від «змінної» частини маски підмережі змінної довжини. VLSM дозволяє розділити простір мережі на нерівні частини.

Розподіляти IP-адреси необхідно згідно до вимог, вказаних в таблиці 4.1.

Таблиця 4.1 – Кількість вузлів в підмережах

172.16.68.0/22				
LAN1 Будівля 2	LAN2 Будівля 4	LAN3 Будівля 3	LAN4 Будівля 6	LAN5 Будівля 1
45	40	65	20	140

З рисунка 3.2 видно, що топологія об'єднує 5 підмереж з хост-вузлами, мережними принтерами та серверами, 5 мережі маршрутизаторів з адресами мереж з адресного простору 10.0.9.0/24, одна мережа зовнішнього шлюзу з адресою мережі

209.165.202.0/27, одна мережа для підключення віддаленої мережі 64.100.13.0/30 . Мережі маршрутизаторів та зовнішнього шлюзу потребують по 2 IP-адреси кожна.

Для поділу вихідної мережі необхідно визначити кількість біт, необхідних для визначення п’яти підмереж. Таким чином, необхідно виділити 3 біти (2^3=9).

Далі необхідно упорядкувати мережі за кількістю необхідних IP-адрес. Спочатку виділяються біти під адресацію найбільшої мережі (LAN5 включає 140 вузлів), і далі до найменшої мережі. Для LAN5 необхідно 8 біт для IP-адресації кінцевих пристроїв (2^8 -2=254).

Таким чином, розрахунок IP-адрес методом VLSM для мережі LAN5 має вигляд:

172.16.0100 00|10. |0000 0000

Символами «| |» виділена частина IP-адреси, що визначає під мережу вихідної мережі 172.16.68.0/22. Маска підмережі – 24 одиниць (255.255.255.0). Адреса підмережі – 172.16.28.0/24. Перша допустима адреса підмережі визначається як значення 1 в молодшому біті IP-адреси у вузловій частині – 172.16.0100 0010. |0000 0001| (172.16.68.1). Остання допустима адреса визначається як значення одиниць в усіх розрядах вузлової частини, окрім молодшого – 172.16.0100 0010. |1111 1110| (172.16.68.254).

Розрахунок IP-адрес методом VLSM для підмережі LAN3:

Необхідний розмір під мережі: 65.

Виділений розмір підмережі: 126 (N = 2^7 – 2 = 126).

Адреса підмережі – 172.16.69.0/25

172.16. 0100 0011. |0|000 0000

255.255.1111 1111.1000 0000

Десятковий формат адреси підмережі для визначеної маски: 255.255.255.128. Префікс: /25

Діапазон допустимих IP-адрес вузлів:

172.16. 0100 0011. 1|0000001 – 172.16. 0100 0011. 1|1111110

172.16.69.1 – 172.16.69.126

Подальші розрахунки виконуються аналогічно.

В таблиці 4.2 представлена схема IP-адресації мережі правління підприємства ПГОК, розрахована за методом VLSM.

Таблиця 4.2 – Схема адресації мережі

Назва підмережі	Розмір	Адреса	Десяткова маска	Діапазон доступних адрес
LAN5	140	172.16.68.0	255.255.255.0	172.16.68.1 - 172.16.68.254
LAN3	65	172.16.69.0	255.255.255.128	172.16.69.1 - 172.16.69.126
LAN1	45	172.16.69.128	255.255.255.192	172.16.69.129 - 172.16.69.190
LAN2	40	172.16.69.192	255.255.255.192	172.16.69.193 - 172.16.69.254
LAN5	20	172.16.70.0	255.255.255.224	172.16.70.1 - 172.16.70.30
VLAN19	30	172.16.68.0	255.255.255.224	172.16.68.1 - 172.16.68.30
VLAN29	30	172.16.68.32	255.255.255.224	172.16.68.33 - 172.16.68.62
VLAN39	30	172.16.68.64	255.255.255.224	172.16.68.65 - 172.16.68.94
VLAN99	30	172.16.68.96	255.255.255.224	172.16.68.97 - 172.16.68.126
WAN1	2	10.0.9.0	255.255.255.252	10.0.9.1 - 10.0.9.2
WAN2	2	10.0.9.4	255.255.255.252	10.0.4.5 - 10.0.9.6
WAN3	2	10.0.9.8	255.255.255.252	10.0.9.9 - 10.0.9.10
WAN4	2	10.0.9.12	255.255.255.252	10.0.9.13 - 10.0.9.14
WAN5	2	10.0.9.16	255.255.255.252	10.0.9.17 - 10.0.9.18
WAN IPS	2	209.165. 202.0	255.255.255.224	209.165.202.1- 209.165.202.2
WAN Remote Network	2	64.100.13.0	255.255.255.252	64.100.13.1- 64.100.13.2

Відповідно до вихідного блока IP-адрес, доступно адрес – 1022. Відповідно до необхідної кількості ПК, що потребують об’єднання в мережу, кількість необхідних IP-адрес – 310. Близько 56% доступного адресного простору вихідної мережі використано, таким чином, за методом VLSM, виконана вимога до мінімальної витрати адрес.

Згідно технічних вимог проектування правління підприємства ПГОК, необхідно скласти таблицю адресації мережевих пристроїв. При цьому:

- перші можливі для використання IP-адреси призначено інтерфейсам і підінтерфейсам маршрутизаторів у LAN;
- другі з можливих IP-адрес призначаються комутаторам у кожній LAN;
- сервери налаштовано і їм привласнено IP-адреси за правилом: IP-адрес дорівнює першому можливому адресу у мережі+4+9;
- останні з використовуваних IP-адрес призначено вузлам;
- в мережах VLAN використовується адресація кінцевих пристроїв по протоколу DHCP.

У таблиці 4.3 представлена адресація всіх пристроїв мережі правління підприємства ПГОК. Таблиця заповнюється на основі даних таблиці 4.2 та логічної топології корпоративної мережі правління підприємства ПГОК.

Таблиця 4.3 – Схема адресації пристроїв мережі

Ім'я пристрою	Інтер-фейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
Будівля 4						
Minenko_R1	G0/1	172.16.69.193	/26	-	-	G0/1
	S0/1/0	10.0.9.13	/30	-	-	S0/1/0
	S0/1/1	10.0.9.9	/30	-	-	S0/0/1
	G0/0	10.0.9.1	/30	-	-	G0/0
Minenko_Sw4	Vlan1	172.16.69.194	/26	172.16.69.193	-	G0/1
PC1_B4-PC8_B4	NIC	172.16.69.254-172.16.69.248	/26	172.16.69.193	-	Fa0/1- Fa0/8
Printer1_B4	NIC	172.16.69.200	/26	172.16.69.193	-	Fa0/22
Printer2_B4	NIC	172.16.69.201	/26	172.16.69.193	-	Fa0/23
Server_TFTP	NIC	172.16.69.213	/26	172.16.69.193	-	Fa0/24

Продовження таблиці 4.3

Будівля 2						
Minenko_R4	G0/1	172.16.69.129	/26	-	-	G0/1
	S0/1/0	10.0.9.14	/30	-	-	S0/1/0
	S0/1/1	10.0.9.10	/30	-	-	S0/1/1
	S0/0/1	10.0.9.18	/30	-	-	S0/0/1
Minenko_Sw3	Vlan1	172.16.69.130	/26	172.16.69.129	-	G0/1
PC1_B2-PC8_B2	NIC	172.16.69.192-172.16.69.184	/26	172.16.69.129	-	F0/0-F0/7
ServerDNS	NIC	172.16.69.139	/26	172.16.69.129	-	Fa0/24
Будівля 6						
Minenko_R0	G0/1	172.16.70.1	/27	-	-	G0/1
	G0/2	64.100.13.2	/30	-	-	G0/2
Minenko_Sw2.1	Vlan1	172.16.70.2	/27	172.16.70.1	-	G0/1
Minenko_Sw2.2	Vlan1	172.16.70.3	/27	172.16.70.1	-	G0/1
Minenko_Sw2.3	Vlan1	172.16.70.4	/27	172.16.70.1	-	G0/1
PC1_B6-PC8_B6	NIC	172.16.70.30-172.16.70.28	/27	172.16.70.1	-	Fa0/1- Fa0/8
Будівля 3						
Minenko_R3	G0/1	172.16.69.1	/25	-	-	G0/1
	G0/2	10.0.9.6	/30	-	-	G0/2
	S0/0/0	209.165.202.2	/27	-	-	S0/0/0
	S0/0/1	10.0.9.17	/30	-	-	S0/0/1
Minenko_Sw2	Vlan1	172.16.69.2	/25	172.16.69.1	-	G0/1
PC_UP1-PC_UP8		172.16.69.126-172.16.69.118	/25	172.16.69.1	-	Fa0/1- Fa0/8
ServerTFTP	NIC	172.16.69.10	/25	172.16.69.1	-	Fa0/24
Будівля 1						
Minenko_R2	G0/1	-	-	-	-	-
	G0/1.19	172.16.68.33	/27	-	19	G0/1
	G0/1.29	172.16.68.65	/27	-	29	G0/1
	G0/1.39	172.16.68.97	/27	-	39	G0/1
	G0/0.99	172.16.68.1	/27	-	99	G0/1
PC19.1-PC19.3	NIC	172.16.68.62-172.16.68.60	/27	172.16.68.33	19	Fa0/4-8
PC29.1-PC29.3	NIC	172.16.68.94-172.16.68.91	/27	172.16.28.65	29	Fa0/10-14
ServerHTTP	NIC	172.16.68.75	/27	172.16.68.65	-	Fa0/14
PC39.1-PC39.3	NIC	172.16.68.126-172.16.68.123	/27	172.16.68.97	39	Fa0/15-20
Minenko_Sw1.1	G0/1	172.16.68.2	/27	172.16.68.1	99	-
Minenko_Sw1.2	F0/1	172.16.68.3	/27	172.16.68.1	99	-

Продовження таблиці 4.3

IPS						
Rout_IPS	S0/0/0	209.165.202.1	/27	-	-	S0/0/0
	G0/2	64.100.13.1	/30	-	-	G0/2
Host_ IPS	NIC	209.165.200.5	/25	209.165.200.5	-	G0/0

4.2 Розробка фізичної топологічної схеми корпоративної мережі

Фізична топологія мережі показує, як розташоване обладнання мережі на об’єкті впровадження, розташування та тип кабелів, місце встановлення та тип обладнання, підключення живлення до обладнання мережі, довжину кабельних трас, карту підключень.

Як базова технологія мережі обрана технологія Ethernet. Дана технологія здатна забезпечити найбільшу швидкість, надійність і якість передачі даних та найбільш розповсюджена. На рівні доступу для під’єднання робочих груп застосовано технологію Fast Ethernet. Між маршрутизатором і комутатором – GigabitEthernet.

Кабельна інфраструктура повинна відповідати стандартам TIA/EIA-568-A та TIA/EIA-569. Кабельна розводка всередині будівлі проектного бюро виконується кабелем типу «неекранована кручена пара» (UTP-кабель категорії 5e), що забезпечує високу надійність і швидкість передачі даних в поєднанні з високою технологічністю.

Підмережі КС розбиті на підмережі. Максимальний сегмент кабелю в підмережі має довжину 170 м, що відповідає вимогам.

Підмережі, що оснащуються мережним обладнанням, розташовані на першому та другому поверхах будівлі.

Виходячи з даних про обстеження об`єкту у кімнатах будівлі потребується організація 8 робочих місць у двох кімнатах на першому поверсі; 8 і 16 робочих місць у чотирьох кімнатах на другому поверсі; 8 робочих місць у двох кімнатах на третьому поверсі.

Для цього доцільно встановити по одному комутатору на першому та третьому поверхах та два комутаторі на второчу поверсі.

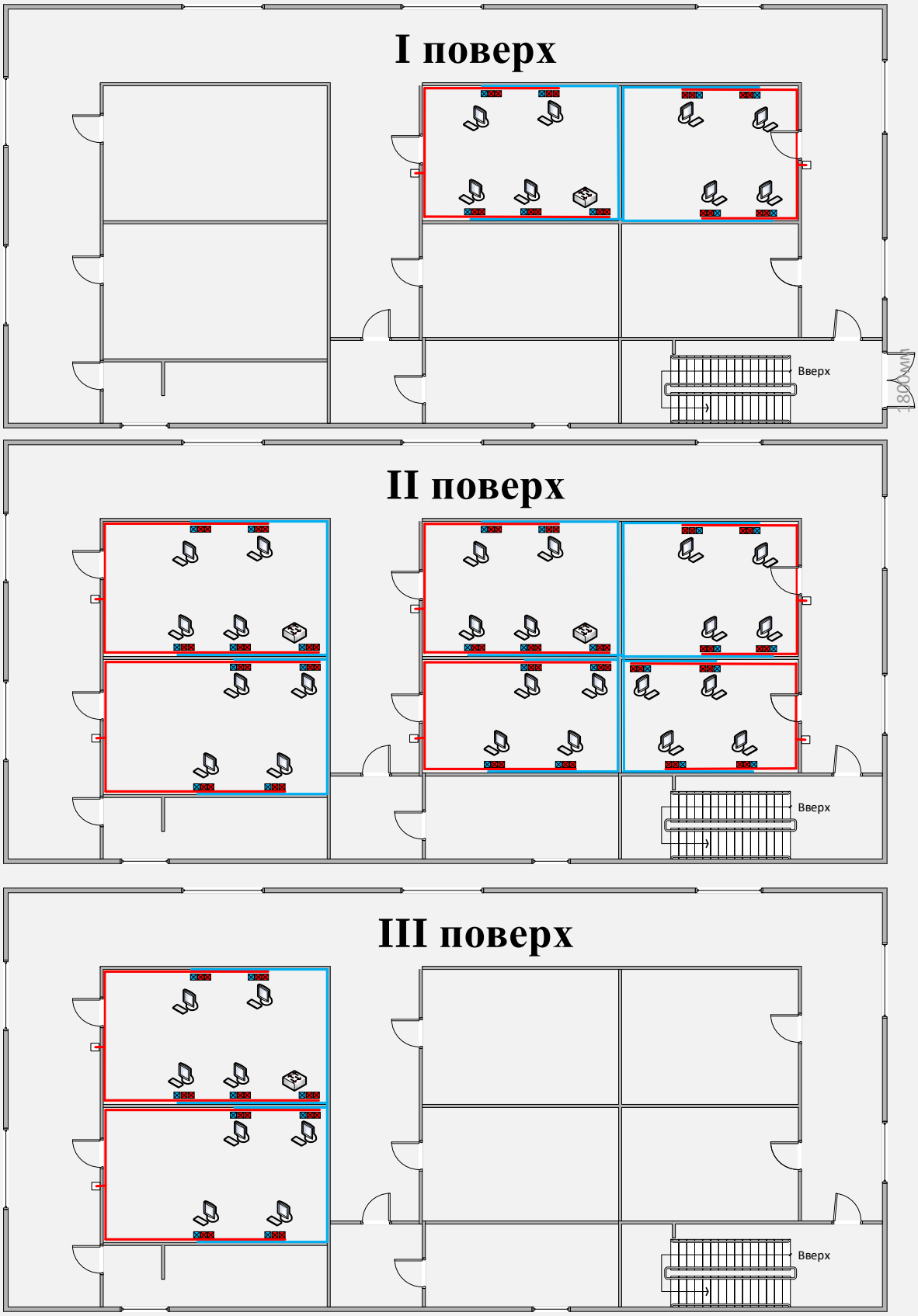

Рисунок 4.1 – Схема фізичної топології мережі будівлі проектного бюро

Загалом у даних підмережах встановлюється 40 точок підключення. Точка підключення являє собою двох портову інформаційну розетку RJ-45.

Для виконання з'єднання WAN між маршрутизаторами будівель необхідне застосування технології послідовної передачі даних Serial DCE/DTE. В мережі WAN використаний кабель Serial CAB-6060X DCE для інтерфейсів Serial.

Кабель прокладено за допомогою пластикових кабельних каналів, забезпечуючи точками підключення кожне приміщення.

4.3 Налаштування та перевірка роботи комп'ютерної системи

4.3.1 Базове налаштування конфігурації пристроїв

Згідно до технічних вимог було приведено базове налаштування активних мережних пристроїв комп'ютерної системи.

Розроблено базову конфігурацію пристроїв. При цьому додатково:

- застосувати паролі для привілейованого режиму, консолі і vty;
- зашифровано усі паролі, що зберігаються у відкритому вигляді;
- настроєно банер MOTD;
- настроєно на усіх лініях vty використання протоколу ssh і локальних облікових записів. Для цього створено користувача 12317sk_Minenko паролем admincisco. В якості імені домена використані назви пристроїв. Для шифрування даних створено ключ RSA завдовжки 1024 біт;
- налаштовано IPv4-адреси відповідно до таблиці 4.3;
- на DCE-інтерфейсах маршрутизаторів встановлено значення тактової частоти – 128000.

Приклад налаштування на Minenko _R1.

Заборонено пошук DNS (DNS lookup) на маршрутизаторах, щоб заборонити виконувати перетворення доменних імен у випадку помилкового введення в командний рядок не інтерпретованих слів замість коректних команд:

Router(config)#no ip domain-lookup

Задання пристрою унікального імені:

Router(config)#hostname Minenko _R1

Зашифровано всі паролі, що зберігаються у відкритому вигляді:

Minenko _R1(config)#service password-encryption

Встановлення паролю на віхд до привілейованого режиму:

Minenko _R1(config)#enable secret class

Встановлено парою на вхід до консольної лінії:

Minenko _R1(config)#line console 0

Minenko _R1(config-line)#password cisco

Налаштування запиту пароля при вході:

Minenko _R1(config-line)#login

Minenko _R1(config-line)#exit

Налаштування банера MOTD:

Minenko _R1(config)#banner motd # 123sk-16 Minenko This area have PASSword#

Налаштування протоколу SSH, Створення користувача 12317_Minenko з паролем admincisco:

Minenko _R1(config)#username 12317_Minenko password admincisco;

Створення домену:

Minenko _R1(config)#ip domain-name Minenko _R1

Для шифрування даних створено ключ RSA довжиною 1024 біт:

Minenko _R1(config)#crypto key generate rsa

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

Налаштування лінії VTY:

Minenko _R1(config)#line vty 0 4

Встановлення необхідності введення логіну та пароля для входу лінії:

Minenko _R1(config-line)#login local

Встановлення входу на лінію тільки по протоколу SSH:

Minenko _R1(config-line)#transport input ssh

Встановлення IPv4-адрес відповідно до таблиці 4.3:

Minenko _R1(config)#interface g0/1

Minenko _R1 (config-if)# ip address 172.16.69.193 255.255.255.192

Для запуску інтерфейсу до роботи слід його обов’язково увімкнути:

Minenko _R1(config-if)#no shutdown

4.3.2 Налаштування маршрутизаторів корпоративної мережі

Згідно технічних вимог, в мережі правління підприємства ПГОК використовується протокол динамічної маршрутизації OSPF 9. 9 – номер автономної системи, це сукупність мереж під єдиним адміністративним керуванням, що забезпечує загальну для всіх вхідних в автономну систему маршрутизаторів політику маршрутизації.

Протокол OSPF (Open Shortest Path First), описаний в стандарті RFC 2328. Протокол OSPF був розроблений, щоб задовольнити потребу інтернет-спільноти в функціональному, непропріетарном протоколі внутрішнього шлюзу (IGP) для сімейства протоколів TCP/IP. Протокол OSPF заснований на технології відстеження стану каналу.

OSPF має такі переваги:

– висока швидкість збіжності в порівнянні з дистанційно-векторними протоколами маршрутизації;
– підтримка мережевих масок змінної довжини (VLSM);
– оптимальне використання пропускної здатності з побудовою дерева найкоротших шляхів.

Для кожного маршрутизатора оголошені безпосередньо підключені мережі і відключено поширення оновлень маршрутизації на інтерфейси в локальні мережі. На Minenko _R1 налаштований маршрут за замовчуванням в інтернет (ISP) і поширене його через оновлення маршрутизації.

Включити протокол OSPF на маршрутизаторі командою:

Minenko _R1(config)#router ospf 9

Протоколу потрібно об’явити мережі, підключені до маршрутизатора.

Minenko _R1(config-router)#network 172.16.69.192 0.0.0.63 area 0

Minenko _R1(config-router)#network 10.0.9.0 0.0.0.3 area 0

Minenko _R1(config-router)#network 10.0.9.8 0.0.0.3 area 0

Minenko _R1(config-router)#network 10.0.9.0 0.0.0.3 area 0

Маршрут за замовчуванням на Minenko _R1:

ip route 0.0.0.0 0.0.0.0 209.165.202.1

На serial-інтерфейсах відповідно до технічних умов задано пропускну спроможність = 128 Кб/с та визначим швидкість каналу 128000, та вартість метрики = 7500.

Minenko _R1(config)#interface s0/1/0

Minenko _R1(config-if)#bandwidth 128

Minenko _R1(config-if)# clock rate 128000

Minenko _R1(config-if)# ip ospf cost 7500

Виконаємо перевірку таблиць маршрутизацій на маршрутизаторах (рисунок 4.2-4.6). Кожний маршрутизатор окрім безпосередньо підключених мереж з символом «С» має відомості про всі віддалені мережі, отримана по протоколу OSPF з символом «О». Також мають записи маршруту за замовчуванням, який складається з восьми нулів, для підключення до маршрутизатора IPS.

```
Minenko_R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C       10.0.9.0/30 is directly connected, GigabitEthernet0/0
L       10.0.9.1/32 is directly connected, GigabitEthernet0/0
O       10.0.9.4/30 [110/2] via 10.0.9.2, 01:17:08, GigabitEthernet0/0
C       10.0.9.8/30 is directly connected, Serial0/1/1
L       10.0.9.9/32 is directly connected, Serial0/1/1
C       10.0.9.12/30 is directly connected, Serial0/1/0
L       10.0.9.13/32 is directly connected, Serial0/1/0
O       10.0.9.16/30 [110/7502] via 10.0.9.2, 01:17:08, GigabitEthernet0/0
     172.16.0.0/16 is variably subnetted, 8 subnets, 4 masks
O       172.16.68.0/27 [110/2] via 10.0.9.2, 01:17:08, GigabitEthernet0/0
O       172.16.68.32/27 [110/2] via 10.0.9.2, 01:17:08, GigabitEthernet0/0
O       172.16.68.64/27 [110/2] via 10.0.9.2, 01:17:08, GigabitEthernet0/0
O       172.16.68.96/27 [110/2] via 10.0.9.2, 01:17:08, GigabitEthernet0/0
O       172.16.69.0/25 [110/3] via 10.0.9.2, 01:17:08, GigabitEthernet0/0
O       172.16.69.128/26 [110/7501] via 10.0.9.10, 01:17:38, Serial0/1/1
C       172.16.69.192/26 is directly connected, GigabitEthernet0/1
L       172.16.69.193/32 is directly connected, GigabitEthernet0/1
     209.165.202.0/27 is subnetted, 1 subnets
O       209.165.202.0/27 [110/7502] via 10.0.9.2, 01:17:08, GigabitEthernet0/0
S*   0.0.0.0/0 [1/0] via 209.165.202.1
```

Рисунок 4.2 – Таблиця маршрутизації на Minenko _R1

```
Minenko_R2#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C       10.0.9.0/30 is directly connected, GigabitEthernet0/0
L       10.0.9.2/32 is directly connected, GigabitEthernet0/0
C       10.0.9.4/30 is directly connected, GigabitEthernet0/2
L       10.0.9.5/32 is directly connected, GigabitEthernet0/2
O       10.0.9.8/30 [110/7501] via 10.0.9.1, 01:18:03, GigabitEthernet0/0
O       10.0.9.12/30 [110/7501] via 10.0.9.1, 01:18:03, GigabitEthernet0/0
O       10.0.9.16/30 [110/7501] via 10.0.9.6, 01:18:03, GigabitEthernet0/2
     172.16.0.0/16 is variably subnetted, 11 subnets, 4 masks
C       172.16.68.0/27 is directly connected, GigabitEthernet0/1.99
L       172.16.68.1/32 is directly connected, GigabitEthernet0/1.99
C       172.16.68.32/27 is directly connected, GigabitEthernet0/1.19
L       172.16.68.33/32 is directly connected, GigabitEthernet0/1.19
C       172.16.68.64/27 is directly connected, GigabitEthernet0/1.29
L       172.16.68.65/32 is directly connected, GigabitEthernet0/1.29
C       172.16.68.96/27 is directly connected, GigabitEthernet0/1.39
L       172.16.68.97/32 is directly connected, GigabitEthernet0/1.39
O       172.16.69.0/25 [110/2] via 10.0.9.6, 01:18:03, GigabitEthernet0/2
O       172.16.69.128/26 [110/7502] via 10.0.9.1, 01:18:03, GigabitEthernet0/0
                         [110/7502] via 10.0.9.6, 01:18:03, GigabitEthernet0/2
O       172.16.69.192/26 [110/2] via 10.0.9.1, 01:18:03, GigabitEthernet0/0
     209.165.202.0/27 is subnetted, 1 subnets
O       209.165.202.0/27 [110/7501] via 10.0.9.6, 01:18:03, GigabitEthernet0/2
S*   0.0.0.0/0 [1/0] via 209.165.202.1
```

Рисунок 4.3 – Таблиця маршрутизації на Minenko _R2

```
Minenko_R3#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
O       10.0.9.0/30 [110/2] via 10.0.9.5, 01:18:42, GigabitEthernet0/2
C       10.0.9.4/30 is directly connected, GigabitEthernet0/2
L       10.0.9.6/32 is directly connected, GigabitEthernet0/2
O       10.0.9.8/30 [110/7502] via 10.0.9.5, 01:18:42, GigabitEthernet0/2
O       10.0.9.12/30 [110/7502] via 10.0.9.5, 01:18:42, GigabitEthernet0/2
C       10.0.9.16/30 is directly connected, Serial0/0/1
L       10.0.9.17/32 is directly connected, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 9 subnets, 5 masks
S       172.16.68.0/22 is directly connected, GigabitEthernet0/1
O       172.16.68.0/27 [110/2] via 10.0.9.5, 01:18:42, GigabitEthernet0/2
O       172.16.68.32/27 [110/2] via 10.0.9.5, 01:18:42, GigabitEthernet0/2
O       172.16.68.64/27 [110/2] via 10.0.9.5, 01:18:42, GigabitEthernet0/2
O       172.16.68.96/27 [110/2] via 10.0.9.5, 01:18:42, GigabitEthernet0/2
C       172.16.69.0/25 is directly connected, GigabitEthernet0/1
L       172.16.69.1/32 is directly connected, GigabitEthernet0/1
O       172.16.69.128/26 [110/7501] via 10.0.9.18, 01:19:07, Serial0/0/1
O       172.16.69.192/26 [110/3] via 10.0.9.5, 01:18:42, GigabitEthernet0/2
     209.165.202.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.202.0/27 is directly connected, Serial0/0/0
L       209.165.202.2/32 is directly connected, Serial0/0/0
S*   0.0.0.0/0 [1/0] via 209.165.202.1
```

Рисунок 4.4 – Таблиця маршрутизації на Minenko _R3

```
Minenko_R4#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 209.165.202.1 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O       10.0.9.0/30 [110/7501] via 10.0.9.13, 01:19:45, Serial0/1/0
O       10.0.9.4/30 [110/7501] via 10.0.9.17, 01:19:45, Serial0/0/1
C       10.0.9.8/30 is directly connected, Serial0/1/1
L       10.0.9.10/32 is directly connected, Serial0/1/1
C       10.0.9.12/30 is directly connected, Serial0/1/0
L       10.0.9.14/32 is directly connected, Serial0/1/0
C       10.0.9.16/30 is directly connected, Serial0/0/1
L       10.0.9.18/32 is directly connected, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 8 subnets, 4 masks
O       172.16.68.0/27 [110/7502] via 10.0.9.13, 01:19:45, Serial0/1/0
                       [110/7502] via 10.0.9.17, 01:19:45, Serial0/0/1
O       172.16.68.32/27 [110/7502] via 10.0.9.13, 01:19:45, Serial0/1/0
                        [110/7502] via 10.0.9.17, 01:19:45, Serial0/0/1
O       172.16.68.64/27 [110/7502] via 10.0.9.13, 01:19:45, Serial0/1/0
                        [110/7502] via 10.0.9.17, 01:19:45, Serial0/0/1
O       172.16.68.96/27 [110/7502] via 10.0.9.13, 01:19:45, Serial0/1/0
                        [110/7502] via 10.0.9.17, 01:19:45, Serial0/0/1
O       172.16.69.0/25 [110/7501] via 10.0.9.17, 01:20:20, Serial0/0/1
C       172.16.69.128/26 is directly connected, GigabitEthernet0/1
L       172.16.69.129/32 is directly connected, GigabitEthernet0/1
O       172.16.69.192/26 [110/7501] via 10.0.9.13, 01:20:20, Serial0/1/0
     209.165.202.0/27 is subnetted, 1 subnets
O       209.165.202.0/27 [110/15000] via 10.0.9.17, 01:20:20, Serial0/0/1
S*   0.0.0.0/0 [1/0] via 209.165.202.1
```

Рисунок 4.5– Таблиця маршрутизації на Minenko _R4

Виходячи з адресації маршрутизаторів ми бачимо, що всі наявні мережі вказані в таблицях, тому топологія повністю сходиться, а це значить, що з будь-якої мережі можна відправляти повідомлення до іншої, та це повідомлення буде обов'язково прийняте.

4.3.3 Налаштування роботи Інтернет

Згідно до технічних вимог для розгортання корпоративної мережі заданий блок адрес з діапазону приватних адрес. Для надання можливості доступу робочих станцій організації до мережі Internet, на прикордонному маршрутизаторі необхідно застосувати технологію NAT.

NAT – це механізм зміни мережевої адреси в заголовках IP датаграм, поки вони проходять через маршрутизуючий пристрій з метою відображення одного адресного простору в інший. Завдяки NAT можна, використовуючи одну або кілька

зовнішніх IP-адрес, виданих провайдером, підключити до мережі практично будь-яку кількість комп’ютерів. Більшість маршрутизаторів дозволяють виконувати трансляцію адрес, завдяки чому їх можна використовувати для підключення невеликих мереж до інтернету, використовуючи одну зовнішню IP-адресу.

NAT на прикордонному маршрутизаторі налаштовано згідно з вимогами:

- пул адрес: з 209.165.202.1 по 209.165.202.30;
- 172.16.29.107/28 – адреса Server HTTP;
- номер списку доступу: 9;
- ім'я пулу: Internet.

NAT на Minenko_R3:

Minenko_R3(config)#access-list 9 permit 172.16.68.0 0.0.3.255//список контролю доступу, що дозволяє всі адреси внутрішньої мережі

Minenko_R3(config)#ip nat pool Internet 209.165.202.5 209.165.202.30 netmask 255.255.255.224// пул для динамічного виділення інтернет адрес

Minenko_R3(config)#ip nat inside source list 9 pool Internet// підміна адреси внутрішньої мережі на інтернет адреси згідно з списком контролю доступу

Minenko_R3(config)#i ip nat inside source static 172.16.69.139 209.165.200.5// статичний NAT для серверу HTTP

Minenko_R3(config)#interface Serial0/0/0

Minenko_R3(config-if)#ip nat outside // коли пакет надходить на порт то відбувається заміна інтернет адреси на адресу внутрішньої мережі при проходженні через порт

Minenko_R3(config-if)#interface Serial0/0/1

Minenko_R3(config-if)#ip nat inside // коли пакет надходить на порт то відбувається заміна адреси внутрішньої мережі на інтернет адресу

Для перевірки роботи NAT відобразим таблицю перетворювань (рис.4.6).

NAT Table for Minenko_R3

Protocol	Inside Global	Inside Local	Outside Local	Outside Global
icmp	209.165.202.5:2	172.16.68.108:2	209.165.200.5:2	209.165.200.5:2
icmp	209.165.202.5:3	172.16.68.108:3	209.165.200.5:3	209.165.200.5:3
icmp	209.165.202.8:1	172.16.69.141:1	209.165.200.5:1	209.165.200.5:1
icmp	209.165.202.6:4	172.16.69.18:4	209.165.200.5:4	209.165.200.5:4
icmp	209.165.202.7:2	172.16.69.207:2	209.165.200.5:2	209.165.200.5:2
---	209.165.200.5	172.16.69.139	---	---

Рисунок 4.6 – Таблиця перетворювань NAT на Minenko_R3

4.3.4 Налаштування агрегування каналів PAgP

Port Aggregation Protocol (PAgP) (агрегування каналів) – пропріетарний протокол компанії Cisco Systems, служить для автоматизації агрегування фізичних Ethernet портів комутатора в один логічний. Таке об'єднання дозволяє збільшувати пропускну здатність і надійність каналу. Агрегування каналів може бути налаштоване між двома комутаторами, комутатором і маршрутизатором, між комутатором і хостом.

Налаштування EtherChannel на Minenko_Sw2.2:

Minenko_Sw2.2(config)# interface range f0/1-2
Minenko_Sw2.2(config-if-range)# channel-group 1 mode auto
Minenko_Sw2.2(config-if-range)# interface range f0/3-4
Minenko_Sw2.2(config)# channel-group 3 mode auto
Minenko_Sw2.2(config)# interface Port-channel 1
Minenko_Sw2.2(config)# switchport mode trunk
Minenko_Sw2.2(config)# interface Port-channel 3
Minenko_Sw2.2(config)# switchport mode trunk

Налаштування EtherChannel на Minenko_Sw2.3:

Minenko_Sw2.3*(config)# interface range f0/1-2*
Minenko_Sw2.3*(config-if-range)# channel-group 1 mode desirable*
Minenko_Sw2.3*(config)# interface range f0/5-6*

Minenko_Sw2.3*(config-if-range)# channel-group 2 mode desirable*
Minenko_Sw2.3*(config)# interface Port-channel 1*
Minenko_Sw2.3*(config)# switchport mode trunk*
Minenko_Sw2.3*(config)#interface Port-channel 2*
Minenko_Sw2.3*(config)# switchport mode trunk*

Налаштування EtherChannel на Minenko_Sw2.1:

Minenko_Sw2.1(config)# interface range f0/3-4
Minenko_Sw2.1(config-if-range)# channel-group 3 mode auto
Minenko_Sw2.1(config)# interface range f0/5-6
Minenko_Sw2.1(config-if-range)# channel-group 2 mode desirable
Minenko_Sw2.1(config)# interface Port-channel 2
Minenko_Sw2.1(config)# switchport mode trunk
Minenko_Sw2.1(config)#interface Port-channel 3
Minenko_Sw2.1(config)# switchport mode trunk

Для переверки роботи протоколу PAgP застосуємо команду *Minenko_Sw2.2#sh etherchannel summary*. Результат перевірки наведений на рисунку 4.7.

```
Minenko_Sw2.2#sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------
+---------------------------------------------

1      Po1(SU)           PAgP   Fa0/1(P) Fa0/2(P)
3      Po3(SD)           PAgP   Fa0/3(I) Fa0/4(I)
Minenko_Sw2.2#
```

Рисунок 4.7 – Переверка роботи протоколу PAgP, сумарна інформація про стан Etherchannel на Minenko_Sw2.2

З наведеного результату роботи команди, можна зробити висновок, що налаштування протоколу PAgP виконані вірно.

4.3.5 Налаштування віртуальної приватної мережі site-to-site VPN з використанням IPsec

Налаштувати віртуальну приватну мережу site-to-site VPN з використанням IPsec для трафіку, що проходить між Підмережою зділ Освіти та молоді» та віддаленою мережою «Відділ адміністрування»через Internet.

Налаштування на Minenko_R0:

Minenko_R0(config)#access-list 110 permit ip 172.16.69.0 0.0.0.127 172.16.70.0 0.0.0.31

Налаштування параметрів 1 фази ISAKMP

Minenko_R0(config)#crypto isakmp policy 10

Minenko_R0(config-isakmp)#encryption aes

Minenko_R0(config-isakmp)#authentication pre-share

Minenko_R0(config-isakmp)#group 2

Minenko_R0(config-isakmp)#exit

Minenko_R0(config)#crypto isakmp key cisco address 209.165.202.2

Налаштування параметрів 2 фази ISAKMP

Minenko_R0(config)#crypto ipsec transform-set VPN-CONF esp-3des esp-sha-hmac

Minenko_R0(config)#crypto map VPN-MAP 10 ipsec-isakmp

Minenko_R0(config-crypto-map)#description VPN connection to Minenko_R3

Minenko_R0(config-crypto-map)#set peer 209.165.202.2

Minenko_R0(config-crypto-map)#set transform-set VPN-CONF

Minenko_R0(config-crypto-map)#match address 110

Minenko_R0(config-crypto-map)#exit

Налаштування криптографічного порівняння

Minenko_R0(config)#interface Serial 0/0/1

Minenko_R0(config-if)#crypto map VPN-MAP

```
Minenko_R0$sh crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPN-MAP, local addr 64.100.13.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.69.0/255.255.255.128/0/0)
   remote  ident (addr/mask/prot/port): (172.16.70.0/255.255.255.224/0/0)
   current_peer 64.100.13.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 0.0.0.0, remote crypto endpt.64.100.13.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x0(0)
```

Рисунок 4.8 – Перевірка стану IPSec SA

4.3.6 Перевірка роботи комп’ютерної системи

Для перевірки роботи комп’ютерної системи перевіримо доступність вузлів мережі, налаштування безпечного віддаленого доступу до активних мережних пристроїв, перевірку зв'язку між вузлами з різних VLAN при автоматичному призначенні адрес.

Для перевірки SSH зробимо підключення з командного рядка PC5_B4 з підмережі «Будівля 4» маршрутизатора Minenko_R1 від користувача 12317sk_ Minenko з паролем *admincisco* командою, що наведена на рисунку 4.9.

Для перевірки роботи доступність вузлів мережі виконаємо команду ping для вузлів з різних підмереж, вузол P5_B2 Buh з підмережі «Будівля 2» пінгує хост PC3_B3 172.16.69.18 з підмережі «Будівля 3».

В мережах VLAN користувачі отримують мережеві налаштування по протоколу DHCP. Для цього необхідно налаштувати маршрутизатор Minenko_R1 та вузли мережі на підтримку DHCP.

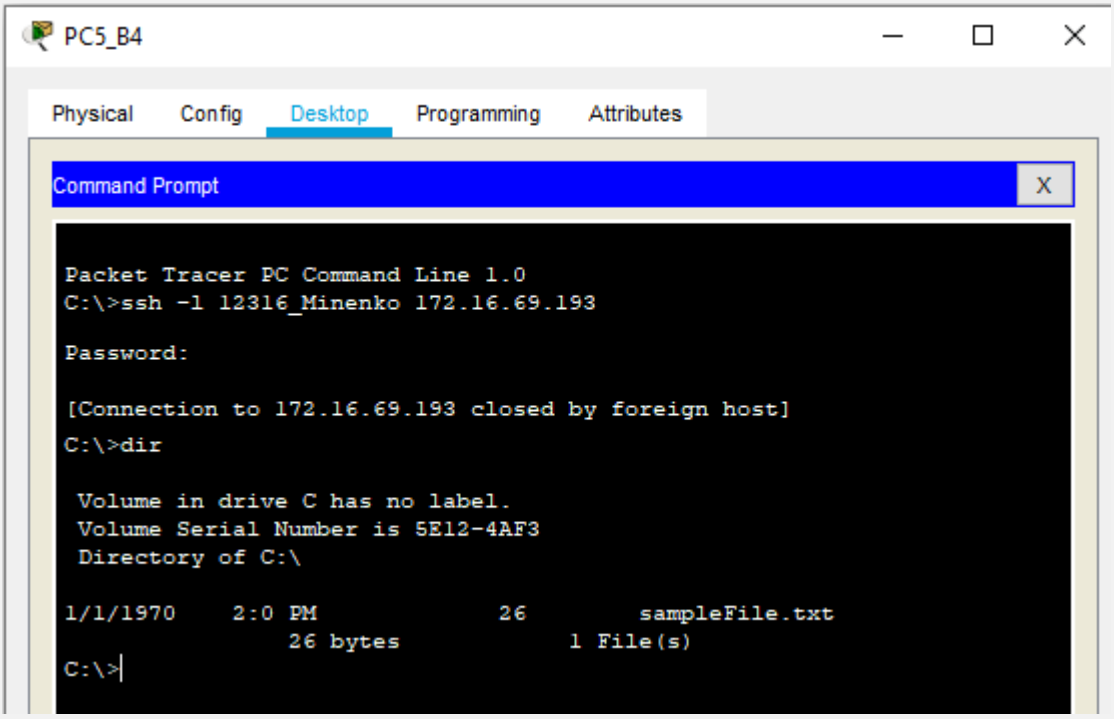

Рисунок 4.9 – Перевірка підключення до маршрутизатора Minenko_R1 за допомогою SSH

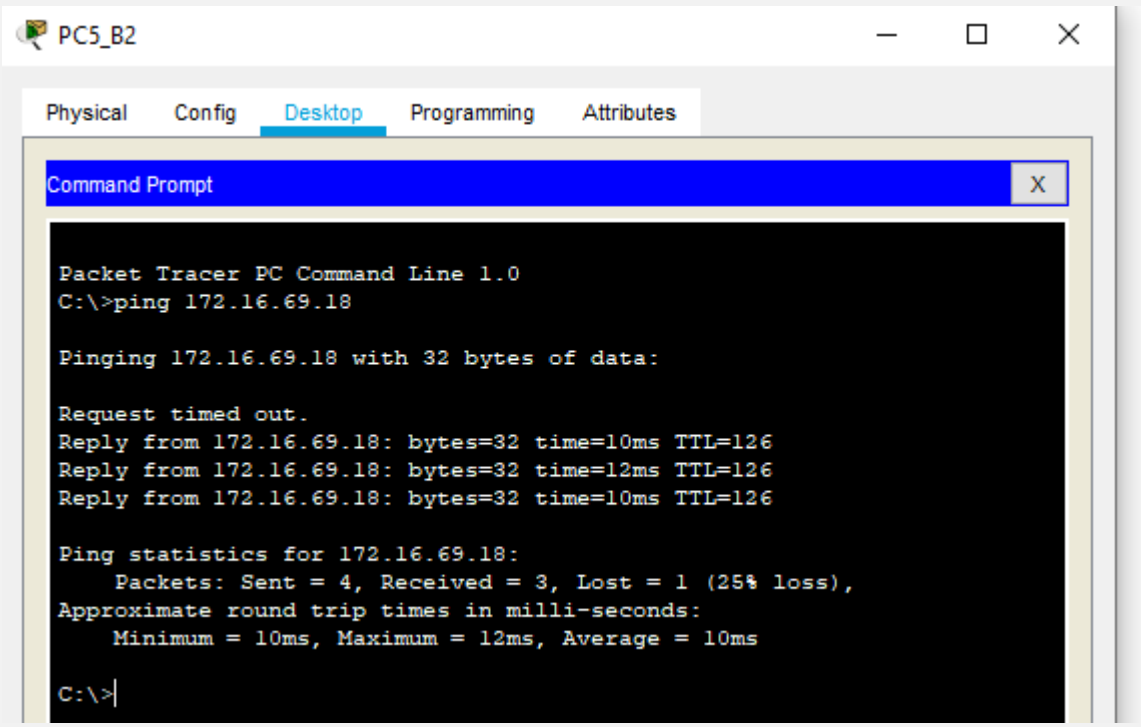

Рисунок 4.10 – Результат перевірки доступності вузлів мережі

DHCP – це протокол, який дозволяє комп'ютерам автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі. Протокол DHCP працює за схемою клієнт-сервер. Під час запуску системи комп’ютер, який є DHCP-клієнтом, відправляє в мережу запит на отримання IP-адреси. DHCP-сервер відповідає і відправляє повідомлення-відповідь, яка містить IP-адресу і деякі інші конфігураційні параметри.

Згідно до технічних вимог налаштовано маршрутизатор *Minenko_R2*, що здійснює маршрутизацію між VLAN і виступає в якості DHCP-серверу для мереж VLAN19-VLAN39. Створені пули DHCP під назвами pollvlan19- pollvlan39. Виключені з пулу перші 10 адрес. Для кожного пулу вказана адреса DNS-сервера і шлюз за замовчуванням.

Налаштування маршрутизації між VLAN за допомогою технології інкапсуляції на маршрутизаторі *Minenko_R2*:

```
Minenko_R2(config)#interface GigabitEthernet0/1
Minenko_R2(config-if)#no shutdown
Minenko_R2(config-if)#interface GigabitEthernet 0/1.19
Minenko_R2(config-if)#encapsulation dot1Q 19
Minenko_R2(config-if)#ip address 172.16.68.33 255.255.255.224
Minenko_R2(config-if)#interface GigabitEthernet 0/1.19
Neklesa_RouteR4(config-if)#encapsulation dot1Q 19
Minenko_R2(config-if)#ip address 172.16.68.65 255.255.255.224
Minenko_R2(config-if)#interface GigabitEthernet 0/1.19
Minenko_R2(config-if)#encapsulation dot1Q 19
Minenko_R2(config-if)#ip address 172.16.68.97 255.255.255.224
Minenko_R2(config-if)#interface GigabitEthernet 0/1.99
Minenko_R2(config-if)#encapsulation dot1Q 99
Minenko_R2(config-if)#ip address 172.16.68.1 255.255.255.224
```

Перевіримо динамічне призначення IP-адрес вузлам за допомогою протоколу DHCP, які знаходяться у VLAN-ах, а також перевіримо маршрутизацію між ними.

```
Minenko_R2#sh ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
172.16.68.44     0001.96C6.2DD8          --                      Automatic
172.16.68.45     0030.F267.CB94          --                      Automatic
172.16.68.46     0001.43D5.358D          --                      Automatic
172.16.68.76     0007.EC0D.C5CD          --                      Automatic
172.16.68.77     0090.21CB.33A4          --                      Automatic
172.16.68.78     0030.F2B4.38CD          --                      Automatic
172.16.68.108    000A.41C6.9889          --                      Automatic
172.16.68.109    00D0.FF6B.8E7C          --                      Automatic
Minenko_R2#
```

Рисунок 4.11 − Таблиця призначення IP-адрес вузлам за протоколом DHCP

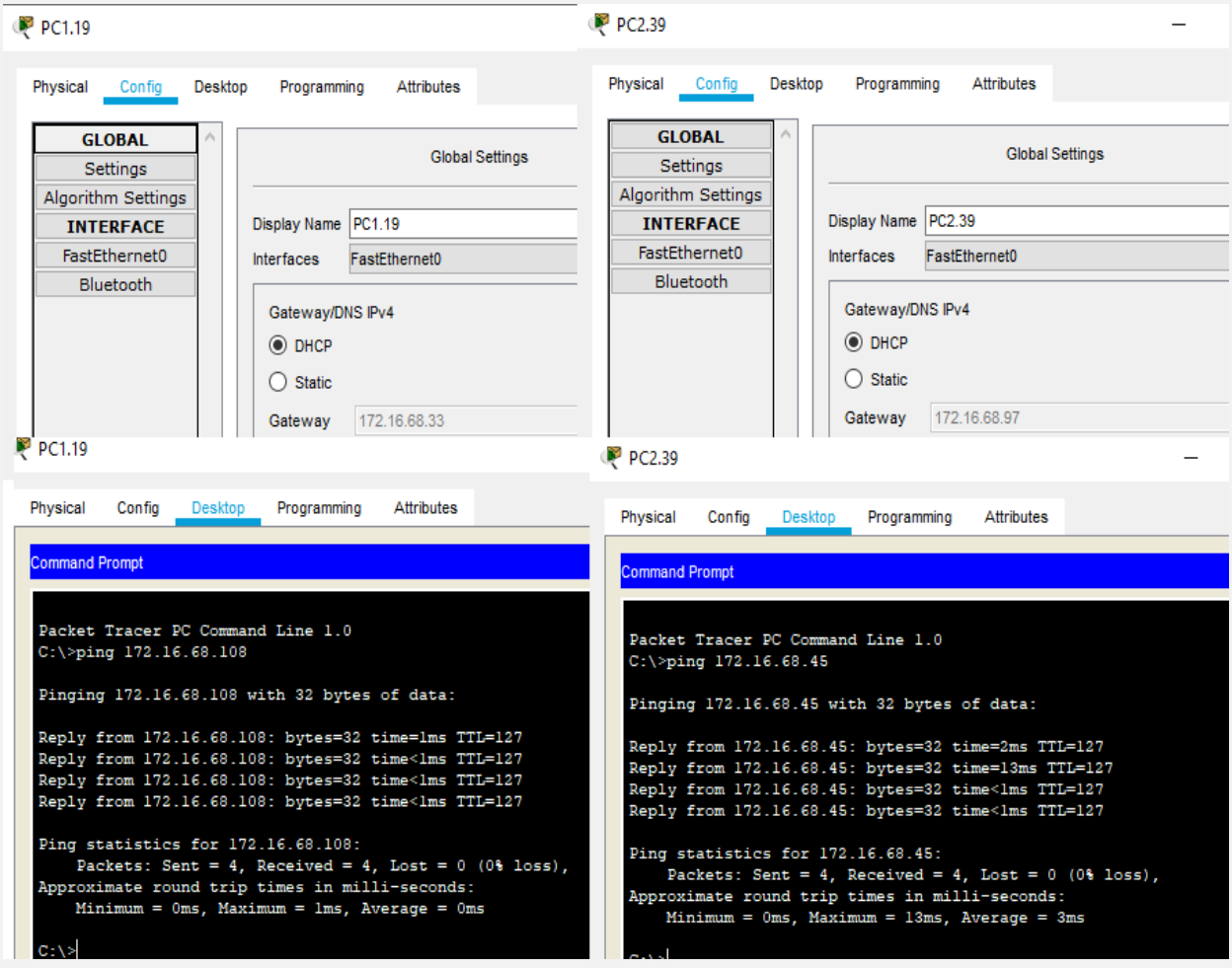

Рисунок 4.12 – Перевірка зв'язку між вузлами з різних VLAN при автоматичному призначенні адрес через DHCP

Виконане пінгування хостів, один з яких належть мережі VLAN 19, а інший мережі VLAN 39.

Передача трафіку між VLAN здійснюється за допомогою маршрутизатора. Для того щоб маршрутизатор міг передавати трафік з одного VLAN в інший (з однієї мережі в іншу), необхідно щоб в кожній мережі у нього був інтерфейс. Налаштування маршрутизації між VLAN буде здійснюватись на маршрутизаторі Minenko_R2 на інтерфейсі GigabitEthernet 0/1 pf технологією інкапсуляції 802.1Q .

На комутаторі Minenko_Sw1.1 порт G0/1, що веде до маршрутизатора, налаштований як тегованих порт (в термінах Cisco – транк).

Для логічних підінтерфейсів на маршрутизаторі необхідно вказувати те, що інтерфейс буде отримувати тегованих трафік і вказувати номер VLAN відповідний цьому інтерфейсу.

Minenko_R2(config)#interface g0/1

Minenko_R2(config-if)#no shutdown

Minenko_R2(config)#interface g0/0.19 // налаштування підінтерфейсу для маршрутизації трафіку між VLAN

Minenko_R2(config-subif)#encapsulation dot1Q 19 // тегування пакетів для данного підінтерфейсу.

Minenko_R2(config-subif)#ip address 172.16.68.33 255.255.255.224

Перевірка налаштувань наведена на рисунку 4.13.

Port Status Summary Table for Minenko_R2

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
GigabitEthernet0/0	Up	--	10.0.9.2/30	<not set>	00E0.B0C6.3E10
GigabitEthernet0/1	Up	--	<not set>	<not set>	00D0.D349.A876
GigabitEthernet0/1.19	Up	--	172.16.68.33/27	<not set>	00D0.D349.A876
GigabitEthernet0/1.29	Up	--	172.16.68.65/27	<not set>	00D0.D349.A876
GigabitEthernet0/1.39	Up	--	172.16.68.97/27	<not set>	00D0.D349.A876
GigabitEthernet0/1.99	Up	--	172.16.68.1/27	<not set>	00D0.D349.A876
GigabitEthernet0/2	Up	--	10.0.9.5/30	<not set>	00D0.58E9.86D1
Serial0/0/0	Down	--	<not set>	<not set>	<not set>
Serial0/0/1	Down	--	<not set>	<not set>	<not set>
Serial0/1/0	Down	--	<not set>	<not set>	<not set>
Serial0/1/1	Down	--	<not set>	<not set>	<not set>
Vlan1	Down	1	<not set>	<not set>	00E0.F727.37D0

Hostname: Minenko_R2

Рисунок 4.13 – Перевірка налаштування VLAN на Minenko_R2

5 ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНІЙ СИСТЕМІ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

5.1 Розробка методів для захисту інформації в комп'ютерній системі

Для захисту інформації в комп'ютерній системі від несанкціонованого доступу розробляються і описуються методи:

- налаштування мереж VLAN і маршрутизації між ними;
- на портах комутаторів, підключених до серверів, налаштовуються функції безпеки портів;
- маршрутизатори мережі налаштовуються на підтримку служби AAA та RADIUS-сервера.

5.2 Налаштування маршрутизаторів на підтримку служби AAA

Авторизація користувачів при підключені до мережевих пристроїв виконується за допомогою сервісів AAA (Authentication Authorization and Accounting). AAA – система аутентифікації, авторизації і обліку подій, вбудована в операційну систему Cisco IOS, служить для надання користувачам безпечного віддаленого доступу до мережного обладнання Cisco. Вона дозволяє централізовано керувати користувачам та доступом їх до мережевого обладнання. Вона пропонує різні методи ідентифікації користувача, авторизації, а також збору і відправки інформації на сервер.

Minenko _R2(config)#aaa new-model //запуск служби AAA

Minenko_R2(config)#aaa authentication login default local // налаштування методу аутентифікації за замовчуванням з використання локальної бази користувачів

Minenko _R2(config)#aaa authentication login Login group radius local // налаштування методу аутентифікайфії Login з використанням сереверу RADIUS, а якщо він недоступний, то з використанням локальної бази користувачів

Minenko _R2(config)#line console 0

Minenko _R2(config-line)#login authentication Login // застосування методу аутентифікайфії Login на консольній лінії

Minenko _R2(config)#line vty 0 4

Minenko _R2(config-line)#login authentication default // застосування методу аутентифікайфії за замовчуванням на vty-лінії

Налаштування RADIUS-сервер:

Minenko _R2(config)#radius-server host 172.16.69.139 auth-port 1645

Minenko _R2(config)#radius-server key radius12317

В якості облікового запису користувачів використовується ім’я пристрою з паролем *Admin12317.*

Перевіримо роботу аутентифікації, приєднавшись до маршрутизатора Minenko _R2(через консоль (рисунок 5.1), провівши аутентифікацію через сервер RADIUS.

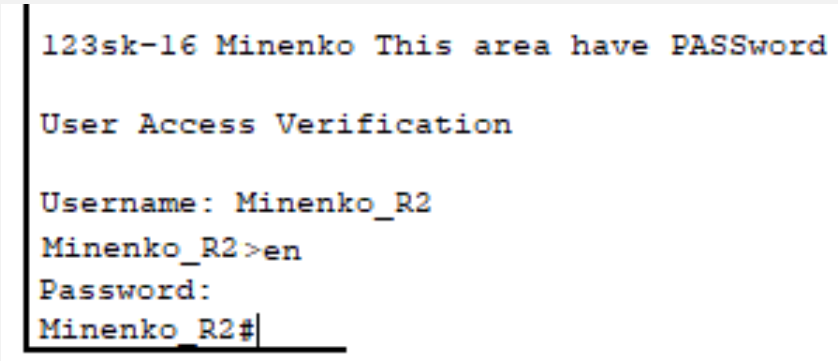

Рисунок 5.1 – Аутентифікація на маршрутизаторі за допомогою служби AAA та сервера RADIUS

Для того що зайти в режим користувача потрібно було ввести ім'я користувача та пароль, що був налаштований на сервері RADIUS.

5.3 Налаштування мереж VLAN

VLAN (від англ. Virtual Local Area Network) – віртуальна локальна обчислювальна мережа, відома так само як VLAN, являє собою групу хостів із загальним набором вимог, які взаємодіють так, як якщо б вони були підключені до широкомовному домену, незалежно від їх фізичного місцезнаходження. VLAN має ті ж властивості, що й фізична локальна мережа, але дозволяє кінцевим станціям, групуватися разом, навіть якщо вони не знаходяться в одній фізичній мережі. Така

реорганізація може бути зроблена на основі програмного забезпечення замість фізичного переміщення пристроїв.

На пристроях Cisco, протокол VTP (VLAN TrunkingProtocol) передбачає VLAN-домени для спрощення адміністрування. Згідно до вимог підмережа «Будівля 1» розділяється на чотири підмережі VLAN, та до них ще одна підмережа для керування VLAN. Відповідно до архітектури мережі в КС правління підприємства ПГОК створені мережі VLAN з присвоєним кожній з них ім'ям.

Таблиця 5.1 – Назви VLAN для підмережі «Будівля 1»

Номер VLAN	Ім’я VLAN	Примітка
1	Default	Не використовується
19	Tehn_Kontrol	Відділ технічного контролю
29	Perv_Oblik	Відділ рервичного обліку
39	Soc_Vopros	Відділ соц. запитань
99	Management	Для управління пристроями
100	Native	Власна

Додатково виконані налаштування:

− відповідно до технічних вимог настроєно транкові порти і порти доступу;

− вимкнено усі невикористовувані фізичні порти комутаторів;

− на портах комутаторів, підключених до серверів, настроєно функцію безпеки портів так, щоб:

a) тільки двом унікальним пристроям був дозволений доступ до порту;

b) MAC- адреса пристрою розпізнавалася динамічно і додавалася в поточну конфігурацію;

c) при порушенні системи безпеки вирушало повідомлення, а порт залишався включеним;

− налаштовано SVI-інтерфейси на комутаторах, призначивши по таблиці 4.3 IPv4- адреси з мережі Management VLAN;

− налаштувано маршрутизацію між мережами VLAN.

Налаштування на Minenko_Sw1.1:

Об’ява VLAN:

Switch (config)#hostname Minenko_Sw1.1
Minenko_Sw1.1(config)#vlan 9
Minenko_Sw1.1(config-vlan)#name Tehn_Kontrol
Minenko_Sw1.1(config-vlan)# vlan 29
Minenko_Sw1.1(config-vlan)#name Perv_Oblik
Minenko_Sw1.1(config-vlan)#vlan 39
Minenko_Sw1.1(config-vlan)#name Soc_Vopros
Minenko_Sw1.1(config-vlan)#vlan 99
Minenko_Sw1.1(config-vlan)# name Management
Minenko_Sw1.1(config-vlan)#vlan 100
Minenko_Sw1.1(config-vlan)# name Native

Налаштування транкових каналів:

Minenko_Sw1.1(config)#interface g0/1, f0/1
Minenko_Sw1.1(config-if)#switchport trunk native vlan 100
Minenko_Sw1.1(config-if)#switchport trunk allowed vlan 19,29,39,99-100
Minenko_Sw1.1(config-if)#switchport mode trunk
Minenko_Sw1.1(config-if)#exit

Налаштування портів доступу:

// включити режим access для інтерфейсів кожної vlan
Minenko_Sw1.1(config)#interface range f0/4-8
Minenko_Sw1.1(config-if)#switchport mode access
Minenko_Sw1.1(config-if)# switchport access vlan 19
Minenko_Sw1.1(config)#interface range f0/10-14
Minenko_Sw1.1(config-if)#switchport mode access
Minenko_Sw1.1(config-if)# switchport access vlan 29
Minenko_Sw1.1(config)#interface range f0/15-20
Minenko_Sw1.1(config-if)#switchport mode access
Minenko_Sw1.1(config-if)# switchport access vlan 39

Налаштування SVI-интерфейсу:

Minenko_Sw1.1(config)# interface Vlan99

Minenko_Sw1.1(config-if)# ip address 172.16.68.3 255.255.255.224
Minenko_Sw1.1(config-if)#no shutdown
Minenko_Sw1.1(config-if)#ip default-gateway 172.16.68.1

Для перевірки налаштування відобразимо сумарну інформацію про налаштування VLAN на комутаторах і відповідних їм портів (рис. 5.2-5.3)

Port Status Summary Table for Minenko_Sw1.1

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	--	--	00D0.BCC5.C401
FastEthernet0/2	Down	1	--	00D0.BCC5.C402
FastEthernet0/3	Down	1	--	00D0.BCC5.C403
FastEthernet0/4	Up	19	--	00D0.BCC5.C404
FastEthernet0/5	Up	19	--	00D0.BCC5.C405
FastEthernet0/6	Down	19	--	00D0.BCC5.C406
FastEthernet0/7	Down	19	--	00D0.BCC5.C407
FastEthernet0/8	Down	19	--	00D0.BCC5.C408
FastEthernet0/9	Down	1	--	00D0.BCC5.C409
FastEthernet0/10	Up	29	--	00D0.BCC5.C40A
FastEthernet0/11	Down	29	--	00D0.BCC5.C40B
FastEthernet0/12	Down	29	--	00D0.BCC5.C40C
FastEthernet0/13	Down	29	--	00D0.BCC5.C40D
FastEthernet0/14	Up	29	--	00D0.BCC5.C40E
FastEthernet0/15	Up	39	--	00D0.BCC5.C40F
FastEthernet0/16	Down	39	--	00D0.BCC5.C410
FastEthernet0/17	Down	39	--	00D0.BCC5.C411
FastEthernet0/18	Down	39	--	00D0.BCC5.C412
FastEthernet0/19	Down	39	--	00D0.BCC5.C413
FastEthernet0/20	Down	39	--	00D0.BCC5.C414
FastEthernet0/21	Down	1	--	00D0.BCC5.C415
FastEthernet0/22	Down	1	--	00D0.BCC5.C416
FastEthernet0/23	Down	1	--	00D0.BCC5.C417
FastEthernet0/24	Down	1	--	00D0.BCC5.C418
GigabitEthernet0/1	Up	--	--	00D0.BCC5.C419
GigabitEthernet0/2	Down	1	--	00D0.BCC5.C41A
Vlan1	Down	1	<not set>	00D0.973B.1AC8
Vlan99	Up	99	172.16.68.2/27	00D0.973B.1A01

Hostname: Minenko_Sw1.1

Рисунок 5.2 – Налаштування VLAN на Minenko_Sw1.1

Port Status Summary Table for Minenko_Sw1.2

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	--	--	000C.CF1D.9B01
FastEthernet0/2	Down	1	--	000C.CF1D.9B02
FastEthernet0/3	Down	1	--	000C.CF1D.9B03
FastEthernet0/4	Up	19	--	000C.CF1D.9B04
FastEthernet0/5	Down	19	--	000C.CF1D.9B05
FastEthernet0/6	Down	19	--	000C.CF1D.9B06
FastEthernet0/7	Down	19	--	000C.CF1D.9B07
FastEthernet0/8	Down	19	--	000C.CF1D.9B08
FastEthernet0/9	Down	1	--	000C.CF1D.9B09
FastEthernet0/10	Up	29	--	000C.CF1D.9B0A
FastEthernet0/11	Up	29	--	000C.CF1D.9B0B
FastEthernet0/12	Down	29	--	000C.CF1D.9B0C
FastEthernet0/13	Down	29	--	000C.CF1D.9B0D
FastEthernet0/14	Down	29	--	000C.CF1D.9B0E
FastEthernet0/15	Up	39	--	000C.CF1D.9B0F
FastEthernet0/16	Down	39	--	000C.CF1D.9B10
FastEthernet0/17	Down	39	--	000C.CF1D.9B11
FastEthernet0/18	Down	39	--	000C.CF1D.9B12
FastEthernet0/19	Down	39	--	000C.CF1D.9B13
FastEthernet0/20	Down	39	--	000C.CF1D.9B14
FastEthernet0/21	Down	1	--	000C.CF1D.9B15
FastEthernet0/22	Down	1	--	000C.CF1D.9B16
FastEthernet0/23	Down	1	--	000C.CF1D.9B17
FastEthernet0/24	Down	1	--	000C.CF1D.9B18
GigabitEthernet0/1	Down	1	--	000C.CF1D.9B19
GigabitEthernet0/2	Down	1	--	000C.CF1D.9B1A
Vlan1	Down	1	<not set>	0001.9693.6375
Vlan99	Up	99	172.16.68.3/27	0001.9693.6301

Hostname: Minenko_Sw1.2

Рисунок 5.3 – Налаштування VLAN на Minenko_Sw1.2

5.4 Налаштування параметрів безпеки комутаторів

На портах комутаторів, підключених до серверів, використана функція безпеки портів таким чином, що:

- тільки одному узлу дозволений доступ до порту;
- MAC-адреса пристрою додається статично в поточну конфігурацію;
- при порушенні системи безпеки порт виключається.

Команди використані на комутаторі Minenko_Sw2 згідно технічних вимог.

Налаштування на портах комутаторів, що підключені до серверів функції безпеки портів:

Minenko_Sw2(config)#interface fa0/24// вхід в інтерфейс

Minenko_Sw2(config)#switchport mode access// режим інтерфейса для отримання доступу

Вхід до налаштування безпеки порту:

Minenko_Sw2(config)#switchport port-security

Дозволити тільки одному вузлу доступ до порту:

Minenko_Sw2(config)#switchport port-security maximum 1

Увімкнення запам’ятовування MAC-адрес:

Minenko_Sw2(config)#switchport port-security mac-address sticky

Налаштування реагування на порушення безпеки порту – порушення безпеки призводить до того, що інтерфейс переводиться в стан error-disabled і вимикається негайно:

Minenko_Sw2(config)#switchport port-security violation shutdown

6 ЕКОНОМІЧНА ЧАСТИНА

6.1 Техніко-економічне обґрунтування розробки

У дипломній роботі розглядається комп'ютерна система правління підприємства ПГОК з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі. Функціями Системи є забезпечення безперервного обміну інформацією між складовими елементами мережі підприємства, зберігання інформації у базах даних, забезпечення доступу у інтернет і т.і. між підрозділами підприємства.

Впровадження Системи дозволяє підвищити надійність та ефективність роботи підрозділів, зменшити вплив людського фактору, реалізувати моніторинг та ведення архіву даних.

Для обґрунтування економічної ефективності застосування Системи, необхідно виконати:

- розрахунок капітальних витрат на придбання складових Системи;
- розрахунок річних експлуатаційних витрат;
- величину річного економічного ефекту.

6.2 Розрахунок капітальних витрат

6.2.1 Розрахунок капітальних витрат на придбання складових комп'ютерної системи

Капітальні вкладення – це кошти, призначені для створення і придбання основних фондів та нематеріальних активів, що підлягають амортизації.

Кошторис капітальних витрат на обладнання, яке необхідно для реалізації комп'ютерної системи, приведена в таблиці 6.1.

Капітальні витрати розраховуються за формулою:

$$К_{пр} = К_{об} + К_{тр} + К_{мн} + К_{пз}, \quad (6.1)$$

де $К_{об}$ – вартість обладнання, грн.,

$К_{тр}$ – вартість транспортно-заготівельних витрат, грн.,

$К_{мн}$ – вартість монтажно-налагоджувальних робіт, грн.,

$К_{пз}$ – вартість розробки програмного забезпечення.

Таблиця 6.1 – Кошторис капітальних витрат

№ з/п	Найменування обладнання	Ед. виміру	Кіль-кість	Вартість од. облад-я, грн	Сумма, грн.
1	Маршрутизатор Cisco 2811	од.	6	5638	33828
2	Комутатор Cisco Catalyst 2948-24TT	од.	8	14040	112320
3	Комутатор FoxGate S6009	од.	3	1771	5313
4	Комутатор D-Link DES-1018P	од.	1	5843	5843
5	Робоча станція ASUS Vivo AiO V222UA	од.	40	10519	420760
6	Кабель канал 40х60	м	738	125	92250
7	Кабель канал 20х40	м	228	72	16416
8	Розетка мережева	од.	44	63	2772
9	Розетка живлення		24	120	2880
10	Кабель F/UTP	м	966	44	42504
Разом					734886

Загальна вартість обладнання $К_{об}$=734886 грн.

Вартість транспортно-заготівельних і складських витрат становить 7% від вартості обладнання.

$К_{тр}$=734886*7%=51442 грн.

Вартість монтажно-налагоджувальних робіт становить 8% від вартості обладнання.

$К_{мн}$=734886*8%=58791 грн.

6.2.2 Розрахунок капітальних витрат на програмне забезпечення

6.2.2.1 Розрахунок часу на розробку програмного забезпечення

Трудомісткість розробки програмного забезпечення:

$$t = t_o + t_д + t_a + t_n + t_{нал} + t_{док}, \quad (6.2)$$

де t_o - витрати праці на підготовку й опис поставленого завдання;

$t_д$ - витрати праці на дослідження алгоритму розв'язку завдання;

t_a - витрати праці на обробку блок-схеми алгоритму;

t_n - витрати праці на програмування по готовій блок-схемі;

$t_{нал}$ - витрати праці на налаштування програм на ЕОМ;

$t_{док}$ - витрати праці на підготовку документації за завданням.

Складові частини витрат праці визначаються на підставі умовної кількості оброблюваних операторів у програмному забезпеченні. До них відносять ті оператори, які необхідно написати в процесі роботи над програмою з урахуванням можливих уточнень у постановці завдання й удосконалення алгоритму.

Умовна кількість операторів у програмі:

$$Q = q \cdot c \cdot (1+p), \quad (6.3)$$

де q –кількість операторів, використовуваних у програмі.

Виходячи з ПЗ q = 280;

c – коефіцієнт складності програми;

p – коефіцієнт корекції програми в процесі її обробки.

Коефіцієнт складності «c» програми визначає відносну складність програми відносно типового завдання, складність якого відповідає 1. c = 1,25.

Коефіцієнт корекції програми «p» визначає збільшення обсягу робіт за рахунок внесення змін в алгоритм або програму в результаті уточнення постановки завдання. Ухвалюємо p=0,1, це відповідає внесенню 3…5 корекцій, що тягнуть за собою переробку 5-10% готової програми.

Таким чином, для програми, описаної в дипломному проекті:

Q = 280·1,25(1+0,1) = 385

Оцінка витрат праці на підготовку й опис завдання становлять

$t_0 = 50$ люд.-годин.

Витрати праці на вивчення опису завдання визначаються з урахуванням уточнення опису й кваліфікації програміста по формулі:

$$t_д = \frac{Q \cdot B}{(75...85) \cdot k} \text{ люд.-годин} \quad (6.4)$$

де В – коефіцієнт збільшення витрат праці, В=1,4;

k – коефіцієнт кваліфікації програміста, які визначається залежно від стажу роботи зі спеціальності. У нашому випадку коефіцієнт кваліфікації програміста становить k= 1,2.

Для розроблюваного програмного забезпечення:

$t_{д}=\frac{385*1,4}{80*1,2}=5,6$ люд.-годин.

Витрати на розробку алгоритму розв'язку завдання:

$$t_a = \frac{Q}{(20...25)\cdot k} \text{ люд.-годин} \qquad (6.5)$$

Для розроблювального програмного забезпечення:

$t_a = \frac{385}{20\cdot 1,2}$ = 16 люд.-годин.

Витрати праці на складання програми по готовій блок-схемі алгоритму:

$$t_n = \frac{Q}{(20...25)\cdot k} \text{ люд.-годин} \qquad (6.6)$$

Для розроблюваного програмного продукту:

$t_n = \frac{385}{20\cdot 1,2}$ =16 люд.-годин.

Витрати праці на налагодження програми на ЕОМ розраховуються по формулі:

$$t_{нал} = \frac{Q}{(4...5)\cdot k} \text{ люд.-годин} \qquad (6.7)$$

Для конкретного програмного продукту:

$t_{нал} = \frac{385}{5\cdot 1,2}$ = 64,2 люд.-годин.

Витрати праці на підготовку документації за завданням визначаються по формулі:

$$t_Д = t_{ДР} + t_{ДО,} \text{ люд.-година} \qquad (6.8)$$

де $t_{ДР}$ – трудомісткість підготовки матеріалів до написання;

$t_{ДО}$ – трудомісткість редагування, друку й оформлення документації.

$$t_{ДР} = Q/(15…20)\cdot k, \quad (6.9)$$

$t_{ДР}$ = 385/18·1,2 = 17,8 люд.-година;

$$t_{ДО} = 0,75\cdot t_{ДР}, \quad (6.10)$$

$t_{ДО}$ = 0,75· 17,8 = 13,35 люд.-година.

Для розроблюваного програмного забезпечення витрати праці на підготовку документації за завданням будуть становити:

$t_{Д}$ = 17,8+ 13,35 = 31 люд.-година.

Трудомісткість розробки програмного забезпечення буде становити:

t = 50 + 5,6 + 16 + 16 + 64,2 + 31 = 182,8 людино-годин.

6.2.2.2 Розрахунки витрат на розробку програмного продукту

Витрати на розробку програмного продукту $К_{пз}$ містять витрати на заробітну плату розробника програми $З_{зп}$ і вартість машинного часу, необхідного для налаштування програми на ЕОМ $З_{мч}$

$$К_{пз} = З_{зп} + З_{ми}, \text{ грн.} \quad (6.11)$$

Заробітна плата розробника програмного забезпечення:

$$З_{зп} = t\cdot С_{пр}, \text{ грн.} \quad (6.12)$$

де t – загальна трудомісткість обробки програмного забезпечення;

$С_{пр}$ – середня годинна тарифна ставка програміста становить:

$С_{пр}$ = 67 грн./година.

Заробітна плата за розробку програмного забезпечення дорівнює:

$З_{зп}$ = 182,8 ·67 =122478 грн.

Вартість машинного часу, необхідного для налаштування програми на ЕОМ:

$$З_{мч} = t_{отл}\, С_{мг}, \text{ грн.} \quad (6.13)$$

де:

$t_{отл}$ – трудомісткість налаштування програми на ЕОМ, людино-годин;

$С_{мг}$ – вартість машино-години ЕОМ, грн./година. $С_{мг}$ = 5 грн/година.

$З_{мч}$ = 64,2 ·5 = 321

Витрати на розробку програмного забезпечення системи керування будуть становити:

$К_{пз}$ = 122478+ 321= 122799

Певні, таким чином, витрати на створення програмного забезпечення є частиною одноразових капітальних витрат на створення Системи.

Очікувана тривалість розробки програмного забезпечення:

$$T = \frac{t}{B_k \cdot F_p}, \text{ міс.} \quad (6.14)$$

де, $B_к$ – кількість розробників. Програма розроблялася однією людиною, тому $В_к$ = 1;

F_p – місячний фонд робочого часу (Fp = 176 годин).

Визначимо тривалість розробки ПО:

$$T = \frac{182{,}8}{1 \cdot 176} = 1{,}04 \text{ міс.}$$

Таким чином, капітальні витрати розраховані за формулою (6.1) дорівнюють:

$К_{пр}$ = 734886+51442+58791+122799= 967918 грн.

6.3 Розрахунок річних експлуатаційних витрат на Систему

Експлуатаційні витрати визначаються за такими статтями витрат:

– амортизаційні відрахування ($С_а$);

– заробітна плата обслуговуючого персоналу ($С_{зп}$);

– відрахування на соціальні заходи ($С_с$);

– витрати на технічне обслуговування і поточний ремонт обладнання ($С_{то}$);

– вартість спожитої електроенергії ($С_е$)

– інші ($С_і$).

Таким чином, експлуатаційні витрати розраховуються за формулою:

$$С = С_а + С_{зп} + С_с + С_{то} + С_е + С_і \quad (6.15)$$

Для розрахунку показників економічної ефективності необхідно розрахувати експлуатаційні витрати по проектному варіанту комп’ютерної системи та існуючому. За даними бухгалтерії підприємства капітальні витрати на існуючу КС склали 1386472 грн.

6.3.1 Розрахунок амортизаційних відрахувань

Комп’ютерні система відносяться до четвертої групи (машини і обладнання) відповідно до класифікації груп основних засобів та інших необоротних активів. Для систем на базі комп’ютерної техніки мінімальний термін експлуатації становить 5 років. Амортизація для комп’ютерної системи визначається методом прискореного зменшення залишкової вартості, з терміном експлуатації в 5 років.

Норма амортизації розраховується за формулою:

$$Ha = \frac{2}{T} \tag{6.16}$$

де , Т – строк корисного використання КС.

$Ha = 2/5 = 0,4$

Таким чином, амортизаційні відрахування по обладнанню, будуть визначатися по формулі 6.17:

$$С_{а.п} = К_{пр} \cdot Н_а, \text{ грн.} \tag{6.17}$$

Амортизаційні відрахування (за перший рік експлуатації) для апаратного забезпечення системи становитимуть: $С_{а.п}$ = 967918 *0,4=387167 грн

Для існуючої системи: $С_{а.і}$ = 1386472 *0,4=554589 грн

6.3.2 Розрахунок річного фонду заробітної плати

Розрахунок річного фонду заробітної плати обслуговуючого персоналу, згідно форми, наведено в таблиці 6.2.

Для виконання робіт з контролю за роботою мережевого устаткування з 8-ми годинний зміною необхідні два штатних системних програміста, два системних адміністратора та один черговий системний адміністратор для існуючої мережі. Для проектного варіанта можна скоротити ставки для чергового системного адміністратор та одного штатного системних програміста.

Номінальний річний фонд робочого часу одного працівника визначається за формулою 6.18.

$$F_{ном} = (Т_к - Т_{пр} - Т_{вих} - Т_{відп}) * Т_{см}, \text{ годин} \tag{6.18}$$

Номінальний річний фонд робочого часу системного програміста або адміністратора:

$F_{ном}$=(365-9-104-21)*8=1848 годин

Таблиця 6.2 – Річний фонд заробітної плати

№ п/п	Найменування професії працівників	Кількість працюючих, люд.		Годинна тарифна ставка, грн	Номінальний річний фонд робочого часу	Всього пряма заробітна плата, грн.	Додаткова заробітна плата (10%)	Доплати (7%)	Всього заробітна плата, грн.
		явочне	списочне						
1	2	3	4	5	6	7	8	9	10
Існуючий варіант									
1	Системний програміст	2	2	57	1848	210672	21067	14747	246486
2	Системний адміністр-р	2	2	55	1848	203280	20328	14230	237838
3	Черговий системний адміністр-р	1	1	55	1848	203280	20328	14230	237838
Всього									722162
Проектний варіант									
4	Системний програміст	1	1	57	1848	105336	10533	7374	123243
5	Системний адміністр-р	2	2	55	1848	203280	20328	14230	237838
Всього									361081

$С_{зп.пр}$ = 361081 грн.

$С_{зп.і}$ = 722162 грн.

6.3.3 Розрахунок відрахувань на соціальні заходи

Відрахування на соціальні заходи становлять 22% від заробітної плати (формула 6.19):

$$C_c = C_{зп} * 22\%, \text{ грн.} \quad (6.19)$$

$C_{с.п}$=361081*0,22= 79438 грн.

$C_{с.і}$=722162*0,22= 158876 грн.

6.3.4 Визначення річних витрат на технічне обслуговування і поточний ремонт

Витрати на технічне обслуговування і поточний ремонт включають витрати на матеріали, запасні частини, заробітну плату ремонтним робітником. Вони складають 4% від капітальних витрат:

$$C_{то} = K_{пр} * 4\%, \text{ грн.} \quad (6.20)$$

$C_{то.п}$=$К_{пр}$*0,04=967918 *0,04= 38717 грн.

$C_{то.і}$=$К_{пр}$*0,04=1386472 *0,04= 55459 грн.

6.3.5 Розрахунок вартості споживаної електроенергії

Вартість спожитої електроенергії визначається за формулою:

$$C_е = М * F_р * а, \text{ грн,} \quad (6.21)$$

де М – встановлена потужність апаратури,

$F_р$ – річний фонд робочого часу апаратури (5840 годин – обладнання працює 16 годин на добу),

а – тариф на електроенергію для підприємств від постачальника ПАТ «ПОЛТАВАОБЛЕНЕРГО» (для користувачів електроенергії 2 класу тариф складає 825,40 грн. за МВт без ПДВ. З урахуванням ПДВ тариф Т = 825,40 * 1,2 / 1000 = 0,99 грн за кВт).

Сумарна споживана потужність пристроїв автоматики складе: маршрутизатори 1,2кВт; комутатори 1,1кВт; робочі станції 12кВт. Загалом 14,3кВт.

Се.п=14,3*5840*0,99=82677 грн.

Се.і=0,8*5840*0,99=4625 грн.

6.3.6 Визначення інших витрат

Інші витрати по експлуатації об'єкта проектування включають витрати на навчання персоналу підприємства обслуговування нового обладнання, з охорони праці, придбання спец одягу та ін. Ці витрати складають 4% від річного фонду заробітної плати обслуговуючого персоналу.

$$C_i = C_{зп}*4\%, \text{ грн.} \quad (6.22)$$

$C_{i.п} = 361081 \cdot 0,04 = 4625$ грн.

$C_{i.і} = 722162 \cdot 0,04 = 28887$ грн.

6.3.7 Визначення та аналіз показників економічної ефективності проекту

Результати розрахунків експлуатаційних витрат по проектованому і існуючому варіантам зведені в табл. 6.3.

Таблиця 6.3 – Річні експлуатаційні витрати

Найменування показника	Проектний варіант	Існуючий варіант
Амортизація	387167	554589
Фонд заробітної плати	361081	722162
Відрахування на соц. виплати	79438	158876
Ремонт і тех.обслуговування	38717	55459
Електроенергія	82677	4625
Інші	4625	28887
Разом	953705	1524598

Відповідно до формули 6.15 експлуатаційні витрати для комп'ютерної системи складуть $C_п$=953705 грн., для існуючого проекту: $C_і$=1524598 грн.

Річна економія на експлуатаційних витратах становить:

$$\Delta C = C_і - C_п, \quad (6.23)$$

где $C_п$ та $C_і$ – експлуатаційні витрати на зміст проектної та існуючої систем відповідно, грн.

$\Delta C = 1524598 – 953705 = 570893$ грн.

Термін окупності (Тр) проектованої системи:

$$T_р = K_{пр}/ \Delta C, \text{ лет} \quad (6.24)$$

$T_р = 967918 / 570893 = 1,7$ року

Отже, капітальні витрати на впровадження проектної системи окупляться через 1,7 року за рахунок скорочення працівників.

Коефіцієнт ефективності капітальних витрат визначається за формулою:

$$К_{эфф} = 1/ Т_р, \text{ грн.} \quad (6.25)$$

$К_{эфф}$ =1/1,7=0,59 грн.

Отже, на 1 грн. капітальних витрат припадає 0,59 грн. прибутку.

Висновок

Удосконалення комп'ютерної система правління підприємства ПГОК з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі доцільно, так як при капітальних витратах в 967918 грн. річна економія експлуатаційних витрат складе 570893 грн., а капіталовкладення окупляться за рахунок загальної економії від впровадження об'єкта проектування через 1,7 року. Коефіцієнт ефективності капітальних витрат дорівнює 0,59 грн. при мінімальному терміні експлуатації в 5 років.

Таким чином, комп’ютерна система є економічно вигідною.

7 ОХОРОНА ПРАЦІ, ПРОМИСЛОВА БЕЗПЕКА ТА ЦИВІЛЬНИЙ ЗАХИСТ

У дипломній роботі розглядається комп'ютерна система правління підприємства ПГОК з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі. На підприємствах гірничо-збагачувального комплексу передбачаються технічні та організаційні заходи, що забезпечують чистоту приміщень, безпеку персоналу, безпечну роботу устаткування, безпеку протікання технологічних процесів. Ці заходи спрямовані на захист персоналу в небезпечних зонах. У цих зонах діють постійно або періодично небезпечні для життя або здоров'я фактори: електромагнітні, теплові або інші випромінювання, підвищені шуми, підвищена вологість, запиленість, в тому числі пилом органічного походження, хвороботворні мікроорганізми.

Елементи комп’ютерної мережі розташовані на території виробничого комплексу у адміністративних приміщеннях. Таким чином, об'єктом для аналізу небезпечних і шкідливих факторів взяті робочі міста робітників керуючої структури з урахуванням праці за персональним комп'ютером.

7.1 Аналіз шкідливих і небезпечних вражаючих факторів

У приміщеннях адміністративних будівель на працівника можуть впливати небезпечні і шкідливі виробничі фактори, які вказані в таблиці 7.1.

Таблиця 5.1 – Аналіз шкідливих і небезпечних вражаючих факторів

№ п/п	Найменування ШНВФ	Джерела ШНВФ	Нормуючий документ
1	Специфічний характер зорової роботи; вимушена локалізована поза	Монітор, робоче місце оператора ПЕОМ	СанПин 2.2.2/2.4.1340-03
2	Недостатня освітленість робочої зони	Робоче місце оператора	СНіП II-4-79

Продовження таблиці 5.1

3	Патогенні мікроорганізми	Устаткування технологічної лінії	ДЕСТ 12.1.007-76.
4	Підвищений рівень шуму і вібрації на робочому місці	Персональний комп'ютер, периферійні пристрої, устаткування технологічної лінії	ДЕСТ 12.1.003-85.
5	Тепловиділення від устаткування	Персональний комп'ютер, периферійні пристрої	СанПиН 2.2.4.548-96
6	Можливість ураження електричним струмом	Електропроводка, блок живлення персонального комп’ютера	ДЕСТ 12.1.038-82. 82

7.2 Інженерно-технічні заходи з охорони праці

7.2.1 Заходи по боротьбі з шкідливими факторами при роботі з персональним комп'ютером

У штатному режимі робота ведеться з ПК. В даному випадку робітник схильний до впливу напруги зору. Робітник повинен постійно працювати у текстових та графічних редакторах за монітором. Все це призводить до підвищеного стомлення зору і загального стомлення

Необхідно дотримуватися таких правил при облаштуванні робочого місця робітника. Дисплей розміщується на столі так, щоб відстань від очей до екрана коливалося в межах 40-80 см, при цьому кут між нормаллю до центра екрана і горизонтальною лінією погляду повинен становити 20º. У горизонтальній площині кут спостереження екрана не повинен перевищувати 60º. Розмір монітора повинен бути не менше 15 ", при цьому висота символів текстових позначень і повідомленя на екрані складе не менше 3,8 мм. Клавіатура розміщується на висувній підставці столу так, щоб висота розташування клавіатури щодо статі становила 65 см. Кут нахилу клавіатури до горизонтальної плокості 15º. Основне положення підставки клавіатури - закрите. Паперові документи (довідкові, а також для записів і позначок)

маємо на столі АРМ перед монітором, при цьому кут між екраном дисплея і документом в горизонтальним площині повинен складати 30-40º.

Щоб освітлення не створювало сліпучих відблисків, комп'ютер повинен бути розташований так, щоб пряме світло не попадало на екран

Площа на одне робоче місце має становити не менше 6 $м^2$, об'єм - не менше 20 $м^3$.

Для організації робочого місця робітника застосовується звичайний офісний стіл двотумбовий марки 2СД160.

Для робочих місць використовувати обертові офісні крісла з регулюванням висоти. Оздоблення - гігієнічна м'яка з штучної шкіри.

Кімната для розміщення робітників повинна висвітлюватися природно, вікна повинні бути звернені на північ або північний схід. При розташуванні вікон на південь використовувати жалюзі.

Для зниження зорового і загального стомлення необхідно вибрати оптимальний режим праці та відпочинку персоналу.

У добре освітленому і вільному доступу допуск до місць кімнат робітників вивісити стенд з описом режиму праці та відпочинку персоналу, а також комплексів вправ загальнофізичної та для зняття зорової напруги, розроблених відділом охорони праці підприємства.

7.2.2 Освітлення робочої зони

На виробництві в приміщеннях працівників використовується поєднане природне і штучне освітлення. Згідно СНиП 23.05-95 – середня точність зорової роботи, найменший розмір об'єкта розрізнення складає 0,3÷0,5 мм.

Штучне освітлення може бути двох систем – загальне і комбіноване. В приміщеннях адміністративних робітників використана система комбінованого освітлення, тобто до загального освітлення додано місцеве, створюване світильниками, концентрує світловий потік безпосередньо на робочих місцях.

Для освітлення приміщення використані, найбільш економічні люмінесцентні лампи типу ЛБ. Для місцевого освітлення використані лампи розжарювання.

На робочому місці відсутні різкі тіні.

Для внутрішнього оздоблення інтер'єру приміщень з ВДТ і ПЕОМ використані дифузійно-відбивні матеріали з коефіцієнтами відбиття світла для стелі 0,7÷0,8; для стін 0,5÷0,6; для підлоги 0,3÷0,5.

7.2.3 Заходи щодо захисту від пилу

Виробничий процес пов'язаний підприємства пов’язано з підвищеною запиленістю, тому не рідше 1 разу на добу проводиться вологе прибирання приміщень робітників.

Додатково, системи вентиляції будівель забезпечуються змінними фільтрами класу G4.

7.2.4 Заходи щодо захисту від шуму і вібрації

АРМ робітників організовано на відстані від основного виробництва і не потребує застосування додаткових заходів по захисту від шуму і вібрації. У самих приміщеннях рівень шуму не перевищує звуковий тиск у 75 дБА в діапазоні від 16 до 20000 Гц.

7.2.5 Заходи щодо захисту від підвищеної температури

При виконанні робіт за комп’ютерною технікою, пов'язаних з нервово-емоційним напруженням в приміщеннях повинні дотримуватися оптимальні умови мікроклімату (температура повітря 22 - 24 °С, відносна вологість 60 - 40%, швидкість руху повітря не більше 0,1 м/сек.).

Кімната робітників повинна бути обладнана власною системою вентиляції та кондиціонування на базі спліт-системи продуктивністю 510 $м^3$/год, яка стабілізує температуру повітря в регульованих межах 14 ... 32 ± 2ºС.

7.2.6 Заходи щодо забезпечення електробезпеки

Відповідно до класифікації ПУЕ за небезпекою ураження електричним струмом приміщення с оргтехнікою відноситься до приміщень з підвищеною небезпекою, так як існує можливість одночасного дотику до опалювальних батарей приміщення, з'єднаних з землею і корпусів електрообладнання. В приміщеннях

використовується обладнання з напругою живлення 220 В. Лінія електромережі для живлення ПЕОМ та периферійного обладнання виконується як окрема групова трьохпровідна мережа шляхом прокладки фазного і нульового робочого та захисного провідників. Нульовий захисний провідник служить для занулення електроприймачів. При напрузі до 1000 В застосовують трьохпровідну мережу з ізольованою нейтраллю.

Струмовий захист реалізується з використанням автоматів, які розривають електричну мережу при високих струмах навантаження. Для забезпечення захисного відключення використовуємо УЗО ВД1-63, основним призначенням якого є забезпечення безпеки людини в разі дотику до зануленого (заземленого) корпусу при замиканні на нього фази, а також при безпосередньому дотику до струмоведучих частини електроустановки. Електропроводка в приміщеннях повинна бути виконана прихованим методом, прокладена в гнучких металоруковах або кабельканалах, що робить силові ланцюги недоступними для працюючих.

Основні заходи, спрямовані на попередження випадків ураження електричним струмом в операторській, такі:

- щодня проводити очистку монітора від пилу;
- забороняється знімати захисну кришку системного блоку комп'ютера;
- усунення можливості випадкового дотику до струмоведучих частин електроустаткування, що знаходиться під напругою;
- малі напруги;
- надійна ізоляція струмоведучих частин електрообладнання і своєчасний його ремонт;
- захисне занулення;
- захисне відключення та застосування плавких запобіжників.

Контроль і профілактику ізоляції здійснювати при приймально-здавальних випробуваннях. Періодично контроль ізоляції проводити після монтажу в терміни встановлені правилами або в разі виявлення дефектів. Застосувати додаткові засоби захисту: діелектричні килимки, калоші, рукавички, діелектричні прокладки.

7.3 Пожежна профілактика

Приміщення ділянки по пожежної безпеки відноситься до категорії Г – негорючі речовини і матеріали в гарячому, розпеченому або розплавленому стані, процес обробки яких супроводжується виділенням променистого тепла, іскор і полум'я; горючі гази, рідини і тверді речовини, які спалюються або утилізуються як паливо. Приміщення адміністративних будівель оператора з вибухопожежної безпеки відноситься до категорії В - горючі і важко горючі рідини, тверді горючі і важко горючі речовини і матеріали, здатні при взаємодії з водою, киснем повітря або один з одним тільки горіти.

Вогнестійкість приміщення визначається по таблиці меж вогнестійкості будівельних конструкцій. Для приміщень адміністративних будівель вона становить Г1, для кімнати оператора - Г2.

Згідно правил протипожежної безпеки, територія приміщень повинна постійно утримуватися в чистоті, сміття систематично збирати на спеціально відведені ділянки. Куріння і застосування відкритого вогню в приміщеннях категорично забороняється, про що на видимих місцях необхідно вивісити чіткі написи. Куріння допускається тільки в спеціально відведеному місці на території підприємства.

Приміщення ділянки має мати запасний вихід.

Необхідно дотримуватися протипожежні норми при влаштуванні опалення та вентиляції, виборі та монтажу електрообладнання. Проходи, основні і запасні виходи повинні постійно утримуватися в справному стані, не захаращуватися, а в нічний час освітлюватися. У вентиляційній системі передбачити пристрої, що перегороджують при виникненні пожежі можливість поширення вогню в інші приміщення. Для швидкого виклику пожежної служби підприємства в разі виникнення пожежі, в приміщеннях встановити телефонний, зв'язок. До всіх засобів зв'язку забезпечити вільний доступ в будь-який час доби. Для подачі сигналу пожежної тривоги на території вузла зв'язку встановити спеціальні установки (сирени). Весь пожежний інвентар, протипожежне обладнання та первинні засоби пожежогасіння необхідно утримувати в справному стані, перебувати на видному місці і до них повинен бути забезпечений безперешкодний доступ в будь-який час

доби. Всі станційні та переносні засоби пожежогасіння періодично перевіряти і випробовувати.

Виходячи з категорії Г з пожежної безпеки необхідно встановити по одному ручному вогнегаснику ОП-5 у кожній кімнаті будівлі з оргтехнікою. Додатково встановити один пожежний щит до складу якого входять два вуглекислотних вогнегасники ОУ-5. Всі вогнегасники розташовані в легкодоступних місцях. Щит розташувати в безпосередній близькості від запасного виходу.

7.4 Заходи з ергономіки

Дослідження оцінки соціально-економічної ефективності впровадження ергономіки підтверджують, що ергономічні заходи дають від 2 до 5% підвищення продуктивності праці. Впровадження такого підходу для робочих місць підприємство повинно забезпечити.

Робоче місце робітника з ПК – це частина простору, в якому працівник здійснює трудову діяльність, і проводить велику частину робочого часу. Робоче місце, добре пристосоване до трудової діяльності працівника, правильно і доцільно організоване, у відношенні простору, форми, розміру забезпечує йому зручне положення при роботі і високу продуктивність праці при найменшому фізичному і психічному напрузі.

На робочому місці повинні бути передбачені заходи захисту від можливого впливу небезпечних і шкідливих факторів виробництва. Рівні цих факторів не повинні перевищувати граничних значень, обумовлених правовими, технічними і санітарно-технічними нормами. Ці нормативні документи зобов'язують до створення на робочому місці умов праці, при яких вплив небезпечних і шкідливих чинників на працюючих або усунуто зовсім, або знаходиться в допустимих межах.

Забарвлення приміщень і меблів повинна сприяти створенню сприятливих умов для зорового сприйняття, гарного настрою. У службових приміщеннях, в яких виконується одноманітна розумова робота, що потребує значної нервової напруги і великого зосередження, фарбування повинна бути спокійних тонів - малонасичені відтінки холодного зеленого або блакитного кольорів.

Робоче місце і взаємне розташування всіх його елементів повинне відповідати антропометричним, фізичним і психологічним вимогам. Велике значення має також характер роботи. Зокрема, при організації робочого місця робітника з ПК повинні бути дотримані наступні основні умови:

- оптимальне розміщення устаткування, що входить до складу робочого місця;
- достатній робочий простір, що дозволяє здійснювати всі необхідні рухи і переміщення;
- необхідно природне і штучне освітлення для виконання поставлених завдань;
- рівень акустичного шуму не повинен перевищувати допустимого значення.

Головними елементами робочого місця робітника з ПК є письмовий стіл і крісло. Основним робочим положенням є положення сидячи. конструкція робочого стільця (крісла) повинна забезпечувати підтримку раціональної робочої пози під час роботи на ПК. Робочий стілець (крісло) повинен бути підйомно-поворотним і регульованим по висоті і кутам нахилу сидіння і спинки, а також відстані спинки від переднього краю сидіння.

Конструкція робочого столу повинна забезпечувати оптимальне розміщення на робочій поверхні використовуваного обладнання з урахуванням його кількості і конструктивних особливостей (розмір ПК, клавіатури та ін.), Характеру виконуваної роботи.

ВИСНОВКИ

У даній роботі проведено аналіз об’єкту за для проектування нової мережі підрозділу підприємства та розробити специфікацію апаратних засобів комп’ютерної системи, у тому числі засобів збору та передачі даних. Виконати вибір відповідного фізичного середовища, кабелів, портів і з'єднувачів для підключення мережевих пристроїв до інших пристроїв мережі і вузлів, вибір мережевих пристроїв і компонентів, необхідних для задоволення технічних вимог мережі і аналітичні розрахунки споживаної потужності, об’ємів і швидкостей передачі даних каналами мережі з урахуванням вибраних апаратних засобів, затримок на обробку даних на вузлах мережі.

Виконана розробка комп'ютерної системи правління підприємства ПГОК з детальним опрацюванням побудови, налаштування та безпеки корпоративної мережі на основі мережевого обладнання Cisco™ для основних мережевих вузлів.

Виконано розрахунок налаштувань для заданої топології мережі, обрано інтерфейси каналів зв’язку та протоколи обміну, розрахована топологічна схема комп’ютерної системи, розраховані налаштування маршрутизації комп’ютерної мережі, а також виконане подальше моделювання і перевірка роботи комп’ютерної системи.

ПЕРЕЛІК ПОСИЛАНЬ

1. ДСТУ 3008-2015. Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання. – К.: Держстандарт, 1998. – 37 с.

2. Положення про організацію атестації здобувачів вищої освіти НТУ «Дніпровська політехніка» / М-во освіти і науки України, Нац. техн. ун-т. – Д. : НТУ «ДП», 2018. – 40 с

3. ДСТУ ГОСТ 7.1:2006. Бібліографічний запис, бібліографічний опис. Загальні вимоги та правила складання: метод. рекомендації з впровадження / Уклали: Галевич О. К., Штогрин І. М. – Львів, 2008. – 20 с.

4. ГОСТ 34.602-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы. – М.: Госстандарт, 1992. – 54 с.

5. ГОСТ 19.701-90. ЕСПД. Единая система программной документации. Схема алгоритмов, программ, данных и систем. Обозначения условные и правила выполнения. – М.: Госстандарт, 1990. – 128 с.

6. Воробьёва Н.И., Корнейчук В.И., Савчук Е.В. Надёжность компьютерных систем. – К.: «Корнійчук», 2002. – 144 с.

7. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2001. – 172 с.

8. Цвіркун Л.І. Розробка програмного забезпечення комп’ютерних систем. Програмування: навч. посіб. [Електронний ресурс] / Л.І. Цвіркун, А.А. Євстігнєєва, Я.В. Панферова ; під заг. ред. проф. Л.І. Цвіркуна ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – 1 електрон. опт. диск (CD-ROM) ; 12 см. – Систем. вимоги (мінімальні): Процесор 32-розрядний (x86) 233 МГц ; 512 МБ RAM ; 128 МБ Video ; від 4-х до 48-х CD-ROM ; Windows 7. – Назва з контейнера. – Дніпро: НТУ «ДП», 2019. – ISBN 978-966-350-638–8.

9. Цвіркун Л.І. Інженерна та комп'ютерна графіка. AutoCAD : навч. посіб. / Л.І. Цвіркун, Л.В. Бешта ; під. заг. ред. Л.І. Цвіркуна ; М-во освіти і науки України, НТУ “Дніпровська політехніка”. – Дніпро: НТУ “ДП” , 2018. – 209 с. – ISBN 978-966-350-663-0.

10. Цвіркун, Л.І. Розробка програмного забезпечення комп’ютерних систем. Програмування: навч. посібник / Л.І. Цвіркун, А.А. Євстігнєєва, Я.В. Панферова, під заг. ред. Л.І. Цвіркуна. – 3-є вид., випр. – Д.: Національний гірничий університет, 2016. – 223 с. – ISBN 978-966-350-595-4.

11. Цвіркун Л.І. Глобальні комп’ютерні мережі. Програмування мовою PHP: навч. посібник / Л.І. Цвіркун, Р.В. Липовий, під заг. ред. Л.І. Цвіркуна. – Д.: Національний гірничий університет, 2013. – 239 с. – ISBN 978-966-350-417-9.

12. Дипломування. Методичні вказівки для бакалаврів галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова ; М-во освіти і науки України, Нац. гірн. ун-т. – Дніпро: НГУ, 2016. – 56 с.

13. Цвіркун Л.І. Комп’ютерні мережі. Методичні рекомендації до виконання курсового проекту студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, Я.В. Панферова, Л.В. Бешта ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – 28 с.

14. Цвіркун Л.І. Комп’ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч. 1. – 60 с.

15. Цвіркун Л.І. Комп’ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова ; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч. 2. – 39 с.

Додаток А

Текст програми
налаштування комп’ютерної мережі підприємства

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ДНІПРОВСЬКА ПОЛІТЕХНІКА»

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП'ЮТЕРНОЇ СИСТЕМИ

Текст програми

804.02070743.20005-01 12 01

Листів 20

2020

АНОТАЦІЯ

Даний документ містить ПЗ налаштувань роутерів та комутаторів Cisco для структурної схеми моделі комп’ютерної системи, розробленої за варіантом завдання дипломної роботи.

Текст програми реалізований на мові конфігураційних скриптів для мережного обладнання Cisco.

Середовище розробки та налагодження скриптів – пакет моделювання мереж Packet Tracer 7 в середовищі операційної системи Windows 10.

ЗМІСТ

ТЕКСТ ПРОГРАМИ

Minenko_R2_startup-configversion 15.1

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
hostname Minenko_R2
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
ip dhcp excluded-address 172.16.68.1 172.16.68.10
ip dhcp excluded-address 172.16.68.33 172.16.68.43
ip dhcp excluded-address 172.16.68.65 172.16.68.75
ip dhcp excluded-address 172.16.68.97 172.16.68.107
ip dhcp pool POOL_VLAN19
 network 172.16.68.32 255.255.255.224
 default-router 172.16.68.33
 dns-server 172.16.69.139
ip dhcp pool POOL_VLAN29
 network 172.16.68.64 255.255.255.224
 default-router 172.16.68.65
 dns-server 172.16.69.139
ip dhcp pool POOL_VLAN39
 network 172.16.68.96 255.255.255.224
 default-router 172.16.68.97
 dns-server 172.16.69.139
aaa new-model
```

```
aaa authentication login Login group radius local
aaa authentication login default local
no ip cef
no ipv6 cef
username 12317_Minenko password 7 082048430017061E010803
license udi pid CISCO2911/K9 sn FTX1524I34V-
no ip domain-lookup
ip domain-name Minenko_R2
spanning-tree mode pvst
interface GigabitEthernet0/0
 ip address 10.0.9.2 255.255.255.252
 duplex auto
 speed auto
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
interface GigabitEthernet0/1.19
 encapsulation dot1Q 19
 ip address 172.16.68.33 255.255.255.224
interface GigabitEthernet0/1.29
 encapsulation dot1Q 29
 ip address 172.16.68.65 255.255.255.224
interface GigabitEthernet0/1.39
 encapsulation dot1Q 39
```

```
 ip address 172.16.68.97 255.255.255.224
interface GigabitEthernet0/1.99
 encapsulation dot1Q 99
 ip address 172.16.68.1 255.255.255.224
interface GigabitEthernet0/2
 ip address 10.0.9.5 255.255.255.252
 duplex auto
 speed auto
interface Serial0/0/0
 no ip address
 clock rate 2000000
 shutdown
interface Serial0/0/1
 no ip address
 clock rate 2000000
 shutdown
interface Serial0/1/0
 no ip address
 clock rate 2000000
 shutdown
interface Serial0/1/1
 no ip address
 clock rate 2000000
 shutdown
interface Vlan1
```

```
 no ip address
 shutdown
router ospf 9
 log-adjacency-changes
 redistribute static
 passive-interface GigabitEthernet0/1.19
 passive-interface GigabitEthernet0/1.29
 passive-interface GigabitEthernet0/1.39
 passive-interface GigabitEthernet0/1.99
 network 172.16.68.0 0.0.0.255 area 0
 network 10.0.9.0 0.0.0.3 area 0
 network 10.0.9.4 0.0.0.3 area 0
 default-information originate
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1
ip flow-export version 9
no cdp run
banner motd    123sk-16 Minenko This area have PASSword
radius-server host 172.16.69.139 auth-port 1645
radius-server key radius123
line con 0
 password 7 0822455D0A16
line aux 0
line vty 0 4
 password 7 0822455D0A16
```

```
 login authentication default
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 transport input ssh
end
```

Minenko_R3_startup-config

```
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
hostname Minenko_R3
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
ip dhcp excluded-address 172.16.69.1 172.16.69.10
ip dhcp pool POOL_LAN_Bud3
 network 172.16.69.0 255.255.255.128
 default-router 172.16.69.1
 dns-server 172.16.69.139
aaa new-model
aaa authentication login Login group radius local
aaa authentication login default local
no ip cef
no ipv6 cef
license udi pid CISCO2911/K9 sn FTX152475A0-
```

```
license boot module c2900 technology-package securityk9
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
crypto isakmp key cisco address 64.100.13.2
crypto ipsec transform-set VPN-CONF esp-3des esp-sha-hmac
crypto map VPN-MAP 10 ipsec-isakmp
 description VPN connection to Minenko_R0
 set peer 64.100.13.2
 set transform-set VPN-CONF
 match address 110
no ip domain-lookup
ip domain-name Minenko_R3
spanning-tree mode pvst
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
interface GigabitEthernet0/1
 description Bud3
 ip address 172.16.69.1 255.255.255.128
 ip nat inside
 duplex auto
```

```
 speed auto
interface GigabitEthernet0/2
 description R2.2
 ip address 10.0.9.6 255.255.255.252
 ip nat inside
 duplex auto
 speed auto
 crypto map VPN-MAP
interface Serial0/0/0
 description WAN IPS
 bandwidth 128
 ip address 209.165.202.2 255.255.255.224
 ip ospf cost 7500
 ip nat outside
 clock rate 128000
interface Serial0/0/1
 description WAN R4
 bandwidth 128
 ip address 10.0.9.17 255.255.255.252
 ip ospf cost 7500
 ip nat inside
 clock rate 128000
interface Serial0/1/0
 no ip address
 clock rate 2000000
```

```
 shutdown
interface Serial0/1/1
 no ip address
 clock rate 2000000
 shutdown
interface Vlan1
 no ip address
 shutdown
router ospf 9
 log-adjacency-changes
 passive-interface GigabitEthernet0/1
 network 172.16.69.0 0.0.0.127 area 0
 network 10.0.9.4 0.0.0.3 area 0
 network 10.0.9.16 0.0.0.3 area 0
 network 209.165.202.0 0.0.0.31 area 0
 default-information originate
ip nat pool Internet 209.165.202.5 209.165.202.30 netmask 255.255.255.224
ip nat inside source list 9 pool Internet
ip nat inside source static 172.16.69.139 209.165.200.5
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.202.1
ip route 172.16.68.0 255.255.252.0 GigabitEthernet0/1
ip flow-export version 9
access-list 9 permit 172.16.68.0 0.0.3.255
access-list 110 permit ip 172.16.69.0 0.0.0.127 172.16.70.0 0.0.0.31
```

no cdp run

banner motd 123sk-16 Minenko This area have PASSword

radius-server host 172.16.69.139 auth-port 1645

radius-server key radius123

line con 0

 password 7 0822455D0A16

line aux 0

line vty 0 4

 password 7 0822455D0A16

 login authentication default

 transport input ssh

line vty 5 15

 password 7 0822455D0A16

 transport input ssh

end

Minenko_Sw1.1_startup-config

version 12.2

no service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption

hostname Minenko_Sw1.1

enable secret 5 1mERr$hx5rVt7rPNoS4wqbXKX7m0

ip domain-name SW_Minenko1.1

username 12317_Minenko privilege 1 password 7 082048430017061E010803

```
spanning-tree mode pvst
spanning-tree extend system-id
interface FastEthernet0/1
 switchport trunk native vlan 100
 switchport trunk allowed vlan 19,29,39,99
 switchport mode trunk
interface FastEthernet0/2
 shutdown
interface FastEthernet0/3
 shutdown
interface FastEthernet0/4
 switchport access vlan 19
 switchport mode access
interface FastEthernet0/5
 switchport access vlan 19
 switchport mode access
interface FastEthernet0/6
 switchport access vlan 19
 switchport mode access
interface FastEthernet0/7
 switchport access vlan 19
 switchport mode access
interface FastEthernet0/8
 switchport access vlan 19
 switchport mode access
```

```
interface FastEthernet0/9
 shutdown
interface FastEthernet0/10
 switchport access vlan 29
 switchport mode access
interface FastEthernet0/11
 switchport access vlan 29
 switchport mode access
interface FastEthernet0/12
 switchport access vlan 29
 switchport mode access
interface FastEthernet0/13
 switchport access vlan 29
 switchport mode access
interface FastEthernet0/14
 switchport access vlan 29
 switchport mode access
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security violation restrict
interface FastEthernet0/15
 switchport access vlan 39
 switchport mode access
interface FastEthernet0/16
```

```
 switchport access vlan 39
 switchport mode access
interface FastEthernet0/17
 switchport access vlan 39
 switchport mode access
interface FastEthernet0/18
 switchport access vlan 39
 switchport mode access
interface FastEthernet0/19
 switchport access vlan 39
 switchport mode access
interface FastEthernet0/20
 switchport access vlan 39
 switchport mode access
interface FastEthernet0/21
 shutdown
interface FastEthernet0/22
 shutdown
interface FastEthernet0/23
 shutdown
interface FastEthernet0/24
 shutdown
interface GigabitEthernet0/1
 switchport trunk native vlan 100
 switchport trunk allowed vlan 19,29,39,99-100
```

```
 switchport mode trunk
interface GigabitEthernet0/2
interface Vlan1
 no ip address
 shutdown
interface Vlan99
 description LAN Bud1_99
 mac-address 00d0.973b.1a01
 ip address 172.16.68.2 255.255.255.224
ip default-gateway 172.16.68.1
banner motd    123sk-16 Minenko This area have PASSword
line con 0
 password 7 0822455D0A16
 login
line vty 0 4
 password 7 0822455D0A16
 login local
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 login local
 transport input ssh
end
```

Minenko_Sw1.2_startup-config

```
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
hostname Minenko_Sw1.2
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
ip domain-name _SW_Minenko1.2
username 12317_Minenko privilege 1 password 7 082048430017061E010803
spanning-tree mode pvst
spanning-tree extend system-id
interface FastEthernet0/1
 switchport trunk native vlan 100
 switchport trunk allowed vlan 19,29,39,99
 switchport mode trunk
interface FastEthernet0/2
 shutdown
interface FastEthernet0/3
 shutdown
interface FastEthernet0/4
 switchport access vlan 19
 switchport mode access
interface FastEthernet0/5
 switchport access vlan 19
 switchport mode access
```

```
interface FastEthernet0/6
 switchport access vlan 19
 switchport mode access
interface FastEthernet0/7
 switchport access vlan 19
 switchport mode access
interface FastEthernet0/8
 switchport access vlan 19
 switchport mode access
interface FastEthernet0/9
 shutdown
interface FastEthernet0/10
 switchport access vlan 29
 switchport mode access
interface FastEthernet0/11
 switchport access vlan 29
 switchport mode access
interface FastEthernet0/12
 switchport access vlan 29
 switchport mode access
interface FastEthernet0/13
 switchport access vlan 29
 switchport mode access
interface FastEthernet0/14
 switchport access vlan 29
```

```
 switchport mode access
interface FastEthernet0/15
 switchport access vlan 39
 switchport mode access
interface FastEthernet0/16
 switchport access vlan 39
 switchport mode access
interface FastEthernet0/17
 switchport access vlan 39
 switchport mode access
interface FastEthernet0/18
 switchport access vlan 39
 switchport mode access
interface FastEthernet0/19
 switchport access vlan 39
 switchport mode access
interface FastEthernet0/20
 switchport access vlan 39
 switchport mode access
interface FastEthernet0/21
 shutdown
interface FastEthernet0/22
 shutdown
interface FastEthernet0/23
 shutdown
```

```
interface FastEthernet0/24
 shutdown
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface Vlan1
 no ip address
 shutdown
interface Vlan99
 description LAN Bud1_99
 mac-address 0001.9693.6301
 ip address 172.16.68.3 255.255.255.224
ip default-gateway 172.16.68.1
banner motd    123sk-16 Minenko This area have PASSword
line con 0
 password 7 0822455D0A16
 login
line vty 0 4
 password 7 0822455D0A16
 login local
 transport input ssh
line vty 5 15
 password 7 0822455D0A16
 login local
 transport input ssh
end
```