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

Навчально-науковий
інститут електроенергетики
(інститут)
Факультет інформаційних технологій
(факультет)
Кафедра інформаційних технологій та комп'ютерної інженерії
(повна назва)

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи ступеня бакалавра
(бакалавра, спеціаліста, магістра)

студента Булата Павла Павловича
(ПІБ)

академічної групи 123-20ск-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 служби таксі Opti з реалізацією побудови та налаштування корпоративної мережі»
(назва за наказом ректора)

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	Проф. Олевський В.І.			
розділів:				
розробка апаратної частини	доц. Ткаченко С.М.			
розробка корпоративної мережі	ас. Бешта Л.В.			
Рецензент	Проф. Лактіонов І.С.			
Нормоконтролер	проф. Цвіркун Л.І.			

Дніпро 2023

ЗАТВЕРДЖЕНО:

завідувач кафедри
інформаційних систем
та комп'ютерних технологій
(повна назва)
_____ Гнатушенко В.В.
(підпис) (прізвище, ініціали)
« » 2023 року

ЗАВДАННЯ

на кваліфікаційну роботу ступеня бакалавр

студента Булат П.П. **академічної групи** 123-20ск-1
(прізвище та ініціали) (шифр)

спеціальності 123 Комп'ютерна інженерія

за освітньо-професійною програмою 123 Комп'ютерна інженерія
(офіційна назва)

на тему «Комп'ютерна система служби таксі Opti з реалізацією побудови та налаштування корпоративної мережі»

затверджену наказом ректора НТУ «Дніпровська політехніка» від 16.05.2023 № 350-с

Розділ	Зміст	Термін виконання
Стан питання та постановка завдання	На основі матеріалів виробничих практик, інших науково-технічних джерел конкретизується предмет та мету роботи та виконується постанова завдання	10.05.2023
Розробка апаратної частини	На основі аналізу підприємства формулюються технічні вимоги до комп'ютерної системи та розробляється апаратна частина системи	17.05.2023
Розробка корпоративної мережі	Виконується розрахунок налаштувань корпоративної мережі та перевірка роботи системи, розробляються методи та налаштування обладнання для захисту інформації в системі	24.05.2023

Завдання видано _____ проф. Олевський В.І.
(підпис керівника) (прізвище, ініціали)

Дата видачі 19.04.2023

Дата подання до екзаменаційної комісії 06.07.2023

Прийнято до виконання _____ Булат П.П.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка містить: 57 ст., 6 рис., 9 табл., 1 дод., 8 джерел.

VPN, КОМП’ЮТЕРНА МЕРЕЖА, LAN, VLAN, REST, HTTP

Об’єкт: комп’ютерна система та комп'ютерної інженерії з реалізацією побудови та налаштування корпоративної мережі.

Мета: створення комп’ютерної системи служби таксі “Opti” з реалізацією побудови та налаштування корпоративної мережі.

Система побудована на основі принципів відкритості її архітектури, що дозволяє здійснювати технічну і програмну її модернізацію. Компанія складається з 5 основних відділів: управління верхнього рівня, диспетчерського центру, транспортного відділу, відділу кадрів та фінансового відділу.

Розробка комп’ютерної мережі виконана відповідно до завдання на кваліфікаційну 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

ЗМІСТ

РЕФЕРАТ 3
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ 6
ВСТУП 7
1.СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ 8
1.1 Загаліні відомості про підприємство. 8
1.2 Загальна характеристика галузі та умови застосування комп`ютерної системи, що проектується. 9
1.3 Організація комп`ютерної мережі підприємства та топологічне розміщення структурних підрозділів підприємства. 10
1.4 Відомості про технології збору та передачі інформації. 14
1.5 Види та конфігурація обладнання, що використовується в компанії. 15
1.6 Аналітичний огляд існуючих способів обробки та передачі інформації, принципів побудови об`єкта проектування, відомих рішень у галузі. 17
1.7 Завдання і мета роботи. 17
1.8 Визначення можливих напрямків рішення поставлених завдань. 18
2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП'ЮТЕРНОЇ СИСТЕМИ ..18
2.1. Вимоги до системи в цілому 18
2.1.1 Вимоги до структури і функціонування системи 18
2.1.2 Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами системи 19
2.1.3 Вимоги до сумісності з суміжними системами 19
2.1.4 вимоги до діагностування системи 20
2.1.5 Перспективи розвитку системи 20
2.1.6 Вимоги до чисельності і кваліфікації персоналу, що обслуговує систему, і режиму його роботи. 20
2.1.7 Вимоги до показників призначення 21
2.1.8 Вимоги до надійності системи 21
2.1.9 Вимоги до експлуатації, технічного обслуговування, ремонта і збере-ження 22
2.1.10 Вимоги до ергономіки та технічної естетики 22
2.1.11 Вимоги до захисту інформації від несанкціонованого доступу 23
2.1.12 Вимоги до патентної чистоти 23

2.1.13 Вимоги до уніфікації та стандартизації....23
2.2 Вимоги до функцій, які виконуються системою 24
2.2.2 Вимоги до інформаційного забезпечення підсистем 24
2.2.3 Вимоги до математичного забезпечення підсистем....25
2.2.4 Вимоги до програмного забезпечення....26
2.2.5 Вимоги до методичного забезпечення....27
3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ 34
3.1 Розрахунок схеми адресації корпоративної мережі 34
3.2 Налаштування та перевірка роботи комп'ютерної системи 35
3.2.1 Базове налаштування конфігурації пристроїв 35
3.2.2 Налаштування маршрутизаторів корпоративної мережі 36
3.2.3 Налаштування роботи Інтернет....36
3.2.4 Налаштування агрегування каналів....37
3.3 Захист інформації в комп`ютерній системі від несанкціонованого доступу 38
3.3.1 Розробка методів для захисту інформації в комп'ютерній системі....38
3.3.2 Налаштування маршрутизаторів на підтримку служби AAA 39
3.3.3 Налаштування мереж VLAN 40
3.3.4 Налаштування параметрів безпеки комутаторів 42
3.3.5 Налаштування віртуальної приватної мережі site-to-site VPN з використанням IPsec....43

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

КС – комп'ютерна система.

VLAN – (Virtual Local Area Network) топологічна локальна комп'ютерна мережа.

ACL – (Access Control List) список управління доступом, який визначає, хто або що може отримувати доступ до об'єкта.

DHCP – (Dynamic Host Configuration Protocol) мережевий протокол, що дозволяє мережевим пристроям автоматично отримувати IP-адресу та інші параметри.

PAT – (Port Address Translation) перетворення адрес портів**.**

NAT – (Network Address Translation) перетворення мережевих адрес.

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

WAN − глобальна мережа;

IP-адреса − унікальний ідентифікатор комп'ютера локальної мережі;

LAN − локальна обчислювальна мережа, ЛВС;

Cisco Packet Tracer − багатофункціональна програма моделювання мереж;

ВСТУП

У сучасному світі, що швидко розвивається, комп'ютерні системи стали невід'ємною частиною нашого повсякденного життя. Від великих підприємств до малого бізнесу комп'ютерні системи відіграють вирішальну роль в оптимізації операцій, підвищенні продуктивності та забезпеченні безперебійного спілкування. Оскільки технологія продовжує розвиватися, зростає потреба в розробці передових комп'ютерних систем, які можуть задовольнити зростаючі вимоги сучасних організацій.

Розробка комп'ютерних систем охоплює проектування, створення, впровадження та обслуговування інтегрованих систем, які забезпечують ефективну обробку даних, зберігання інформації, зв'язок і прийняття рішень. Він передбачає системний та ітераційний підхід, який враховує конкретні вимоги, цілі та обмеження організації чи програми, для яких розробляється система. Процес розробки зазвичай включає кілька етапів, включаючи аналіз, проектування, впровадження, тестування та розгортання.

Метою цієї кваліфікаційної роботи є аналіз існуючих операцій служби таксі, визначення областей для вдосконалення та пропонування інноваційних рішень, які використовують розвиток комп'ютерної системи для вирішення унікальних завдань, з якими стикається галузь. Використовуючи сучасні методи проектування систем ця робота спрямована на створення комплексної та надійної комп'ютерної системи, яка оптимізує роботу служби таксі, оптимізує розподіл ресурсів і покращує загальний досвід обслуговування клієнтів.

1.СТАН ПИТАННЯ І ПОСТАНОВКА ЗАВДАННЯ

1.1 Загаліні відомості про підприємство.

Opti Global — українська група компаній, які надають транспортні, туристичні, охоронні послуги. Заснована 2005 року. Крім України, працює також у Польщі та Литві.

Компанія була заснована в 2005 році Петром Ковтуном під брендом «Оптимальне таксі 579». Спершу служба працювала тільки в Києві. Перший офіс знаходився в приватній квартирі, в якій приймалися і оброблялися замовлення на пасажирські і приватні перевезення.

Зона покриття служби таксі Опті.

До кінця 2000-х років мережа «Оптимальне таксі» увійшла до числа найбільших приватних перевізників у столиці та запровадила свою діяльність в інших великих містах України. У 2009 році компанія почала працювати в містах Львів і Запоріжжя, в 2010 — в м. Одеса та Дніпро, з 2011 по 2013 — в містах Івано-Франківськ, Рівне, Миколаїв.

Максимальний розвиток припав на 2014 рік: за рік філії відкрилися ще в понад 16 містах України (Житомир, Кам'янське, Луцьк, Кривий Ріг, Тернопіль, Хмельницький, Чернівці, Херсон, Біла Церква, Кропивницький, Черкаси, Буковель, Кам'янець-Подільський, Чернігів, Суми, Маріуполь).

У 2019 компанія провела масштабний ребрендинг, за результатами якого з'явилася група компаній «Opti Global» під спільним брендом «Опті» Тоді ж компанія презентувала власний додаток. У додатку є можливість замовити близько 10 окремих транспортних послуг, можливість замовлення адресної і кур'єрської доставки, а також покупки квитків на всі види залізничних, автобусних та авіа рейсів.

Станом на серпень 2021 року компанія Опті має філії в 36 містах України: Київ, Харків, Дніпро, Львів, Одеса, Бердянськ, Черкаси, Чернігів, Маріуполь, Рівне, Івано-Франківськ, Луцьк, Ужгород, Стрий, Ірпінь, Бровари, Ковель, Миколаїв, Буковель, Суми, Херсон, Хмельницький, Кривий Ріг; Кам'янське, Вінниця, Дубно,

Дрогобич, Біла Церква, Кам'янець-Подільський, Трускавець, Тернопіль, Кропивницький, Полтава, Чернівці, Запоріжжя і Житомир. Opti має власний автопарк в Києві, Дніпрі та Львові.

1.2 Загальна характеристика галузі та умови застосування комп`ютерної системи, що проектується.

Галузь таксі є важливою складовою транспортної індустрії і займається наданням послуг перевезення пасажирів за допомогою таксі.

Opti пропонує послуги таксі на замовлення, що дозволяє пасажирам замовляти транспорт за допомогою мобільного додатку або веб-сайту компанії. Крім того, Opti надає послуги таксі аеропорту та корпоративним клієнтам.

Існує кілька типів корпоративних мереж, які зазвичай використовуються організаціями, залежно від їхніх конкретних потреб і вимог до інфраструктури. Ось деякі з основних типів:

Локальна мережа (LAN): локальні мережі — це внутрішні мережі, які з'єднують пристрої в межах обмеженої географічної області, наприклад офісної будівлі чи кампусу. Локальні мережі використовуються для локального зв'язку, спільного використання ресурсів і передачі даних всередині організації. Вони часто використовують технології Ethernet або Wi-Fi.

Глобальна мережа (WAN): глобальні мережі з'єднують географічно рознесені місця, наприклад численні офісні відділення, центри обробки даних або віддалені сайти. Глобальні мережі використовують загальнодоступні або приватні телекомунікаційні мережі для забезпечення зв'язку та обміну даними на великих відстанях. У глобальних мережах зазвичай використовуються підключення до Інтернету, виділені лінії або віртуальні приватні мережі (VPN).

Столична мережа (MAN): MAN охоплює більшу географічну територію, зазвичай охоплюючи місто або столичний регіон. MAN забезпечують зв'язок між декількома локальними мережами та можуть використовуватися для з'єднання офісних відділень або підключення до постачальників послуг.

Віртуальна приватна мережа (VPN): VPN використовують протоколи шифрування та тунелювання для створення безпечних з'єднань через загальнодоступні мережі, наприклад Інтернет. VPN часто використовуються організаціями для забезпечення безпечного віддаленого доступу для співробітників або безпечного підключення віддалених офісів до корпоративної мережі.

Бездротові мережі: бездротові мережі, такі як Wi-Fi, забезпечують бездротове підключення в межах обмеженої території. Вони зазвичай використовуються в офісах або громадських місцях, щоб дозволити співробітникам або відвідувачам підключати свої пристрої до корпоративної мережі бездротовим способом.

Хмарні мережі: хмарні мережі стосуються інфраструктури та підключення, які використовуються для доступу до хмарних служб і ресурсів. Організації можуть використовувати хмарні мережі для підключення до хмарних постачальників і доступу до таких послуг, як хмарне сховище, обчислювальні ресурси або програми програмного забезпечення як послуги (SaaS).

Віртуальна локальна мережа (VLAN): VLAN — це логічні підрозділи в локальній мережі, які розділяють мережеві пристрої на окремі віртуальні мережі. VLAN дозволяють сегментувати мережу для забезпечення безпеки, керування трафіком або організаційних цілей. Пристрої в межах VLAN можуть спілкуватися один з одним наче вони підключені до однієї фізичної мережі, навіть якщо вони фізично розташовані в різних областях.

Екстранет: екстранет – це мережа, яка з'єднує організацію з іншими користувачами , такими як клієнти, постачальники або партнери. Він надає контрольований доступ до певних ресурсів або інформації для авторизованих зовнішніх користувачів, часто використовуючи такі заходи безпеки, як брандмауери та механізми автентифікації.

1.3 Організація комп`ютерної мережі підприємства та топологічне розміщення структурних підрозділів підприємства.

У службі таксі Opti корпоративна комп'ютерна мережа організована для забезпечення ефективного зв'язку, управління даними та операційного контролю.

Інфраструктура мережі:

Підключення до Інтернету: мережа починається з підключення до Інтернету, що забезпечує підключення до зовнішнього світу.

Маршрутизатори та комутатори: ці пристрої керують потоком мережевого трафіку у внутрішній мережі. Маршрутизатори з'єднують різні мережі (наприклад, локальну мережу та Інтернет), тоді як комутатори з'єднують пристрої в локальній мережі.

Локальна мережа (LAN):

Сервери: служба таксі має один сервер, який зберігає і керує критично важливими даними та програмами. Це включає сервер бази даних для зберігання інформації про клієнтів, деталей бронювання та інших відповідних даних.

Робочі станції: це комп'ютери, які використовують співробітники для повсякденних завдань, наприклад диспетчери, що керують запитами на поїздки, адміністратори, що виконують адміністративні функції, і представники служби підтримки клієнтів.

Принтери та сканери: ці пристрої під'єднані до мережі, і співробітники можуть отримати до них доступ для друку або сканування документів.

Network Attached Storage (NAS): пристрій NAS можна використовувати для централізованого зберігання файлів і спільного використання, дозволяючи співробітникам отримувати доступ до документів, форм та інших спільних ресурсів і спільно працювати над ними.

Системи зв'язку:

Голос через IP (VoIP): служба таксі використовує системи VoIP для внутрішнього та зовнішнього зв'язку. VoIP дозволяє співробітникам здійснювати дзвінки через Інтернет, забезпечуючи економію коштів і гнучкість.

Private Branch Exchange (PBX): систему PBX можна використовувати для керування вхідними та вихідними дзвінками, скеровуючи їх на відповідні розширення або відділи в організації.

Заходи безпеки:

Брандмауери: брандмауери допомагають захистити мережу від несанкціонованого доступу та зовнішніх загроз, відстежуючи та контролюючи мережевий трафік.

Віртуальна приватна мережа (VPN): VPN реалізований для встановлення безпечних з'єднань для віддаленого доступу до мережі, дозволяючи співробітникам працювати з дому або отримувати доступ до ресурсів компанії в дорозі.

Антивірус і захист від зловмисного програмного забезпечення: ці програмні рішення встановлюються на серверах, робочих станціях та інших мережевих пристроях для виявлення та запобігання зараженню шкідливим програмним забезпеченням.

Резервне копіювання та аварійне відновлення:

Регулярне резервне копіювання даних: необхідно регулярно створювати резервні копії критично важливих даних, щоб забезпечити їх доступність у разі системних збоїв, аварій або катастроф.

Зовнішнє резервне копіювання: для захисту від фізичного пошкодження або втрати даних служба таксі використовує служби хмарного зберігання.

Розглянемо організаційно-штатну структуру підрозділу:

- Управління верхнього рівня: Це вище керівництво компанії, яке включає генерального директора та співласників компанії. Вони встановлюють загальні стратегічні цілі та напрямки розвитку компанії.
- Диспетчерський центр: Це центральний пункт керування роботою служби таксі. Диспетчерський центр включає диспетчерів, які приймають та обробляють замовлення від клієнтів, взаємодіють з водіями та забезпечують координацію поїздок.
- Транспортний відділ: Водії таксі є важливим елементом служби таксі. Вони можуть бути співробітниками компанії або працювати як незалежні підрядники. Водії виконують замовлення та забезпечують перевезення пасажирів. Керівник транспортного відділу слідкує за належним обслуговуванням автопарку компанії.

– Фінансовий відділ: Фінансовий відділ займається фінансовим управлінням компанії, включаючи облік, оплату водіям, операційний контроль та фінансовий звіт.
– Відділ кадрів: Відділ кадрів займається підпором співробітників.

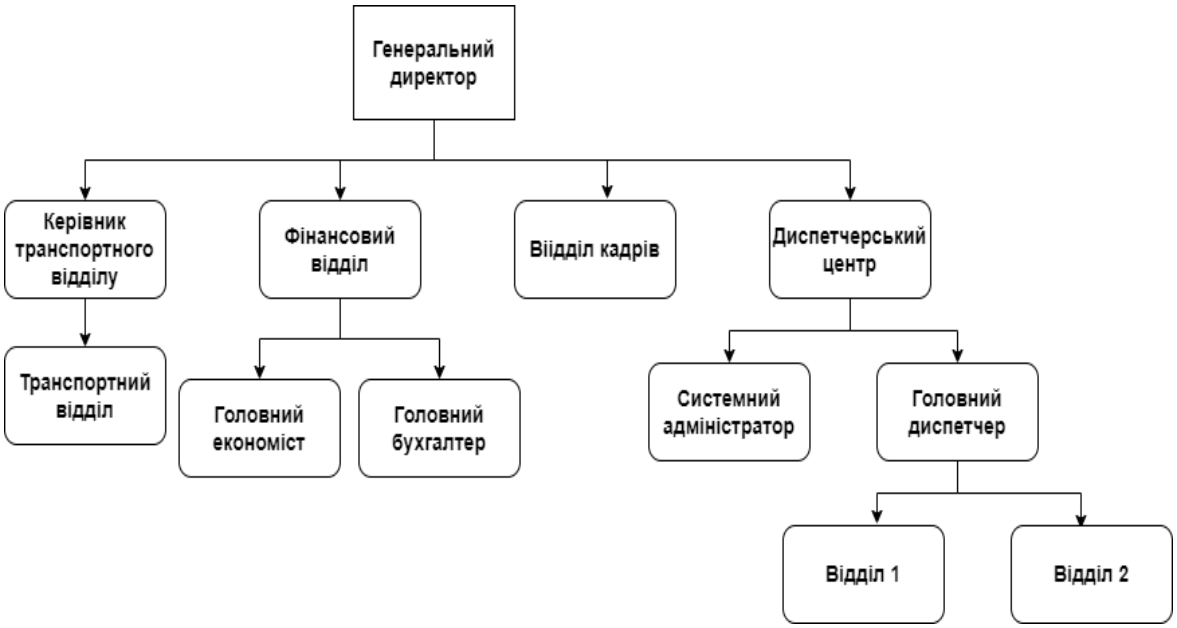

Рисунок 1.1 – Схема організаційної структури компанії “Opti”

Компанія Opti спеціалізується на пасажирських перевезення , тому важливо мати власну мережу з виходом в інтернет. Структура підприємства з багатьох філій по всій Україні. Філія для якого потрібно розробити корпоративну мережу знаходиться у місті Дніпро. Вона складається з офісу для якого орендовано декілька приміщень в п`ятиповерховій будівлі, а також автопарку, який знаходиться поруч.

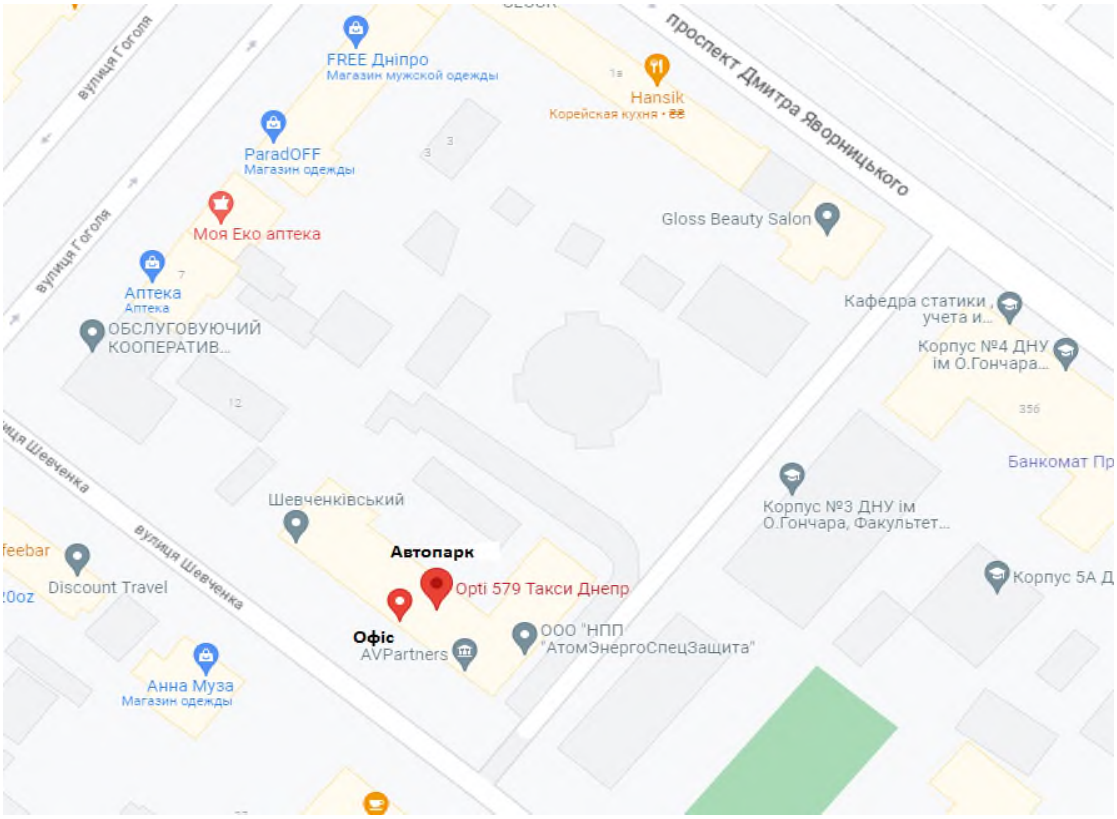

Рисунок 1.2 - топологічна схема розміщення філії компанії “Opti” у місті Дніпро.

1.4 Відомості про технології збору та передачі інформації.

Сучасні служби таксі використовують передові технології для збору та передачі інформації з метою поліпшення процесу замовлення та виконання поїздок. Інновації в цій галузі сприяють покращенню точності та ефективності, забезпечують зручність для клієнтів та оптимізують роботу водіїв. Тут ми розглянемо основні технології збору та передачі інформації в службі таксі.

Мобільні додатки

Однією з ключових технологій є використання мобільних додатків для замовлення таксі. Клієнти можуть завантажити додаток на свої смартфони і замовити таксі всього лише кількома дотиками. Додатки дозволяють вказати місце посадки та пункт призначення, переглянути інформацію про доступні автомобілі та водіїв, а також отримати оцінку часу очікування. Мобільні додатки спрощують процес замовлення та забезпечують зручність для клієнтів.

GPS-навігація

Служба таксі використовує GPS-навігаційні системи для відстеження розташування автомобілів та оптимального маршруту. Це дозволяє диспетчерам в реальному часі відстежувати розташування водіїв і надсилати їм нові замовлення. GPS-навігація також допомагає водіям швидко знайти найкоротший шлях до пункту призначення, зменшуючи час поїздки та забезпечуючи ефективність.

Текстові повідомлення

Для комунікації між диспетчерами та водіями використовуються системи текстових повідомлень. Це дозволяє диспетчерам надсилати інструкції водіям, розв'язувати проблеми та взаємодіяти в режимі реального часу. Текстові повідомлення також використовуються для повідомлення клієнтам про статус їх замовлення та оновлення про прибуття таксі.

Електронна оплата

Служба таксі «Opti» пропонують різні електронну системи оплати, що дозволяють клієнтам зручно оплачувати поїздки. Це може бути зроблено через мобільний додаток або сайт компанії. Електронна оплата спрощує процес оплати для клієнтів та забезпечує безпеку та зручність

1.5 Види та конфігурація обладнання, що використовується в компанії.

На комп`ютерах використовується така конфігурація:

- Процесор: 6-ядерний процесор Intel Core i5-11600K
- Пам'ять: 16 ГБ DDR4 RAM
- Жорсткий диск: 500 ГБ NVMe твердотільний накопичувач (SSD) для операційної системи та програмного забезпечення та 1 ТБ жорсткий диск (HDD) для додаткового зберігання
- Операційна система: Windows XP
- Дисплей: 24-дюймовий IPS-монітор Full HD (1920x1080).
- Відеокарта: Integrated Intel UHD Graphics
- Мережева карта TP-LINK Archer TX3000E

- Підключення: порти USB 3.0, HDMI, DisplayPort, Ethernet і Wi-Fi
- Клавіатура та миша: Ергономічний набір клавіатури та миші
- Функції безпеки: TPM (Trusted Platform Module) для покращеної безпеки та попередньо встановлене програмне забезпечення для захисту від вірусів/шкідливих програм
- Управління шумом і нагріванням: ефективна система охолодження та шумозаглушуючі компоненти

У службі таксі використовується кілька типів серверів для підтримки різних аспектів операцій. Ось сервери, які використовуються в службі таксі:

Диспетчерський сервер: диспетчерський сервер є важливим компонентом служби таксі. Він керує диспетчеризацією водіїв і координує розподіл поїздок. Він отримує запити на поїздки від клієнтів, обробляє їх і призначає доступним водіям. Диспетчерський сервер також може обслуговувати відстеження транспортних засобів у реальному часі та надавати відповідну інформацію як водіям, так і клієнтам.

Сервер бази даних: сервер бази даних зберігає та керує критично важливими даними служби таксі, такими як інформація про клієнта, деталі водія, історія поїздок і записи про платежі. Це забезпечує ефективне зберігання, пошук і обробку даних для загальної роботи служби таксі.

Платіжний сервер: платіжний сервер обробляє платежі та керує транзакціями. Він безпечно обробляє платіжну інформацію, взаємодіє з платіжними шлюзами або процесорами, а також перевіряє та авторизує платежі за завершені поїздки. Цей сервер відповідає за забезпечення безпеки та цілісності фінансових операцій у службі таксі.

GPS/Сервер місцезнаходження: GPS/Сервер місцезнаходження відповідає за збір і обробку даних GPS від транспортних засобів. Він відстежує місцезнаходження таксі в режимі реального часу, оновлює їх положення та надає точну інформацію про місцезнаходження на диспетчерський сервер та інші відповідні системи. Цей сервер відіграє вирішальну роль у ефективному розподілі та відстеженні поїздок.

Комунікаційний сервер: комунікаційний сервер підтримує різні канали зв’язку в службі таксі. Він може включати можливості VoIP (голос через IP) для спілкування між водієм і клієнтом, функції чату для внутрішнього обміну повідомленнями та інтеграцію із зовнішніми системами зв’язку, такими як SMS або служби push-повідомлень.

Веб-сервер/сервер додатків: веб-сервер/сервер додатків розміщує веб- та мобільні додатки служби таксі. Він керує логікою, обробкою та доставкою інформації кінцевим користувачам. Він може містити такі функції, як бронювання поїздок, реєстрація водія, підтримка клієнтів та інтеграція з іншими системами.

Сервер резервного копіювання: сервер резервного копіювання відповідає за регулярне резервне копіювання критично важливих даних для забезпечення їх доступності та відновлення у разі системних збоїв, аварій або катастроф. Він може використовувати програмне забезпечення та процеси резервного копіювання для створення та зберігання резервних копій важливих даних і конфігурацій.

1.6 Аналітичний огляд існуючих способів обробки та передачі інформації, принципів побудови об`єкта проектування, відомих рішень у галузі.

Для більшої безпеки, надійності та ефективності запропоновано розділити мережу на 5 підмереж (LAN) для кожного відділу. Завдяки цьому кожен відділ буде обмежено можливість використанням серверів. Кожен відділ буде мати доступ тільки до свого серверу. Мережу рекомендовано розділити за таким принципом:

Диспетчерський центр розміщено в LAN-5, для транспортного відділу виділено— LAN-2, LAN-3 —для відділу кадрів. , фінансовий відділ буде знаходитись у LAN-4. Відділ управління— LAN-1.

1.7 Завдання і мета роботи.

Завдання роботи - створення комп'ютерної системи, яка буде відповідати вимогам до провідних технологій та новітнього обладнання..

Метою роботи є створення комп’ютерної системи компанії —”Opti”, яка буде характеризуватися актуальністю та своєчасністю. Під час розробки повинно бути

розглянуто сучасні тенденції розвитку та методи розробки спеціалізованих комп`ютерних систем.

1.8 Визначення можливих напрямків рішення поставлених завдань.

Для виконання мети роботи було впроваджено додаткові заходи з безпеки та захисту інформації від несанкціанованого доступу до інформації, такого як:

- Налаштування маршрутизаторів на підтримку служби AAA
- Налаштування мереж VLAN
- Налаштування параметрів безпеки комутаторів
- Налаштування віртуальної приватної мережі site-to-site VPN з використанням IPsec

Для розгортання локальної мережі використовувалася технологія мережі Ethernet. Для підключення до глобальної мережі використовувалися оптоволоконні кабелі.

Зв’язок між компонентами в мережі повинен забезпечуватися за допомогою світчів та роутерів Cisco.

2 РОЗРОБКА АПАРАТНОЇ ЧАСТИНИ КОМП’ЮТЕРНОЇ СИСТЕМИ

2.1. Вимоги до системи в цілому

2.1.1 Вимоги до структури і функціонування системи

У службі таксі Opti комп’ютерна система призначена для забезпечення ефективного зв’язку, управління даними, дозволяє надсилати один одному текстові повідомлення, забезпечує доступ до архівів файлів та веб-сторінок, дозволяє обмінюються голосовими повідомленнями.

Відповідно до організаційної структури, корпоративна мережа служби таксі “Opti” (далі КМ) буде складатися з 5 підсистем:

− підсистема адміністрації;

− підсистема транспортного відділу ;

− підсистема відділу кадрів;

− підсистема фінансового відділу;

− підсистема диспетчерського центру.

Для цього проекту потрібно створити 5 локальних мереж і з використанням технології фрейм-релей. Відповідно, слід використовувати IP-блок-адресу для призначення підмережі 172.22.16.0/20. Кількість вузлів для LAN: LAN1 – 46; LAN2 – 57; LAN3 – 98; LAN4 – 90; LAN5 – 221.

Масштабованість і резервування: спроектувати мережу з урахуванням майбутнього зростання та забезпечення масштабованості додавши до максимальної відстані між компонентами системи в 30м ще 10% запасу.

Фізична структура мережі повинна бути організована за допомогою зон відповідальності (зони впливу) для комутаційного шафи та розташування робочих місць у відповідних групах лану.

2.1.2 Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами системи

Обмін даними між підсистемами повинен здійснюватися за допомогою використання стандартизованих протоколів і форматів обміну даними та проходити в єдиному логічному просторі.

Методи зв'язку повинні підтримувати інтерактивне та чуйне спілкування між компонентами. Вони повинні забезпечувати обмін інформацією в режимі реального часу часі, дозволяючи компонентам взаємодіяти та швидко реагувати на запити та повідомлення один одного.

2.1.3 Вимоги до сумісності з суміжними системами

Методи та засоби комунікації мають бути сумісними з компонентами, задіяними в обміні інформацією. Це включає в себе сумісність з точки зору протоколів, форматів даних та інтерфейсів, щоб забезпечити повну інтеграцію та взаємодію.

Програмне забезпечення системи має забезпечувати інтеграцію і сумісність на інформаційному рівні з іншими системами. Інформаційна сумісність повинна забезпечуватися на рівні експорту-імпорту XML-документів.

2.1.4 вимоги до діагностування системи

Система повинна відстежуватись режимі реального часу, надаючи постійну інформацію про свій стан та виявляючи потенційні проблеми, щойно вони виникають.

Система повинна мати журналювання та звітування для запису діагностичних даних, повідомлень про помилки та системних подій. Повинні генеруватись вичерпні звіти, які підсумовують результати діагностики, що полегшує технікам аналіз та інтерпретацію даних.

Раз на місяць повинна проводитись повна діагностика системи, включаючи апаратне забезпечення, програмне забезпечення, мережеві компоненти та електрообладнання.

2.1.5 Перспективи розвитку системи

Система повинна мати можливість:

- модернізації шляхом удосконалення або заміни на нове технічного та загального програмного забезпечення
- Модернізації апаратного забезпечення для більшої ергономічності, мінімізації енергоспоживання та оптимізації використання ресурсів.
- Інтеграції нових технологій, таких як блокчейн, IoT та штучний інтелект (AI).

2.1.6 Вимоги до чисельності і кваліфікації персоналу, що обслуговує систему, і режиму його роботи.

Вимоги до чисельності і кваліфікації персоналу, необхідного для обслуговування КМ наведено в таблиці 2.1

Таблиця 2.1 - Вимоги до чисельності і кваліфікації обслуговуючого персоналу персоналу КМ

№ п/п	Посада	Кількість	Кваліфікація	Режим роботи
1	Системний адміністратор	2	Вища повна освіта	1 зміна
2	Комп`ютерний інженер	3	Вища повна освіта	1 зміна
3	Інженер-електронік	1	Середня спеціальна освіта	1 зміна

Компанія працює цілодобово, в 2 зміни по 12 годин. В денну зміну працює 1 системний адміністратор, 2 комп`ютерні інженери та 1 інженер-електронік, в нічну – 1 системний адміністратор та 1 комп`ютерний інженер. Всі працівник повинні пройти медогляд та первинний інструктаж. Періодичний інструктаж з техніки безпеки - не рідше 1 разу на рік. Періодичний медогляд - не рідше 2 разів на рік.

2.1.7 Вимоги до показників призначення

пропускна здатність – 1000 Мб/с

передача пакету - не повинна перевищувати 5 мс

час відповіді – не більше 1 с

ping – не більше 110 мс

2.1.8 Вимоги до надійності системи

Система повинна бути розроблена так, щоб справлятися з апаратними або програмними збоями, не впливаючи на загальну продуктивність системи та не спричиняючи втрати даних. Для забезпечення безперебійної роботи мають бути передбачені заходи резервування, такі як резервні джерела живлення, резервні компоненти та механізми відновлення після відмови.

У всіх рівнях повинні бути реалізовані функції коректної автоматичної зупинки роботи технічних засобів, підключених до системи безперебійного електропостачання, в т.ч. автономного, при тривалій відсутності електроживлення.

Системи зберігання повинні бути представлені RAID-системами високої готовності. Надлишкові з'єднання повинні забезпечувати доступність даних навіть у разі виходу з ладу вузлів, контролерів або кабелів. З'єднання з системами зберігання даних в кластері повинно бути реалізовано як з використанням інтерфейсів SCSI, так і на основі Fibre Channel технології.

Для швидкого та ефективного відновлення повинні бути запасні кабелі, комутатори, маршрутизатори та інше критичне обладнання комп`ютерної системи.

2.1.9 Вимоги до експлуатації, технічного обслуговування, ремонта і збере-ження

У приміщеннях, призначених для експлуатації Системи, повинні бути відсутніми агресивні середовища, масова концентрація пилу в повітрі має бути не більше 0,75 мг / м3, електрична складова електромагнітного поля перешкод не повинна перевищувати 0,3 Н/м в діапазоні частот від 0,15 до 300,00 МГц.

Напруга живлення мережі має бути 220 В, 50 Гц.

Вимоги щодо забезпечення пожежної безпеки та електробезпеки (заземлення) у приміщеннях повинні бути виконані відповідно до ГОСТ 12.1.004-91 "ССБТ. Пожежна безпека. Загальні вимоги", ГОСТ Р 50571.22-2000. "Електроустановки будівель. Частина 7. Вимоги до спеціальних електроустановок. Розділ 707. Заземлення устаткування обробки інформації", "Правилами улаштування електроустановок", "Правилами техніки безпеки при експлуатації електроустановок споживачів".

2.1.10 Вимоги до ергономіки та технічної естетики

Сервери та інше обладнання повинно бути розміщено в окремій кімнаті. В цій кімнаті повинна бути встановлена вентиляція для забезпечення нормальних кліматичних умов роботи обладнання.

Робочі місця з ПК слід так розташовувати відносно вікон, щоб природне світло падало збоку переважно зліва. Вони повинні бути розташовані від стіни з вікнами на відстані не менш 1,5м, від інших стін – на відстані 1 м, відстань між ними має становити не менш ніж 1,5 м. Площа приміщення на одне робоче місце повинна становити 6 м2, а об'єм – не менше 20 м3.

2.1.11 Вимоги до захисту інформації від несанкціонованого доступу

Компоненти мережі повинні мати високий рівень захисту від несанкціонованого доступу до налаштувань. Для цього:

- на кожному пристрої мережі повинен бути встановлений логін та пароль користувача не менше 8 символів.
- відсутність змоги підключення зовнішніх носіїв без належних прав.
- повинно бути додано та налаштовано міжмережний екран ASA, який включає в себе встановлення правил фільтрації пакетів, налаштування VPN-з'єднань, налаштування механізмів виявлення та запобігання вторгнень (IDS/IPS) та інших функцій безпеки.
- Для забезпечення безпеки серверів налаштувати функції безпеки портів на комутаторах, що забезпечують підключення до цих серверів.

2.1.12 Вимоги до патентної чистоти

Патентна чистота КМ та всіх її компонентів повинна бути сертифікована забезпечуватися на території України.

2.1.13 Вимоги до уніфікації та стандартизації

КМ повинна бути обладнана персональними комп'ютерами з характеристиками:

- Об`м оперативної пам'яті не менше 8 Гбайт;
- кількість ядер процесора не менше 4;
- тактова частота процесора не менше 3,0 ГГц;
- об`єм пам`яті накопичувача не менше 500 Гбайт;
- операційна система Windows XP.

- Дисплей: 24-дюймовий IPS-монітор Full HD (1920x1080)

Вимоги до лінгвістичної уніфікації

- розробка прикладного програмного забезпечення повинна вестися з використанням мов високого рівня.
- основною мовою взаємодії користувачів і системи повинна бути українська та англійська мови.
- графічний інтерфейс користувача підсистеми повинен бути створений українською та англійськими мовами.

2.2 Вимоги до функцій, які виконуються системою

2.2.2 Вимоги до інформаційного забезпечення підсистем

Інформаційна підсистема служби таксі “Opti” повинна включати наступні компоненти та функції:

Диспетчерська система: інформаційна система включає диспетчерську систему, яка приймає та обробляє запити клієнтів на послуги таксі. Він керує розподілом доступних транспортних засобів за запитами клієнтів на основі таких факторів, як близькість, доступність і пріоритет.

Керування клієнтами: інформаційна система підтримує базу даних клієнтів, у якій зберігається інформація про клієнтів, включаючи контактні дані, уподобання та історичні дані. Це забезпечує ефективне керування клієнтами, полегшує спілкування з клієнтами та підтримує персоналізоване обслуговування.

Відстеження та керування транспортними засобами: інформаційна система включає систему відстеження транспортних засобів, яка використовує технологію GPS для відстеження місцезнаходження та статусу кожного таксі в режимі реального часу. Це дозволяє системі оптимізувати призначення транспортних засобів, контролювати продуктивність автопарку та надавати клієнтам точний очікуваний час прибуття.

Звітність та аналітика: інформаційна система створює різні звіти та надає аналітичну інформацію для моніторингу та управління службою таксі. Він відстежує ключові показники ефективності (KPI), такі як дохід, задоволеність

клієнтів, використання транспортного засобу та продуктивність водія, що дозволяє керівництву приймати обґрунтовані рішення та визначати сфери для вдосконалення.

Керування водієм: інформаційна система включає функції для керування водієм, такі як профілі водія, планування та відстеження продуктивності. Він керує призначеннями водіїв, відстежує доступність водіїв і полегшує зв’язок між водіями та диспетчерською системою.

Інтеграція із зовнішніми системами: інформаційна система інтегрується із зовнішніми системами, такими як картографічні служби, платіжні шлюзи, постачальники інформації про дорожній рух і платформи зворотного зв’язку з клієнтами, щоб покращити функціональність і покращити якість послуг.

2.2.3 Вимоги до математичного забезпечення підсистем

Інформаційна система з підтримки діяльності служби таксі повинна мати функції, які нададуть змогу клієнтам служби швидко знайти автомобіль за їхніми побажаннями за умови, що про якість обслуговування клієнт зможе залишити відгук и поставити оцінку за поїздку. Також необхідно щоб система автоматично розраховувала вартість поїздки. Для цього необхідно:

- бути створено алгоритм пошуку автомобіля і водія згідно умов клієнта;
- бути створено алгоритм моніторингу рейтингу водіїв.
- бути створено алгоритм розрахунку вартості на основі зібраних даних

Для виконання цього завдання необхідно:

- Створити або використати базу даних, яка містить в собі необхідну інформацією про водіїв, автомобілів та клієнтів.
- Вибрати Entity Framework для пошуку автомобіля з водієм.
- Створити інтерфейс для взаємодії з клієнтом

Ця підсистема повинна працювати за наступним алгоритмом:

1. використання Entity Framework для додавання в базу даних відгуку та оцінки;
2. складання шкалу оцінювання водія;

3. надання можливості адміністратору контролювати діяльність водіїв за відгуками;
4. оновлення системою рейтингу кожного водія після завершеної поїздки та контроль оцінки водіїв.
5. плата за проїзд автоматично розраховується системою на основі дальності поїздки та від рейтингу водія.

2.2.4 Вимоги до програмного забезпечення

Служба таксі “Opti” надає послуги з пасажирських перевезень та транспортування роботодавцям із використанням Інтернет-технологій. Для цього необхідно мати відповідне програмне забезпечення.

Таблиця 2.2 – вимоги до програмного забезпечення

Тип ПЗ	Вимоги до ПЗ
Диспетчерське програмне забезпечення	Повинно керувати та оптимізувати розподіл доступних таксі відповідно до запитів клієнтів на основі таких факторів, як розташування, близькість і доступність. А також забезпечувати для диспетчеризації забезпечує ефективну маршрутизацію та своєчасну відповідь на запити клієнтів.
Мобільний додаток	Повинен мати функції бронювання поїздки, відстежування призначеного їм таксі та здійснення платежів.
Бухгалтерське та фінансове програмне забезпечення	Повинно надавати змогу керувати фінансовими аспектами, зокрема нарахуванням заробітної плати, витратами, податками та фінансовою звітністю. ведення фінансового обліку.
Платформи зв’язку та обміну повідомленнями	Повинні включати такі функції, як обмін повідомленнями, голосові дзвінки та push-повідомлення,

Програмне забезпечення для захисту даних і конфіденційності	Повинно включати шифрування, засоби контролю доступу та безпечні протоколи зв’язку для захисту даних від несанкціонованого доступу чи злому.

Служба таксі “Opti використовує програмне забезпечення наведене у таблиці 2.3

Таблиця 2.3 Програмне забезпечення “Opti”

Тип програмного забезпечення	Назва
Операційна система	MS Windows
Антивірусне ПЗ	Avast
ПЗ для роботи з документами	MS Office 2016
ПЗ для роботи з базами даних	OpenOffice Base
Інтернет браузер	Mozilla Firefox
Мобільний додаток	Opti
VoIP-телефонія	Zadarma
Автоматизований комплекс для служб таксі	Нова диспетчерська

2.2.5 Вимоги до методичного забезпечення

Методологічне забезпечення повинно включати навчальні програми та ініціативи для володіння працівниками необхідними навичками та знаннями, необхідними для дотримання встановлених методологій. Навчання повинно проводитися за допомогою майстер-класів, семінарів, онлайн-курсів та внутрішніх тренінгів.

Також методологічне забезпечення повинно включати механізми управління для забезпечення дотримання галузевих стандартів, правових вимог і внутрішньої політики. Для цього повинно бути створено наглядових комітетів і проводитися перевірки відповідності для контролю за дотриманням методологій і нормативних зобов’язань.

2.3 Розробка апаратної частини комп`ютерної системи підприємства

2.3.1 Розробка специфікації апаратних засобів КС

Специфікація обладнання наведена в таблиці 2.4

Таблиця 2.4 - специфікація апаратних засобів КС

Тип, найменування	Технічна характеристика	Кількість
Маршрутизатор Cisco 2911/K9	Інтерфейс підключення (LAN-порт):3x10/100/1000BASE-T Керування: Web-інтерфейс, SNMP Базові можливості: Ethernet Брандмауер (Firewall) NAT Підтримка VPN DHCP-сервер Демілітаризована зона (DMZ)	9
Комутатор Cisco WS-C2960L-24PQ-LL	Підтримка протоколу 802. 1x Живлення через Ethernet Plus (PoE+) з потужністю до 370 Вт RJ45 та USB-консоль для спрощених операцій Порти консолі RJ45 Ethernet USB міні-B USB-A порт для зберігання та Bluetooth консолі Процесор та пам'ять: CPU ARMv7 800 MHz DRAM 512 MB	15

	Flash 256 MB Продуктивність: Швидкість передачі (64-byte L3 packets) 41. 67 Mpps	
Серверне обладнання Cisco UCS C180 M4S	Модель процесора Intel Xeon E5-2420 Частота процесора 2.8 GHz Кількість ядер 8 Об’єм оперативної пам’ятї 8 Gb Інтерфейс SAS, SATA	5

2.3.2 Розробка архітектури мережі підприємства

Для створення архітектури мережі підприємства було враховано фізичну структуру будівлі та розташування вузлів мережі. Всі підрозділи розміщенні на одному поверсі.

Мережа розділена на п’ять підмереж, залежно від можливостей та напряму діяльності підприємства. Підмережа №1 «Відділ управління» призначена для підключення 46 абонентів. Підмережа №2 «Транспортний відділ » призначена для підключення 57 абонентів. Підмережа №3 «Відділ кадрів» призначена для підключення 98 абонентів. Підмережа No4 «Фінансовий відділ» призначена для зв’язку зі 90. Підмережа No5 «Диспетчерський центр» призначена для зв’язку зі 221.

Одним рішень було використання комутаційного шкафа, розміщеного у центральній точці будівлі, звідки виходять кабелі до різних робочих місць та вузлів мережі. Кабельна інфраструктура включає наступні типи кабелів:

1. Кабелі Ethernet для локальної мережі (LAN):
2. Волоконно-оптичний кабель (ОВК):

Фізична структура мережі залежала від розміщення робочих місць, серверних кімнат, комутаційних шаф, а також інфраструктури в будівлі. Розташування кабелів було організоване за допомогою горизонтальних та вертикальних кабельних каналів.

Горизонтальні кабельні канали використовуються для підключення робочих місць до комутаційного шафи.

Довжина горизонтальних кабельних каналів залежить від розміщення робочих місць та їх відстані до комутаційного шафи. Для кожної групи лану з відповідною кількістю вузлів (46, 57, 98, 90, 221), розраховується необхідна довжина горизонтальних кабельних каналів.

Так як комутаційна шафа знаходиться в центральній точці, то всі відділи знаходяться приблизно на одинаковій відстані від комутаційної шафи в 30м . Додамо до цієї відстані ще 10% запасу на облік можливих змін і розширень мережі. Отже, загальна довжина горизонтальних кабельних каналів для кожної групи лану повинна бути:

1. Група 1 (46 вузлів): 46 * (30 + 10%) = 46 * 33 = 1 518 метри.
2. Група 2 (57 вузлів): 57 * (30 + 10%) = 57 * 33 = 1 881 метри.
3. Група 3 (98 вузлів): 98 * (30 + 10%) = 98 * 33 = 3 234 метри.
4. Група 4 (90 вузлів): 90 * (30 + 10%) = 90 * 33 = 2970 метри.
5. Група 5 (221 вузол): 221 * (30 + 10%) = 221 * 33 = 7293 метри.

Загальна довжина горизонтальних кабельних каналів для всієї мережі буде сумою довжин каналів кожної групи лану:

1 518+1 881+3 234+2970+7293 = 16 896 метрів.

Також одним з рішень було створення VLAN - групи хостів з загальним набором вимог, що взаємодіють так, ніби вони прикріплені до одного домену, незалежно від їх фізичного розташування. Це дозволить кінцевим підмережам бути згрупованими разом, перебуваючи на різних мережевих комутаторів.

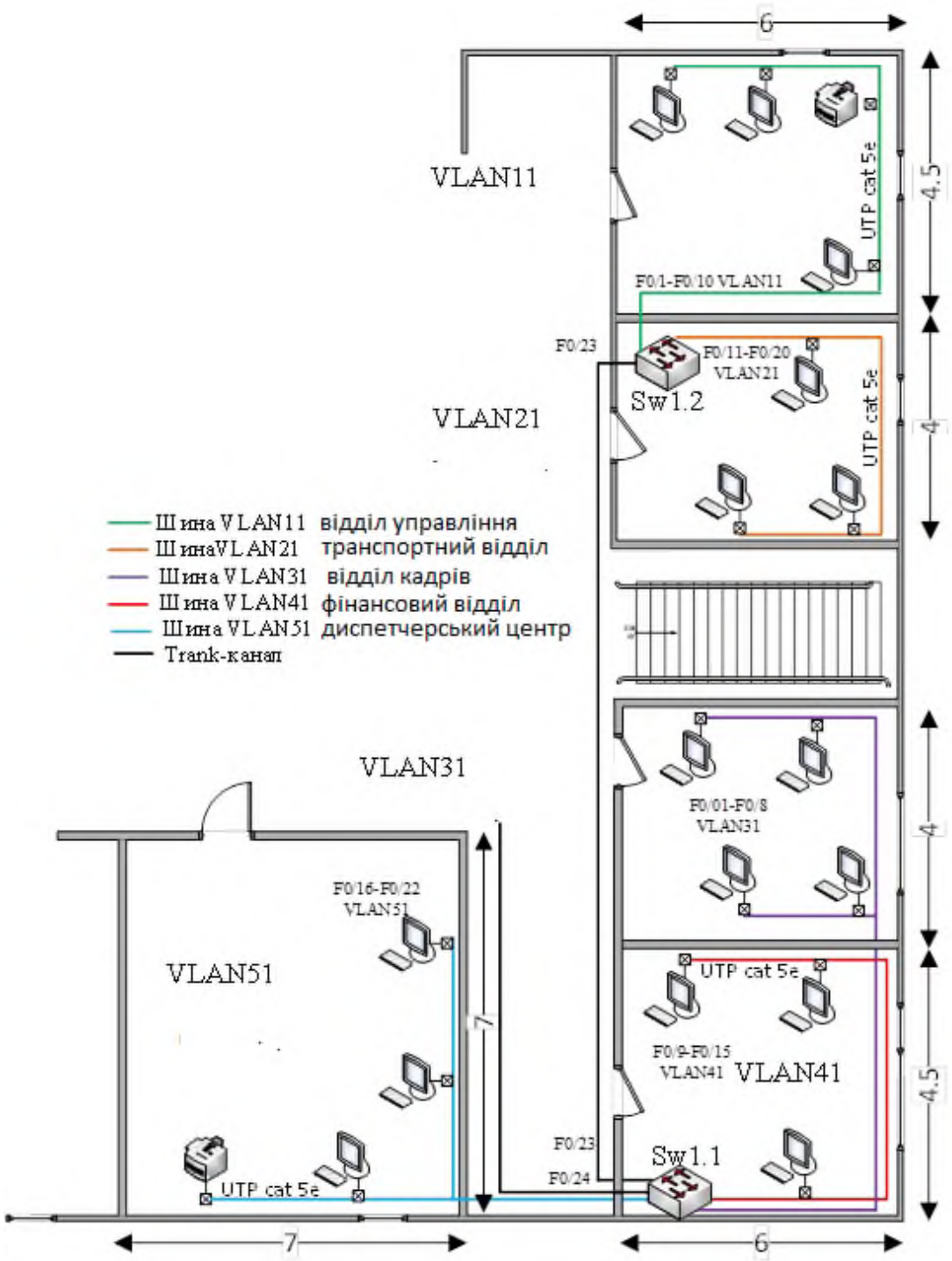

Рис 2.1 – фрагмент схеми фізичної топології мережі

Для організації мережі і вибору та роутерів потрібно врахувати кількість вузлів у кожному лані і загальні потреби мережі в трафіку та пропускній здатності.

На основному рівні є п’ять маршрутизаторів. Мережа будується за допомогою IP-адрес, 172.22.16.0/20. Сегмент середовища (підмережа IP) маршрутизатором розділений на п’ять підмереж .

При розробці мережі, було використано IP-адреси версії 4. Для забезпечення доступу мережі до Інтернету, використовується технологія NAT.

Основною мережевою технологією була обрана технологія Ethernet. На рівні доступу робочі групи підключаються за допомогою технології Fast Ethernet. Між маршрутизатором і комутатором - гігабітний Ethernet .

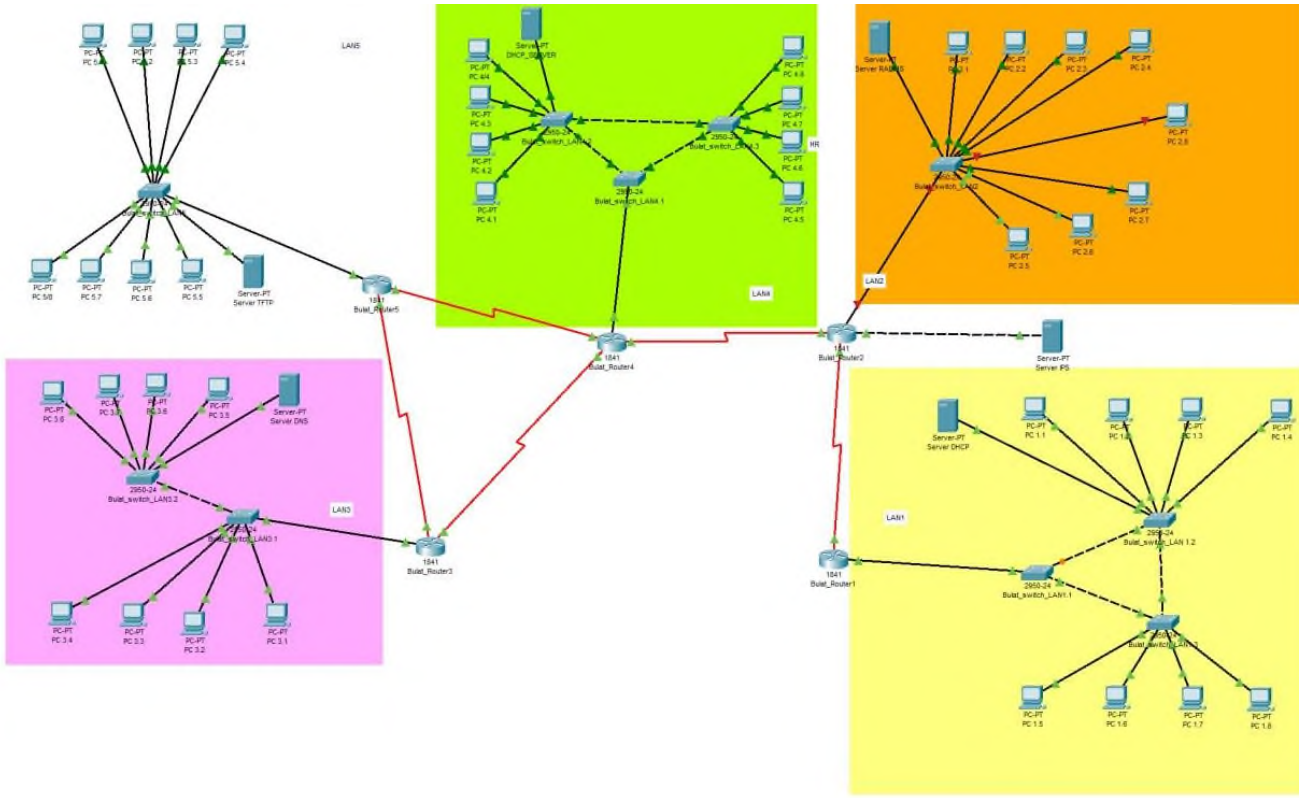

Рис 2.2 – топологічна архітектура мережі

2.3.3 Розрахунок інтенсивності трафіку вихідного трафіку найбільшої локальної мережі підприємства

Для того, щоб зробити розрахунки ключових характеристик вихідного трафіку, треба щоб мережа центру зайнятості була завантажена на 100%. Для вході ми маємо:

- найбільша кількість вузлів 221;
- середній показник інтенсивності трафіку: $\mu = 136$ (кадрів/с);
- розмір повідомлення в середньому: 650 байт;
- передача пакету не повинна перевищувати ≤6 мс.

– пропускна здатність не повинна перевищувати 1000 Мб/с

Перемикач рівня розподілу перенаправляє трафік до маршрутизатора через вихідну лінію з пропускною здатністю 1000 Мбіт / с.

$$\mu вих = 1000\,000\,000 /(650 \cdot 8) = 192\,310 \text{ пакетів/с.}$$

Кожне джерело виробляє в середньому 136 пакетів на секунду, що обмежує його до підключення до максимального розподілу на рівні комутації .

$$N = 192\,310 / 136 = 1\,414 \text{ джерел.}$$

Він заповнює мережу з 212 ПК.

Кожен з 212 ПК посилає потік заявок з інтенсивністю 136 кадрів/с.

Інтенсивність вихідного трафіку від всіх користувачів:

$$\lambda = N \cdot \mu = 212 \cdot 136 = 28\,832 \text{ (пакетів/с).}$$

Коефіцієнт затримки на рівні розподілу, показник навантаження на вихідний канал зв'язку, що впливає на затримку черги .

$$\rho = \lambda / \mu вих = 28\,832/ 192\,310 = 0{,}2$$

Коефіцієнт зайнятості комутатора рівня розподілу :

$$r = \rho / (1 – \rho) = 0{,}2 / (1 - 0{,}2) = 0{,}25$$

Середня довжина черги:

$$L_чер=\rho^2/(1-\rho)=(0{,}2)^2/(1-0{,}2)=0{,}05$$

Ця цифра корисна під час черги пристрою. В апаратному забезпеченні можна вказати максимальний розмір черги пакетів.

Середній час пакетів у черзі:

$$T_оч=L_чер/\lambda=0{,}05/28\,832=4173 \text{ мкс}$$

Це значення менше необхідного значення ≤ 5 мс, що відповідає вимогам.

Пропускна здатність каналу:

$$\lambda= b/l$$

$$b=\lambda*l=28\,832*650*8=149\,926\,400 \text{ біт/с}=149{,}26\text{Мбіт/с}$$

Він відповідає пропускній здатності вихідного каналу 1000 Мбіт / с.

3 РОЗРОБКА КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розрахунок схеми адресації корпоративної мережі

Таблиця 3.1 – Схема адресації мережі

Назва підмережі	Розмір	Адреса	Десяткова маска	Діапазон доступних адрес
LAN1	46	172.22.16.0	255.255.255.192	172.22.16.1 - 172.22.16.62
LAN2	57	172.22.16.64	255.255.255.192	172.22.16.65 - 172.22.16.126
LAN3	98	172.22.16.128	255.255.255.192	172.22.16.129 - 172.22.16.190
LAN4	90	172.22.17.0	255.255.255.192	172.22.17.1 - 172.22.17.62
LAN5	221	172.22.17.64	255.255.255.128	172.22.17.65 - 172.22.17.190
VLAN11	30	172.22.16.0	255.255.255.224	172.22.16.1 - 172.22.16.30
VLAN21	30	172.22.16.32	255.255.255.224	172.22.16.33 - 172.22.16.62
VLAN31	30	172.22.16.64	255.255.255.224	172.22.16.65 - 172.22.16.94
VLAN41	30	172.22.16.96	255.255.255.224	172.22.16.97 - 172.22.16.126
VLAN51	30	172.22.16.128	255.255.255.224	172.22.16.129 - 172.22.16.158
VLAN99	10	172.22.16.160	255.255.255.240	172.22.16.161 - 172.22.16.174
LAN4	30	172.22.17.128	255.255.255.224	172.22.17.129 - 172.22.17.158
LAN5	50	172.22.17.160	255.255.255.192	172.22.17.161 - 172.22.17.222
WAN1	2	10.1.1.1	255.255.255.0	10.1.1.1 - 10.1.1.254
WAN2	2	10.1.1.2	255.255.255.0	10.1.1.1 - 10.1.1.254
WAN3	2	10.1.1.3	255.255.255.0	10.1.1.1 - 10.1.1.254
WAN4	2	10.1.1.4	255.255.255.0	10.1.1.1 - 10.1.1.254
NTTP-сервер	-	209.165.200.4	-	-

Згідно технічних вимог проектування мережі, 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+9+1;
- останні з використовуваних IP-адрес призначено вузлам;
- в мережах VLAN використовується адресація кінцевих пристроїв по протоколу DHCP.

3.2 Налаштування та перевірка роботи комп'ютерної системи

3.2.1 Базове налаштування конфігурації пристроїв

Для захисту мережного обладнання від несанкціонованого доступу виконаємо базове налаштування пристроїв на прикладі Bulat_Router1:

```
Router>enable
Router#config
Router(config)#hostname Bulat_Router1
Bulat_Router1 (config)#line console 0
Bulat_Router1 (config-line)#password cisco
Bulat_Router1 (config-line)#login
Bulat_Router1 (config-line)#line vty 0 15
Bulat_Router1 (config-line)#password cisco
Bulat_Router1 (config-line)#login
Bulat_Router1 (config-line)#enable secret class
Bulat_Router1 (config)#service password-encryption
Bulat_Router1 (config)#banner motd "Bulat_Router1 "
Bulat_Router1 (config)#ip domain-name Bulat_Router1
Bulat_Router1 (config)#crypto key generate rsa
How many bits in the modulus [512]: 1024
Bulat_Router1 (config)#username 123-20ck_Bulat password cisco
Bulat_Router1 (config)#line vty 0 15
Bulat_Router1 (config-line)#transport input ssh
Bulat_Router1 (config-line)#login local
```

Рис 3.1- базове налаштування Bulat_Router1

3.2.2 Налаштування маршрутизаторів корпоративної мережі

Щоб користувачі з віддалених мереж могли взаємодіяти між собою, необхідно на маршрутизаторах налаштувати таблиці маршрутизації. Це можна виконати, додаючи маршрути до мереж статично, або динамічно, тобто за допомогою протоколу маршрутизації EIGRP. Маршрутизатори протоколу EIGRP встановлюють зв'язки зі своїми сусідніми пристроями.

Налаштування EIGRP включає в себе оголошення безпосередньо підключених локальних мереж і відключення поширення оновлень маршрутизації на інтерфейси в локальні мережі:

```
Bulat_Router1(config)#router eigrp 15
Bulat_Router1(config-router)#no auto-summary
Bulat_Router1(config-router)# passive-interface GigabitEthernet0/0
Bulat_Router1(config-router)#passive-interface GigabitEthernet0/1
Bulat_Router1(config-router)#passive-interface GigabitEthernet0/1.25
Bulat_Router1(config-router)# passive-interface GigabitEthernet0/1.35
Bulat_Router1(config-router)#passive-interface GigabitEthernet0/1.45
Bulat_Router1(config-router)# passive-interface GigabitEthernet0/1.99
Bulat_Router1(config-router)#network 172.22.16.0 0.0.0.127
Bulat_Router1(config-router)#network 10.1.15.0 0.0.0.3
Bulat_Router1(config-router)# network 10.1.15.8 0.0.0.3
Bulat_Router1(config-router)# network 172.22.120.0
```

Рис 3.2 - Налаштування EIGRP

3.2.3 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 на прикордонному маршрутизаторі налаштовано згідно з вимогами:

- пул адрес: з 209.165.202.1 по 209.165.202.30;
- 10.4.2.3/26 – адреса Server HTTP;
- номер списку доступу: 4;

– ім'я пулу: Internet.

NAT на Bulat_Router3:

Для перевірки роботи NAT відобразим таблицю перевотрювань (табл.3.3).

Таблиця 3.3 – Таблиця перевотрювань NAT на Bulat_Router3

Протокол	Inside Global	Inside Local	Outside Global	Outside Local
TCP	209.165.202.1	10.4.2.3:80	209.165.200.4:80	10.4.2.3:80
TCP	209.165.202.1	10.4.2.4:443	209.165.200.4:443	10.4.2.4:443
TCP	209.165.202.2	10.4.3.1:22	209.165.200.4:22	10.4.3.1:22
TCP	209.165.202.2	10.4.3.2:3389	209.165.200.4:3389	10.4.3.2:3389
TCP	209.165.202.3	10.4.3.3:80	209.165.200.4:80	10.4.3.3:80
TCP	209.165.202.3	10.4.3.4:443	209.165.200.4:443	10.4.3.4:443

3.2.4 Налаштування агрегування каналів

Port Aggregation Protocol (PAgPЗа технічними вимогами в підмережі «Валютний філіал» на комутаторах застосована технологія агрегування каналів. Виконано об'єднання фізичних портів f0/1-4 в port-channel, використовуючи PAgP в якості канального протоколу.

Для переверки роботи протоколу PAgP застосуємо команду *Bulat_Switch_LAN5#show etherchannel summary*.

Результат перевірки наведений нижче.

interface GigabitEthernet0/1

description Connection to Bulat_Switch_LAN1

channel-group 1 mode desirable

```
interface GigabitEthernet0/2
 description Connection to Bulat_Switch_LAN2
 channel-group 1 mode desirable

interface GigabitEthernet0/3
 description Connection to Bulat_Switch_LAN3
 channel-group 2 mode desirable

interface GigabitEthernet0/4
 description Connection to Bulat_Switch_LAN5
 channel-group 2 mode desirable

interface Port-channel1
 description EtherChannel to Bulat_Switch_LAN1 and Bulat_Switch_LAN2
 switchport mode trunk

interface Port-channel2
 description EtherChannel to Bulat_Switch_LAN3 and Bulat_Switch_LAN5
 switchport mode trunk
```

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

3.3 Захист інформації в комп`ютерній системі від несанкціонованого доступу

3.3.1 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;

– налаштування міжмережного екрану ASA;

– на портах комутаторів, підключених до серверів, налаштовуються функції безпеки портів;

– маршрутизатори мережі налаштовуються на підтримку служби AAA та RADIUS-сервера.

3.3.2 Налаштування маршрутизаторів на підтримку служби AAA

Авторизація користувачів при підключені до мережевих пристроїв виконується за допомогою сервісів AAA (Authentication Authorization and Accounting).

Запуск служби AAA:

arduinoCopy code

Bulat_Router1(config)# aaa new-model

Налаштування методу аутентифікації за замовчуванням з використанням локальної бази користувачів:

scssCopy code

Bulat_Router1(config)# aaa authentication login default local

Налаштування методу аутентифікації "Login" з використанням сервера RADIUS, а у разі недоступності - з використанням локальної бази користувачів:

arduinoCopy code

Bulat_Router1(config)# aaa authentication login Login group radius local

Застосування методу аутентифікації "Login" на консольній лінії:

arduinoCopy code

Bulat_Router1(config)# line console 0 Bulat_Router1(config-line)# login authentication Login

Застосування методу аутентифікації за замовчуванням на vty-лініях:

arduinoCopy code

Bulat_Router1(config)# line vty 0 4 Bulat_Router1(config-line)# login authentication default

Налаштування RADIUS-сервера:

Вказання IP-адреси RADIUS-сервера та настроювання порту аутентифікації:

arduinoCopy code

Bulat_Router1(config)# radius-server host 10.4.3.5 auth-port 1645

Встановлення ключа доступу до RADIUS-сервера:

arduinoCopy code

Bulat_Router1(config)# radius-server key radius123

3.3.3 Налаштування мереж VLAN

Згідно до вимог в підмережі були створені 6 підмережі. Відповідно до архітектури мережі в КС підприємства створені мережі VLAN з присвоєним кожній з них ім'ям.

Таблиця 3.4 – Назви VLAN для мережі

Номер VLAN	Ім’я VLAN	Примітка
1	Default	Не використовується
11	Uprav	Відділ управління
21	Transport	Транспортний відділ
31	Finansoviy	Відділ кадрів
41	Finansoviy	Фінансовий відділ
51	Dyspetch	Диспетчерський центр
99	Native	Транковый канал 802.1Q

Для налаштування VLAN на комутаторах порти, до яких підключені хости, повинні бути в режимі доступу access, а порти, до яких підключені мережеві

пристрої (маршрутизатори, комутатори) в режимі trank. Усі невикористані фізичні порти комутаторів відключаємо.

Для перевірки налаштування відобразимо сумарну інформацію про налаштування VLAN на комутаторах і відповідних їм портів

Таблиця 3.5 – адресація VLAN

VLAN	Ім'я	IP-адреса	Маска	Інтерфейси
1	Default	-	-	Fa0/1-9, Fa0/15-20, G0/1-2, S0/1-2, Vlan1
11	VLAN11	172.22.16.1	255.255.255.0	Fa0/10
21	VLAN21	172.22.17.1	255.255.255.0	Fa0/11
31	VLAN31	172.22.18.1	255.255.255.0	Fa0/12
41	VLAN41	172.22.19.1	255.255.255.0	Fa0/13
51	VLAN51	172.22.20.1	255.255.255.0	Fa0/14
99	Native	10.1.1.1	255.255.255.0	Fa0/21-24, G0/0, G0/3

Ці таблиці відображають налаштування VLAN для вказаної мережі. Кожному VLAN призначено відповідні IP-адреси та маски, а також зазначені відповідні інтерфейси, на яких вони активні. Зовнішня адреса NTTP-сервера не відображається у таблицях налаштувань VLAN, оскільки це адресування відбувається на рівні маршрутизації.

3.3.4 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.

```
interface range FastEthernet0/1-24
 switchport mode access
 switchport access vlan 1
 spanning-tree portfast
 spanning-tree bpduguard enable
 storm-control broadcast level 10
 storm-control action shutdown
 storm-control action trap
 no cdp enable
 no lldp transmit
 no lldp receive

interface range GigabitEthernet0/1-2
 switchport mode trunk
 switchport trunk allowed vlan 1,11,21,31,41,51,99
 switchport trunk native vlan 99
 switchport nonegotiate
 spanning-tree portfast trunk
 spanning-tree bpduguard enable
 storm-control broadcast level 10
 storm-control action shutdown
 storm-control action trap
 no cdp enable
```

```
 no lldp transmit
 no lldp receive

interface Vlan1
 ip access-group 101 in
 ip arp inspection limit rate 10
 ip arp inspection validate src-mac dst-mac
 ip dhcp snooping limit rate 10
 ip dhcp snooping trust
 ip verify source port-security
 storm-control broadcast level 10
 storm-control action shutdown
 storm-control action trap

access-list 101 permit tcp any host 209.165.200.4 eq www
access-list 101 deny ip any any log
```

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

Налаштування на Bulat_Router1:

```
crypto isakmp policy 1
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key vpnkey address 209.165.200.6
crypto ipsec transform-set myset esp-aes 256 esp-sha-hmac
crypto map vpnmap 10 ipsec-isakmp
 set peer 209.165.200.6
 set transform-set myset
 match address 101
```

```
access-list 101 permit ip 10.4.3.0 0.0.0.255 10.4.5.0 0.0.0.255
interface GigabitEthernet0/1
 crypto map vpnmap
```

У цьому коді використовується IPsec для налаштування віртуальної приватної мережі site-to-site VPN. Ключ **vpnkey** використовується для автентифікації між Bulat_Router1 та Bulat_Router2 (зовнішній IP-адреса: 209.165.200.6). Застосовується набір перетворень **myset**, що використовує шифрування AES 256 та аутентифікацію SHA HMAC. Також створюється криптографічне відображення **vpnmap** з використанням цих налаштувань. Список доступу 101 встановлює відповідність між мережами, які будуть обмінюватися даними через VPN. На інтерфейсі GigabitEthernet0/1 встановлюється криптографічне відображення **vpnmap**, яке охоплює трафік VPN.

ВИСНОВОК

Дипломна робота характеризується актуальністю та своєчасністю, оскільки присвячена питанням впровадження та використання комп`ютерних систем у компаніях. На прикладі компанії “Opti” було розглянуто сучасні тенденції розвитку та методи розробки спеціалізованих комп`ютерних систем.

У першому розділі розглянуто питання особливостей галузі компанії для чіткого формулювання завдання та мети роботи.

У другому розділі сформульовані технічні вимоги до розробки комп’ютерної системи та вимоги до інформаційного забезпечення підсистем. Здійснено вибір і обґрунтування структурної схеми комплексу технічних засобів комп’ютерної системи. Також проведена розробка архітектури мережі підприємства та розраховано інтенсивність вихідного трафіку найбільшої локальної мережі підприємства.

У третьому розділі спроектовано комп`ютерну мережу, налаштовано адресацію її компонентів та пристроїв підключених до неї. Розроблено методи для захисту інформації від несанкціонованого доступу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Методичні рекомендації до виконання кваліфікаційної роботи бакалавра студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп'ютерна інженерія / Л.І. Цвіркун, С.М. Ткаченко, Я.В. Панферова, Д.О. Бешта, Л.В. Бешта. – Д.: НТУ «Дніпровська політехніка», 2022.
2. Методичні вказівки до виконання розділу „Охорона праці“ в дипломних проектах (роботах) бакалаврів інституту електроенергетики / В.І. Голінько, В.Ю. Фрундін, Ю.І. Чеберячко, М.Ю. Іконніков. – Д.: Державний ВНЗ «Національний гірничий університет», 2012. – 8 с
3. 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, НТУ «Дніпровська політехніка», 2018. – Ч. 1. – 41 с.
4. Кафедра Інформаційних технологій та комп'ютерної інженерії. Історія створення кафедри [Електронний ресурс] – Режим доступу до ресурсу: https://it.nmu.org.ua/ua/about_department_ist/history_department.php
5. https://ir.nmu.org.ua/bitstream/handle/123456789/156423/
6. https://www.0312.ua/news/cat/24
7. https://studfile.net/preview/5376394/page:4/
8. https://ela.kpi.ua/bitstream/123456789/47283/1/Tseiukov_bakalavr.pdf

ДОДАТОК А

Текст програми налаштування мережі комп’ютерної системи

Міністерство освіти і науки України
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ НАЛАШТУВАННЯ МЕРЕЖІ КОМП’ЮТЕРНОЇ СИСТЕМИ

Текст програми
804.02070743.23001-01 12 01

2023

АННОТАЦІЯ

Дана програма містить в собі частину програмного коду для програмування налаштування компонентів корпоративної мережі комп’ютерної системи.

Програма призначена для забезпечення налаштування DHCP, AAA, інтерфейсів, протоколу маршрутизації NAT, консольних і vty ліній та створення мереж VPN, домену комп’ютерної системи.

ЗМІСТ

1. Код налаштування в мережі VLAN
2. Налаштування безпеки комутаторів

Код налаштування в мережі VLAN :

```
enable
configure terminal

! Налаштування VLAN
vlan 11
name LAN1
exit

vlan 21
name LAN2
exit

vlan 31
name LAN3
exit

vlan 99
name LAN4
exit

vlan 100
name LAN5
exit

! Налаштування інтерфейсів для VLAN
interface FastEthernet0/1
switchport mode access
```

```
switchport access vlan 11
exit

interface FastEthernet0/2
switchport mode access
switchport access vlan 11
exit

interface FastEthernet0/3
switchport mode access
switchport access vlan 21
exit

interface FastEthernet0/4
switchport mode access
switchport access vlan 21
exit

interface FastEthernet0/5
switchport mode access
switchport access vlan 31
exit

interface FastEthernet0/6
switchport mode access
switchport access vlan 31
exit
```

```
interface FastEthernet0/7
switchport mode access
switchport access vlan 99
exit

interface FastEthernet0/8
switchport mode access
switchport access vlan 99
exit

interface FastEthernet0/9
switchport mode access
switchport access vlan 100
exit

interface FastEthernet0/11
switchport mode access
switchport access vlan 100
exit

exit
```

Налаштування безпеки комутаторів подано нижче:

```
enable
configure terminal

! Налаштування безпеки портів для комутаторів

! Налаштування портів комутатора для LAN1
```

```
interface FastEthernet0/1
switchport mode access
switchport access vlan 11
switchport port-security
switchport port-security maximum 2
switchport port-security violation restrict
exit

interface FastEthernet0/2
switchport mode access
switchport access vlan 11
switchport port-security
switchport port-security maximum 2
switchport port-security violation restrict
exit

! Налаштування портів комутатора для LAN2
interface FastEthernet0/3
switchport mode access
switchport access vlan 21
switchport port-security
switchport port-security maximum 2
switchport port-security violation restrict
exit

interface FastEthernet0/4
switchport mode access
switchport access vlan 21
```

```
switchport port-security
switchport port-security maximum 2
switchport port-security violation restrict
exit

! Налаштування портів комутатора для LAN3
interface FastEthernet0/5
switchport mode access
switchport access vlan 31
switchport port-security
switchport port-security maximum 2
switchport port-security violation restrict
exit

interface FastEthernet0/6
switchport mode access
switchport access vlan 31
switchport port-security
switchport port-security maximum 2
switchport port-security violation restrict
exit

! Налаштування портів комутатора для LAN4
interface FastEthernet0/7
switchport mode access
switchport access vlan 99
switchport port-security
switchport port-security maximum 2
```

```
switchport port-security violation restrict
exit

interface FastEthernet0/8
switchport mode access
switchport access vlan 99
switchport port-security
switchport port-security maximum 2
switchport port-security violation restrict
exit

! Налаштування портів комутатора для LAN5
interface FastEthernet0/9
switchport mode access
switchport access vlan 100
switchport port-security
switchport port-security maximum 2
switchport port-security violation restrict
exit

interface FastEthernet0/11
switchport mode access
switchport access vlan 100
switchport port-security
switchport port-security maximum 2
switchport port-security violation restrict
exit
```